1

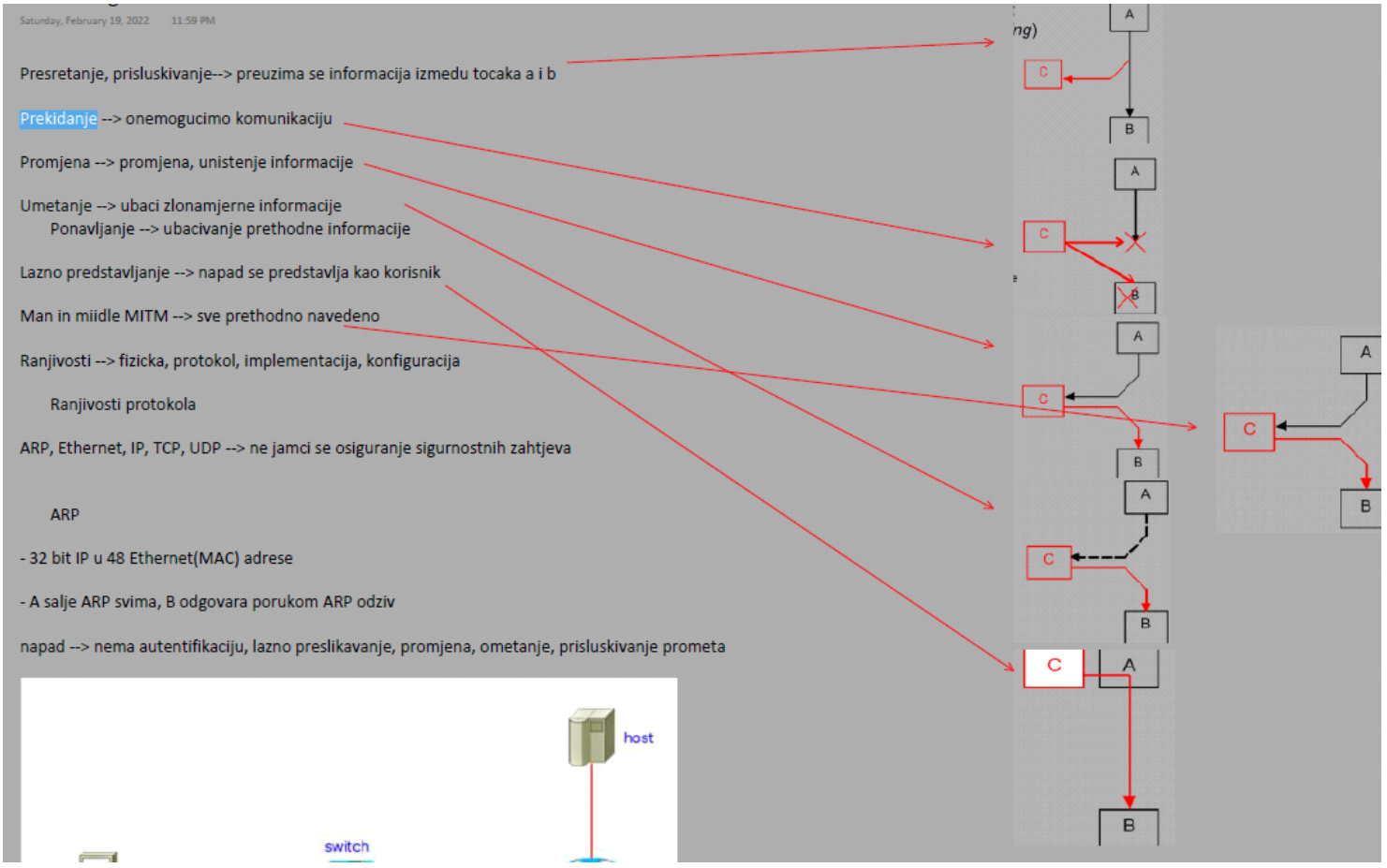
Thursday, April 13, 2023 12:34 PM

ranjivost - slabost u izvedbi sustava koju je moguće iskoristiti kako bi se izazvala šteta

prijetnja - skup okolnosti koji moze nanijeti stetu
cilj : osoblje
metoda: prijevara, zloupotreba
vrsta: namjerna/slucajna, aktivna/pasivna, unutranja/vanjska

napad - iskoristavanje ranjivosti sustava

nadzor - mjere predstoznosti



3 uvjeta zlonamjernog napadaca : metoda, prilika, motiv

napad iznutra - saboteri, zloputreba admin prava

napadi izvana - kriminalne ili teroristicke organizacije, obavjestajne, hackeri, script kiddies

nacini napada - elektronicki (virus, uskracivanje usluge); ostalo (krada, prijevara, krivotvorenje)

cjelovitost --> podaci pohranjeni u izvornom i nepromijenjenom obliku
povjerljivost --> podaci dostupni samo ovlastenim entitetima
raspolozivost --> dostupnost usluge u trenutku

autentifikacija --> provjera identitea

neporecivost --> ne mogu poreci akciju
kontrola pristupa (access control)

ranjivosti - malware, lazne poruke (hoax), drustvene mreze
sigurnost - sposobnost sustava da se odupre neocekivanim dogadajima
ranjivost - posljedica slabosti i nedostataka

2

Thursday, April 13, 2023 4:12 PM

podatkovni sloj - 2 sloj referentnog modela, komunikacija 2 racunala

ethernet - u lokalnim mrezama, 10Mbps do 100 Gbps, zicna (bakar i optika), bezicna
problemi = SNMP (davanje informacija, promjena podataka na switchu)
= LLDP (podaci o topologiji)
= ssh na switch

zastita = fizicka infrastruktura (horizontalno, vertikalno, mrezne ucinice)
= izoliranje prometa po VLANovima
= autentifikacija prije pristupa
= ogranicenje MAC adresa po pristupu
= admin prava, antivirus, SSL, IPSec

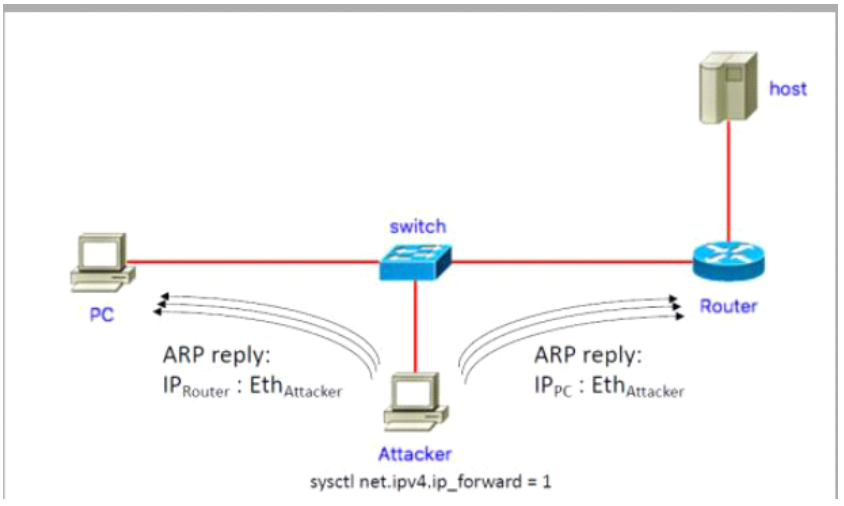
elementi - switch, hub, kabeli (vertikalno, horizontalno, bakrene zice i optika)

Cilj napadaca na ethernetu - medukorak slozenijem napadu, pracenje prometa, pretvaranje
preduvjeti - ovlasti, pristup (Internet, router)

fizicki pristup ethernetu - manipulacija zice (bakrene, optiku teze), pristup mreznim uticnicama, preklopnicima

prisluskivanje prometa - dohvat informacija, (tcpdump, wireshark)
problem za napadaca - ne stize sav promet do svih mreznih kartica
napad na router - genriranje mnostvo laznih MAC adresa <-- zastita (ogranicenje broja MAC adresa po portu)

ARP - jednostavan, nezasticen protokol
napad --> nema autentifikaciju, lazno preslikavanje, promjena, ometanje, prisluskivanje prometa



alati --> arpoison, parasite
otkrivanje --> ispis ARP cache-a, trece racunalo, tesko detektirati,
zastita <-- onemogucavanje i rucna konfiguracija

NDP - zamijenjen ARP, nema autentifikacije, staticki se prepisuju dinamickim, ARP Spoofing --> NDP Spoofing
SEND = NDP + kriptografska zastita
CGA = uredaj RSA kljuceva, zastita od NDP spoofinga
nedostaci = hrpa kriptografskih operacija, cuvanje puno stanja, UNIX

R/STP = razapinjuce stablo, BPDU podatkovne jedinice, cilj --> ostvariti topologiju s najjacim preklopnicima
faze = root brige, root ports, designated ports, stanja pristupa (onemogucen, blokirajuci, osluskuje, ucenje, prosljeduje)

napad = namjerna modifikacija (uskracivanje, preusmjeravanje), izvrsenje napada (na linuxu postoji STP)
problem za napadaca = velika kolicina prometa

zastita = BPDU Guard, Root Guard

Virtualni LAN = izolacija prometa, komunikacija VLANova preko routera, jedan router moze imati vise VLANova (knjigovodstvo, internet)
napadi = switch spoofing (dodavanje pca koje se predstavlja swich)
= double tagging (napadac salje okvir s dvije oznake)
da bi radio --> napadac i zrtva na razlicitim switchevima, napadac MAX adresa, napadac ima VLAN ID
zastita --> ne koristi nativni VLAN

DHCP = DHCP(DORA), fiksiranje adresa na temelju MACa
= klijent salje UDP na broadcast, server salje ponudu

problemi = zastita poruke, lazni DHCP server (uskracivanje, preusmjeravanje)

3 Wifi

Thursday, April 13, 2023 11:33 PM

Osnovna svojstva
-koriste elektromagnetske valove za prijenos podataka

2 nacina rada
Adhoc --> direktno spajanje stanica
infrasturukturni --> koristi se AP kao pristupna tocka

pojedina pristupna tocka = BSSID
skup pristupnih tocaka = ESSID

BSS = jedna pristupna tocka (AP), oglasava SSID
ESS = vise pristupnih tocaka koje imaju isti SSID a razlicti BSSID spojeno na switch, prijelaz iz jednog AP u drugi bez raskidanja komunikacije

Protokoli za sigurnost WIFI-a
WEP, WPA, WPA2, WPA3 (zastita za nedovoljno kompleksne lozinke, maknuti ranjivi kripto algoritmi, Easy connect -spajanje IoT uredaja)

Kontrola pristupa

WPA/WPA2/WPA3
PSK --> dijeljena tajna
jednostavno postavljanje
nedostatak je odlazak zaposlenika koji sa sobom nosi lozinku

-//-Enterprise
centralizirana autentifikacija koju obavlja poseban server

Autentifikacija na EAPu = autentifikacijski server (radius)

EAP = request, response, success, failure, prijenos preko Etherneta u 802.1 definiran je EAPOL

Radius = mrezni protokol za centralizirani AAA (authentication, authorization, accounting) , model server/client (UDP), backend za autentifikaciju
= korisnik salje NAS serveru zahtijev za pristup koristenjem svojih vjerodajnica
= NAS i Radius se stiti IPSec tunelom
= koristi sheme PAP, CHAP, EAP
= verificira se identitet korisnika, adresa, broj telefona, stanje racuna
= NAS salje Radiusu Access Request (username/password, dodatno podaci o korisniku (mrezna adresa, broj telefona))
<-- Radius odgovara (access reject, access challege (pin, token, kartica), access accept

= RADIUSaaS (Radius as Service) - jednostavna i sigurna autentifikacija, provjera opozvanih certifikata
= Diameter (podrska za TCP, SCTP), zastita na transportnom sloju TLS/IPsec

Fizicki sloj
Karakteristike -snaga, frekvencija, modulaicje
Spektar -2.4 i 5 GHz
Oblik i razmjestaj antena/snaga --> utjecce na pokrivenost

Vrste okvira --> podatkovni (korisnicki podaci <--kriptografski zasticeni), upravljacki (MAC) , kontrolni (RTS, CTS)

Napadi uskracivanjem usluge --> RF jamming, virutal jamming, spoofed disconnect, lazni zahtjevi za mrezu

Napadi na kriptografiju
WEP --> aircrack-ng moze nabavit password
WPA --> laziranje sadrzaja poruke
WPA2 --> KRACK

Nekriptografski napadi na WPA i WPA2

WPA PSK --> pogadanje dijeljene tajne
PSK --> komprimitiranje klijenta, ne desifiranje prometa
WPS --> unos broja ili na pritisak gumba
--> potrebno je samo 11000 pokusaja

Napad WPA2 Enterprise - ranjivost ovisi konrektnoj EAP metodi, EAP-MD5 (pogadanje lozinke), EAP-TLS (sigurni ali problem certifikati)

iOS Wifi Poruka - WPA koristi TKIP (nesiguran)
- WPA2 koristi CCMP (sigurniji, AES)
- napad na mrezu WPA + TKIP (four way handshake)
- WPA2 (DoS napad, rouge access)

Neovlastene i otvorene pristupne tocke
Neovlastene pristupne tocke(rouge access) --> usb koji se spaja na laptop
Otvorene pristupne tocke na javnim mjestima --> mogu biti podmetnute

Preporuke za sigurnost - koristiti wpa3, wpa2 enterprise, ne koristi wps

4 Mrezni sloj

Friday, April 14, 2023 3:30 PM

- bilo koja 2 cvora u mrezi, router (salje pakete), sigurnost (firewall)

Ranjivosti IPv4
- nespojna
- laka izmjena paketa
- citljivost podataka

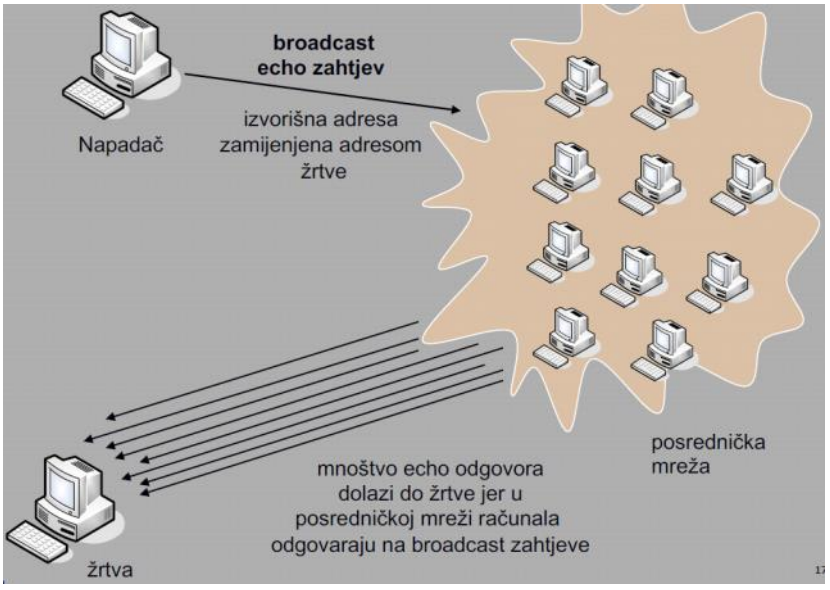
Spoofing --> lazna adresa posiljatelja (DDos)
zastita -->filtriranje neispranih izvorisnihadresa
dobre prakse za antispoofing --> uRPF (filtriranje na ulazu, propusta se ako njegova izvorsna adresa postoji u tablici usmjeravaja i dolazi po istom portu
(access list, savi)

Nonroutable mrezne adrese - 0.0.0.0, 127.0.0.0 localhost

Fragmentacija --> IP datagram > MTU , zavarati firewalle
ID --> da znamo koje treba sastavit
offset --> gdje se nalazi
more --> u svim osim u zadnjem

PingOfDeath --> prekoracuje velicinu IP datagrama (65k)
Teardrop --> fragmenti se prekrivaju pa se kernel skrsi kad ih sastavi
TCP overwrite --> nije ko DoS, poksusava prevarit firewall

ICMP
-icmp redirect se moze zloupotrijebit da napad kaze da se sve njemu salje za prisluskivanje
-kroz ping se skriva promet
-smurf napad --> napadac salje brodcast svima u domeni i posalje IP od zrtve



DHCP
-automatska dodjela adresa (discover, offer, request, ack)
problemi --> poruke nisu zasticene,lazni dhcp, bilo koji kljent moze zatraziti parametre(iscrpljivanje rasplozivih adresa)

IPv6
-adrese su 128 bita, nema arpa, zaglavlje nema zastite (nije sigurniji od ipv4)
-8 grupa po 16 bita (4 hex znamenke)

Ranjivosti kojih nema --> nema skeniranja, nema brodcast adrese, nema fragmentacije
Zajednice ranjivosti (ipv4 i ipv6) --> dhcp , icmpv4 i 6, IpSec

Ranjivosti specificne za IPv6
---> samostalno podesavanje (problem privatnosti) , veliki adresni prostor, viseodredisne adrese
---> objava usmjernickih podataka, automatsko tuneliranje

ICMPv6
-nuzan za IPv6

Poboljsanje sigurnosti na mreznom sloju
--> IP nema zastite
-->opcija --> kriptiranje i zastita (VPN)

Internet - javna mreza
Intranet - privatna, unutar korporacije
Extranet - prosirenje pojma Intranet (korisnici izvan kompanije)

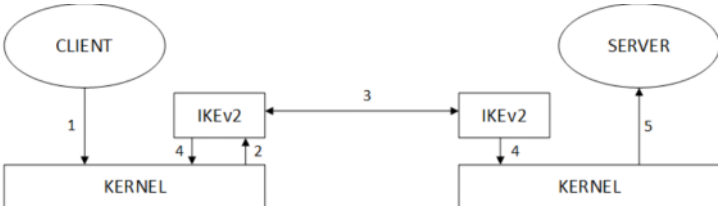
Udaljeni pristup Intranetu - zahtijevi --> privatnost (integritet podataka, IKE,TSL)
--> umrezavanje (dinamicki dodijeljenih IP adresa)
--> upravljivost (razliciti nacini autentifikacije, direktoriji za pohranu i odrzavanje informacija o korisnicima)
--> kontrola pristupa (enkripcijske tehnike ne daju prava pristupa)

Sigurni udaljeni pristup intranetu --> VPN (CIA)

VPN --> privatna mreza nad javnom inrastrukturom
Rjesenja za VPN --> OpenVPN, WireGuard, IPSec

PPTP --> lako saznati podatke, nije siguran
Vrste VPN-a --> Site to Site (private i zasticene nad routerima)
Remote access (uredaj i router)

IPsec --> protokol za krajnje tocke i razmjenu informacija (spaja 2 ili vise mreza, spaja 2 racunala)
Osnove arhitekture
tunelski (esp(ip header (podaci))) ili prijenosni nacin (ip header esp(podaci))
autentifikacija kroz certifikat, dijeljene tajne ili eap
ponasanje kranjih tocaka definirano bazama SPD i SAD
SPD --> sto treba zastititi
SAD --> kako treba stititi
Protokoli : ESP(zastitaCIAuth),
AH(IAuth), IKE



IKEv1/2 (internet ket exchange)
--> auth partnera, razmjena kljuceva, IKEv2 jednostavniji, uklonjena ranjivost

Prednosti IPsec arhitekture

ispod transportong sloja
--> potrebna prilagodba aplikacija i APIa
--> izvesti na pcu, firewallu ili routeru
ako je zakljucen u firewallu, uredaj osigrava granicu prema ostatku mreze
--> lokalni promet se ne opterecuje sigurnoscu
osigrava identitet usmjeritelja

Usluge - CIA, nedostaci (ne autentificira se se korisnik, nema sigurnosti ako sistem nije siguran

5

Friday, April 14, 2023 9:57 PM

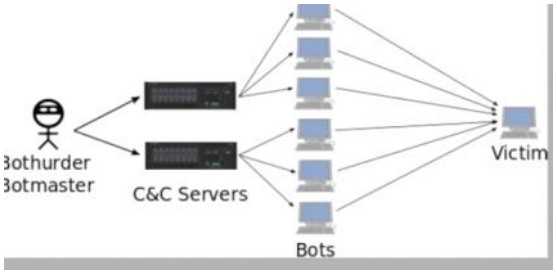
Transportni sloj - komunikacija s kraja na kraj, (70% TCP (e-posta, prijenos datoteka), 30% UDP(VoIP))

UDP
- -nema kontrole toka, pouzdan prijenos, nespojni
- -duljina 8 okteta

spoofing --> mijenjamo izvorisnu adresu i predstavljamo se kao netko drugi
hijacking --> slusa vezu, simulira posluzitelja
storm --> napadac salje samo jedan datagram i posrednik i zrtva beskonacno komuniciraju, (rjesenje <--iskljucit small service)

DoS - teska obrana jer ovisi o napadu i njegovim specificnostima, katastrofalne posljedice za zrtvu

Botnet --> skup zarazenih pc-a kojima upravlja botmaster, izvrsava neki kod
C&C server --> kod se javlja negdje na Internet, napadac moze upravljati, lako otkriti ali tesko napadaca



koristi C&C servere preko HTTPa

Zastita od volumetrickih uskracivanja usluge - poznavanje infrastrukture, dobar odnos s ISPom, napad UDP blokirati UDP

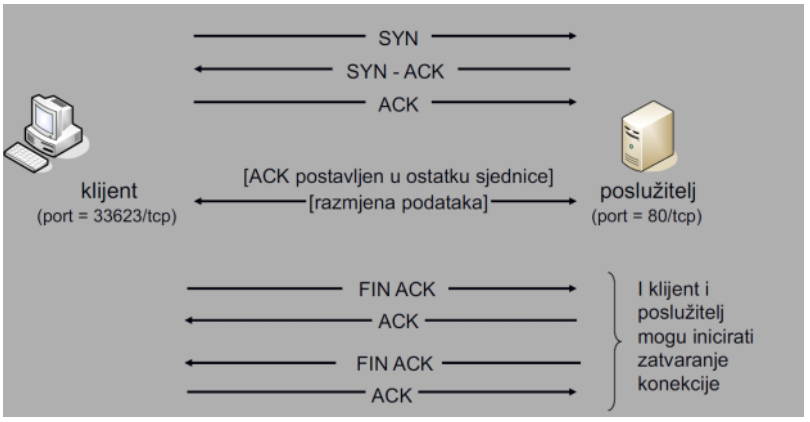
Zastita od DDoS-a -- offsite detekcija, blackholing, hibridna on/off site detekcija,
--> HW (asic, fpga (ograniceno, skupo, brzo))
--> SW (programsko, firewall, netmap)

Usluge zastite specijaliziranih tvrtki - CloudFlare, NeuStar, DPS (DDos Protection Service))
- promjene u DNSU i proxyu
udp amlification i refelction--> lazna izvorna adresa, odziv sadrzi vise podataka od upita
- DNS54 puta
- NTP 556 puta
- SNMP650 puta

TCP
- -spojni transportni protokol
- -pouzdan
- -obostrana veza

SEQ - slijedni broj
ACK - broj potvrde

Flagovi
- SYN - pocetni brojevi za uspostavu veze
- FIN - zavrseno slanje podataka
- ACK - broj potvrde
- URG - urgent
- PSH - sto je prije moguce
- RST - resetira



Napad na TCP --> na putu kojim prolaze TCP segmenti on path(zasitta IPsec),
--> van puta kojim prolaze TCP segmenti off path (pogadanje parametara)

RST napad --> prekine vezu tako da pogodi src i dst ip i port, fin slicno <--obrana {ogranicenje max velicine prozora, dodatni ack segment}
FIN napad --> slican RSTu, zatvara se pojedini kraj veze
zastite od RST i FIN napada --> TCP MD5/AO , ogranicenje velicine prozora

SYN flood --> server primi SYN i rezervira resurse --> ogranicen broj poluotvorenih veza i tako se moze zagusiti promet

napad --> nema potpune zastite,
--> metode zastite --> povecanje broja , skracanje trajanja, smanjenje kolicine stanja poluotvorenih veza
syn cache, syn cookie
--> amplificirani napad -serveru se salje syn segment s laznom adresom

ICMP napad --> poruke o greskama uzrokuju prekid veze, port ili protokol nedostizni <--rjesenje {IPsec, TLS}

6 TLS

Saturday, April 15, 2023 12:31 AM

TLS - zastita komunikacije

Osigurava - autentifikaciju servera i klijenta (provjeru identiteta servera i korisnika)
- privanotst podataka (dijeljeni simetricni kljuc)
- cjelovitost podataka

HTTP + TLS

Upotreba - HTTPS (TCP port 443, https umjesto http, handshake preko protokola record

Funkcionalnost - potvrda identiteta servera i zastita tajnosti i autenticnosti komunikacije

Autentifikacija klijenta i servera - koristenjem certifikata

Presretanje - klijenti dobivaju upozorenje u slucaju proboja, postavljanje vlastitog CA
- skidanje virusa

napadi --> SSL Stripping, BEAST, CRIME

TLS 1.3
--> brzi, sigurniji, maknute stare i nesigurne komponente

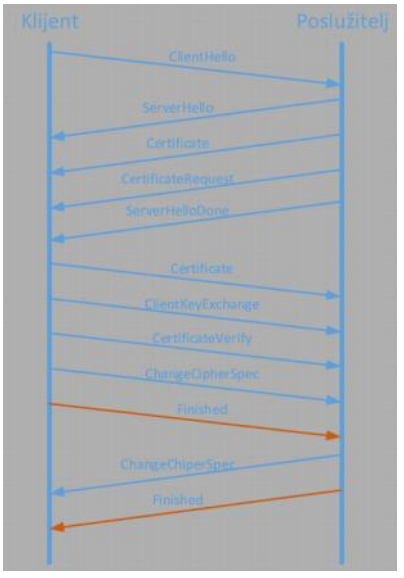
Preporuke
--> 2048 bita RSA ili 256 ECDSA, izbjeci SSL2, SSL3.0, TLS1.0, TLS1.1
--> dovoljna pokrivenost domena, u certifikatu staviti naziv s i bez www
--> Pouzdani CA (podrzava EV, jaki algoritmi za potpis)
--> jaki Key Exchange
--> onemoguciti kompresiju

Utjecaj na performanse
--> latencija je problem zbog kriptografskih operacija na CPU

Implementacija TLSa - LibreSSL, NSS, Schannel

Sigurnost HTTPa

--> kriptirati sve, (js, slike, css)
--> projveravati kriptografski integritet cookiea
--> koristiti HSTS, CSP



6 Certifikati

Saturday, April 15, 2023 10:59 AM

Simetricni --> jedan tajni kljuc

Asimetricni --> javni kljuc dostupan svima, privatni dostupan vlasniku

Problem javnog kljuca --> netko ga je podmetnuo

rjesenje --> CA, provjerava javni kljuc, CA ima svoj certifikat (self signed)

Upralvjanje kljucevima
--> opisani standardima, (kreiranje, distribucija, koristenje, arhiviranje)
--> 20% tehnologija, 80% procedure
PKI --> povezani javni kljucevi cine infrastrukturu javnog kljuca
CRL - opozvani certifikati
CA - jamstvo certifikata
RA - identifikacija i autentifikacija
CP - certificate policy

Certifikat --> digitalni objekt (informacije o subjektu, izdavatelju, valjanosti)
(sadrzi javni kljuc, subjekt je naziv racunala) <--standard (X.509 format)
--> ugradeni su preglednike ili OS
--> izdaje ga izdavatelj certifikata CA

.CER/.CRT/.DER --> binarni, kodirani certifikat
.PEM --> dodatno kodiran po base65

Standardi i preporuke --> ASN (serijalizirati na jedinstven nacin), ITU (BER, CER, DER), BER(format kodiranja apstraknih informacija, CER, DER),
DER (jedan nacin kodiranja ASN), CER (razlika od DERa po duljini podataka)

PKCS (public key standard) --> #12 format datoteke za pohranu X.509 uz javni X.509 certifikat
CMS --> sluzi za potpisivanje, sazimanje, autentifikaciju ili sifriranje bilo kojeg oblika digitalnih podataka

Vazenje certifikata
--> javni kljuc (desetljeca)
--> privatni kljuc (sto krace)
--> opoziv kljuca (ako je kompromitiran treba ga pozvati)
--> provjera certifikata (obvezna)

Valjanosti
CRL --> opozvani certifikati
OCSP --> server koji provjeri je li certifikat valjan

Korisnici PKI
--> organizacije i pojedinci
--> nositelj certifikata (subjekt raspolaze privatnim kljucem)
--> relying parties (korisnici raspolazu javnim kljucem)

CA --> sredisnji servis sustava PKI
--> izdaje i potpisuje certifikate
--> tehnicki smisao (hardver i softver); tehnoloski (skup ljudi, procedura)
--> ugradeni u preglednike

Odgovornosti --> zastita privatnog kljuca
--> odrzavanje azurnosti CRL
--> provjera tocnosti, distribucija certifikata

CP --> skup pravila koji pokazuju na odredenu skupinu sa istim sigurnosnim zahtijevima
--> opisuje pravila rada
--> javno se objavljuje

CPS --> opisuje kako CA implenetira CP

Dodatni servisi
TSA (Timestamp authority)--> usluga vremenske ovjere (valjanost certifikata, nuzno za kvalificiranog potpisa)
TS (timestamp) --> servis vremenske ovjere (NTP, HSM)

Problemi PKI
--> primamljiv cilj
--> veliki napad na CA(DigiNotar)
--> CA ne projverava korisnika
--> zbunjujuce za korisnika
--> razlicite vrste certifikata

Izdavatelji certifikata
--> eOI
--> FINA
--> CARNET

7

Saturday, April 15, 2023 11:52 AM

Osnovno
--> fiksirani root serveri, svaki server moze pruzati usluge
--> Komponente (klijent, resolver, autoritativni server, cache server)

Scrha napada
--> MITM (pometanje laznih sjedista), preuzimanje domena, sprecavanje pristupa

prijetnje <--rjesenje
--> presretanje paketa <--IPsec/TLS nije ok (ne stiti s kraja na kraj)
--> pogadanje ID vrijednosti i predvidanje upita <--IPsec/TLs nije ok (ne stiti s kraja na kraj)
--> name chaining(trovanje cach-a) <--provjera dovibenih informacija
--> uskracivanje usluge <--upotreba anycast adresa

Kaminsky DNS attack --> napadac salje upit i za aaa.paypal i salje laznu ip adresu na paypal i tako sve dok server je ne prihvati i tako server var a korisnike

Zastitta od Cache Poisoning-a (podmetne se lazna domena)
<--mora biti ista poddomena, ne razlicita

Zastita DNS-a : TSIG
--> dinamicka osvjezavanja zone i prijenos na sekundarne polozaje

Zastita DNSa: DNSSEC
--> dokaz ispravnosti podataka, klijent pomocu resolvera dobiva sigurne podatke
--> podaci na RRu se potpisuju privatnim kljucem, potpis osigurava valjanost s kraja na kraj
--> novi zapisi (dnskey, ds, nsec), novi flagovi (cd, ad), novi bitovi(do)

Problemi <--ne osigurava povjerljivost, ne stiti od DDoS napada

Zloupotrebe DNSa --> autorizacija i autentifikacija na temelju domene, raspodjela osjetljivih podataka

Ne skriva meta podatke --> DNS over TLS / DNS over HTTPs

Napadi na usmjeravanje
--> drze mrezu na okupu
--> podjela prema mjestu koristenja (OSPF, BGP)
--> podjela protokola prema nacinu rada (distance vector, link state)

utjecaj --> podoptimalno usmjeravanje, zagusenje, preplavljivanje servera, looping, pristup podacima

OSPF --> stablo najkracih puteva (link)
RIP --> udaljenosti do svojih susjeda (distance vector)

Napadi na link --> presretanje, ometanje, ponavljanje poruka

Vanjsko usmjeravanje BGP (path vector)
--> razmjena informacija izmedu mreza

AS --> skup povezanih mreza pod istom politikom usmjeravanja

Napad na BGP
--> informacije izmedu routera nisu autentificirane
--> koristi TCP
--> krivotvorenje, brisanje, ponavljanje poruka
--> otmanje IP adresa, preusmeravanje prometa

Ciljevi --> auntetifikacija porijekla, integritet, ispravnost

8

Saturday, April 15, 2023 1:01 PM

Aplikacijski sloj --> kombinacija komunikacijskog protokola i dobro poznatih pristupa

Vidljivost aplikacija na mreznom sloju --> netstat

Udaljeno otkrivanje aplikacija --> skeniranje pristupa, otvoren pristup znaci prisutnost aplikacije
TCP skeniranje
-SYN skeniranje(salje se SYN i ceka se odgovor, ako nema odgovora ne znamo kakava je situacija), TCP connect (ako nije ukljuce n filter)
- FIN skeniranje (sigurno se moze znati da nema nicega, vraca se RST inace ignore), skeniranje framgentacijom (izbjegavanje detekcije)

Prikrivanje izvora skeniranja - idlescan (nacin skeniranja koristenjem 3. strane, zombi (mala kolicina, predvidljivi IP))
- ideja (nadi ID koji zombi koristi, salji paket gdje je izvorisna adresa zombijeva)

UDP skeniranje
-slanje praznog udp datagrama
-za zatvoren pristup pristizu poruke "icmp port unreachable"

Problemi skeniranja
-spora tehnika skeniranja, problemi (udp je nepouzdan pa moramo nekoliko puta pokusati da budemo sigurni)
-sporije nego TCP, ako je subnet 24 znaci 254 racunala za skenirat
-filter onemogucava provjeru otvorenosti porta
-ne dolaze poruke to ne znaci da je port otvoren

Poteskoce sa skeniranjem
- velik broj pristupa i skeniranja cvoru
- zbog filtera nije moguce je li port otvoren ili ne
- otvoren port ne znaci da je tamo aplikacija

Detekcija aplikacije
-aplikacija stavlja verziju svoje aplikacije u pozdravnim porukama
-problem za napadaca --> je ako je verzija genericka ili lazna ili se ne mijenja nakon patcha

Detekcija os-a
-snimanje mreznog stacka u usporedbi s bazom poznatih os-a
-detekcija nije pouzdana

Vrste i verzije os-a
-nije pouzdana ali dovoljno dobra (nmap)

Brute force (otkrivanje informacije pogadanjem)
-lozinke korisnicka imena
-online --> interakcija s uslugom, offline -radi na ukradenim podacima
zastita --> ogranicenje broja pristupa, broja pokusaja, 2FA

Sifriranje komunikacije --> IPsec, TLS, tuneliranje (SSH), ugradena enkripcija (HTTP3)

Ranjivosti implementacija - u C/C++ je lako uvesti ranjivost (buffer overflow, double free, krivi tip podataka)

Posljedice ranjivosti - usluge s privilegijama (moguca potpuna kontrola servera); shellcode (pisan u asembleru, pokrece nesto)

Opcenite zastite --> ukljucena sigurnost od pocetka
--> pisanje koda da se ne uvede ranjivost
--> CVSS - izracun ranjivosti
--> iskljuciti nepotrebne usluge, ograniciti pristup

Mail server

-nesiguran, potrebna nadogranja

MTA -mail transfer agent
MUA -mail user agent

MS Exchange -integrirano rjesenje (groupware)

FTP

-anonimni upload i download, nema zastite komunikacije, prijenos lozinke
-povecava kompleksnost firewall-a, zasebne tcp veze, izbjegavati taj protokol

Nadzor mreze

- SNMP (udaljeni nadzor (routera, switcha), koristi UDP, mogucnost DoSa)
- zastita --> provjeriti uredaje kojima je ukljucen SNMP, instalirati patcheve, izolirati VLAN i firewallom ograniciti pristup

SSH

-Open SSH(unix, windows), Putty (windows), SecureCRT (ima i GUI)

SSH Transport

- razmjena kljuceva, simetricni/asimetricni algoritam sifriranja, autentifikacije poruka i kriptografskog sazetka
- prvo se trazi zajednicki algoritam, ako ga nema veza se prekida

Usluge SSH

- udaljen rad --> ssh client
- prijenos datoteka --> scp i sftp
- tuneliranje etherena --> VPN

Problemi SSH

- netko ode iz firme
- tajni kljuc nije zasticen lozinkom
- popis racunala i javnih kljuceva