lab1

Sunday, April 3, 2022 3:14 PM

aes --> block cipher za enkripciiju, 128, 192, 256 duljine kljuceva, svi blokovi 128bit

GCM --> mod aesa koji koristi CTR za enkripciju i Galois mod za autentifikaciju

scrypt has been used instead of PBKDF2 because, in addition to being computationally expensive, it is also memory intensive and therefore more secure against the risk of custom ASICs

From <https://nitratine.net/blog/post/python-gcm-encryption-tutorial/>

scrypt is different from the SHA family --> with salt perventing rainbow table lookupe

From <https://nitratine.net/blog/post/python-gcm-encryption-tutorial/>

key == 32, 32*8 = 256 --> aes-256

salt se upisuje na pocetak datoteke
aes se radi preko kljuca iz scrypta koji je koristio salt i pass
upisuje se nonce --> sekvenca slucajnih bitova iz instance aesa i start brojaca u ctr modu
    zastita ako se koristi isti kljuc ponovno bit ce razlicito
nakon salta se upisuje i nonce za citanje i trazenje pocetka brojanja
ucitat podatke u buffer
enkriptiraj u file
upisi tag --> autentifikacijski kod iz Galois moda < -- identifikacija prilikom dekripcije

dekripcija

procitaj salt
preko scrypta pretvori salt i passwor u key
procitaj nonce .read(16)
pukni nonce i key u instancu aesa
procitaj i dekriptiraj
procitaj tag i potvrdi dekripciju

Total - salt - nonce - tag = encrypted data
    32-16-16

From <https://nitratine.net/blog/post/python-gcm-encryption-tutorial/>

From <https://nitratine.net/blog/post/python-gcm-encryption-tutorial/>

Thursday, February 10, 2022 5:32 PM

*Sigurnost je **kontinuirani proces** čijim provođenjem se osigurava određeno **stanje** (sustava, podataka/informacija). Željeno stanje je definirano **zahtjevima**.*

incident --> narusena sigurnost

Temeljni sigurnosni zahtjevi

- povjerljivost (engl. confidentiality), tajnost (engl. secrecy)
  - podaci/informacije moraju biti dostupne samo ovlaštenim entitetima
- cjelovitost, integritet (engl. integrity)
  - jamstvo da su podaci/informacije poslane, primljene ili pohranjene u izvornom i nepromijenjenom obliku
- raspoloživost (engl. availability)
  - informacije moraju biti raspoložive, a sustavi i usluge u operativnom stanju, usprkos mogućim neočekivanim i nepredvidljivim događajima
    - primjerice nestanku struje, prirodnim nepogodama, nesrećama i zlonamjernim napadima

povjerljivost --> podaci dostupni samo ovlastenim entitetima

cjelovitost --> podaci pohranjeni u izvornom i nepromijenjenom obliku

informacije raspolozive a sustav u operativnom stanju unatoc neocekivanim dogadajima

Dodatni sigurnosni zahtjevi

- Autentičnost (engl. authenticity)
  - potvrda identiteta korisnika; ovjera vjerodostojnosti (autentifikacija) sudionika komunikacije; ovjera izvora podataka
- Neporecivost (engl. non-repudiation)
  - sudionici ne mogu poreći akciju u kojoj su sudjelovali, npr. nemogućnost naknadnog odricanja slanja, odnosno primanja, poruke

autenticnost --> provjera identitea

neporecivost --> ne mogu poreci akciju

- Sigurnosni zahtjevi odlično odgovaraju podacima
- Kod sustava ipak nije tako jednostavno

- Ranjivost (engl. vulnerability) je pogreška ili slabost u dizajnu sustava, implementaciji, upotrebi ili upravljanju koja se može iskoristiti za narušavanje sigurnosti sustava ili informacije.
- Prijetnja (engl. threat) je bilo koja okolnost ili događaj koji ima potencijal narušiti sigurnost sustava ili informacije

Napad je realizacija namjerne prijetnje

Rizik --> ocekivani gubitak koji nastaje kao posljedica prijetnje (kvantitavivni {1,5} kvalitativni {niski, srednji, visoki}

Zastittu nazivamo kontrola --> fizicka (kamera, alarm),
tehnicke (kriptografija, firewall, antivirus),
administrativne (doticaj s pravnim sustavom)

Kiberneticka sigurnost --> spojena na fizicki sustav (ako kontroliras nuklearnu elektranu mozes nekog unistit)

Informacijska sigurnost --> sigurnost informacije (nesto je isto ali razlicito od kiberneticke sigurnost)

Podcrucja primjene sigurnosti
Mrezna sigurnost --> sigurnost komunikacije
Racunalna sigurnost --> sigurnost rac sustava
Aplikacijska sigurnost --> sigurnost aplikacije tijekom dizajna
Upravljacka sigurnost --> ukrade podatke i nekog ozljedi
Racunarstva u oblaku --> sigurnost u cloud

Podjela sigurnosti

- Ofenzivna sigurnost – bavi se napadačkim aspektima
- Defenzivna sigurnost – bavi se obrambenim aspektima

Tehncka sigrunost --> vezana uz tehnicke aspekte
Takticka sigurnost --> vise tehnickih u jednu cijelinu
Operativnu --> vise taktickih u cijelinu
Strateska --> definira svrhu i smisao

Privatnost --> pravo na kontrolu nad vlastitim podacima
Safety --> karakteristika da nece sustav nece prouzrocit stetu (vlak kojem ne smiju otkazat kocnice)

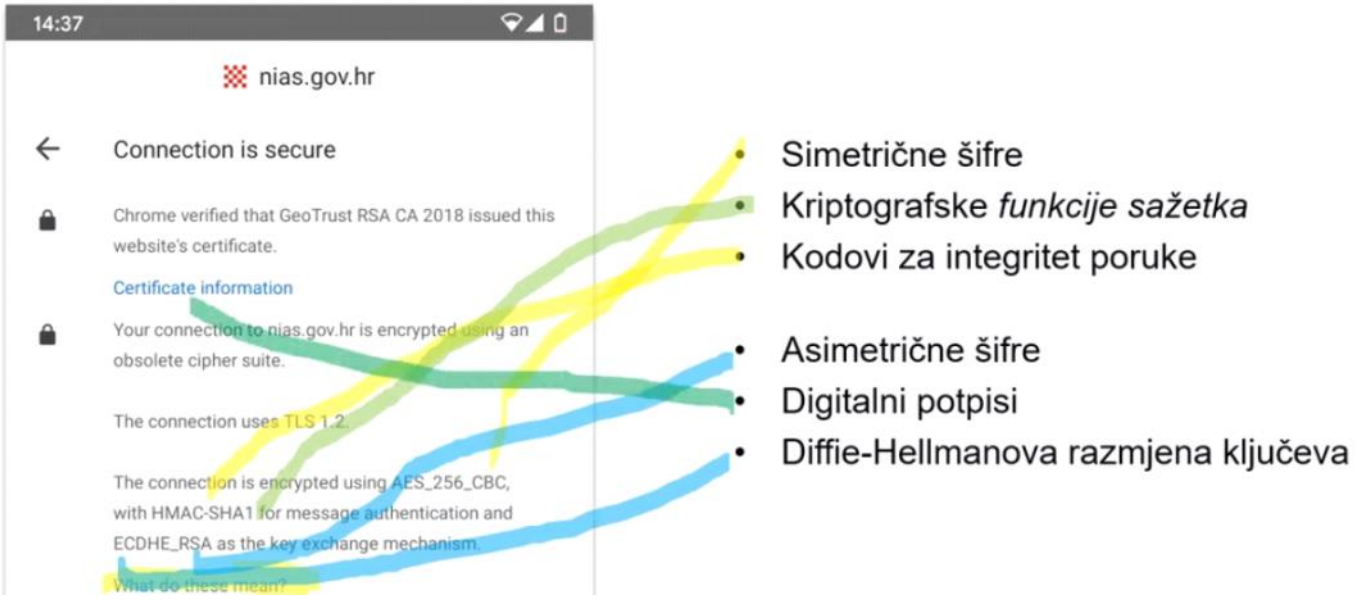
Inzinjer gradi sustav, strucnjak za sustav zeli nastetiti sustavu

Backdoor --> omogucavanje pristupa nekome tko ne bi smio imati pristup (namjerno i slucajno)
Prikriveni kanali --> kanal kojim se prenose podaci a da korisnici nisu svjesni
Sporedni kanal --> moze pristupit cachu i ukrast podatke

Povjerenje --> informirano oslanjanje na karakter, sposobnost, snagu i istinu

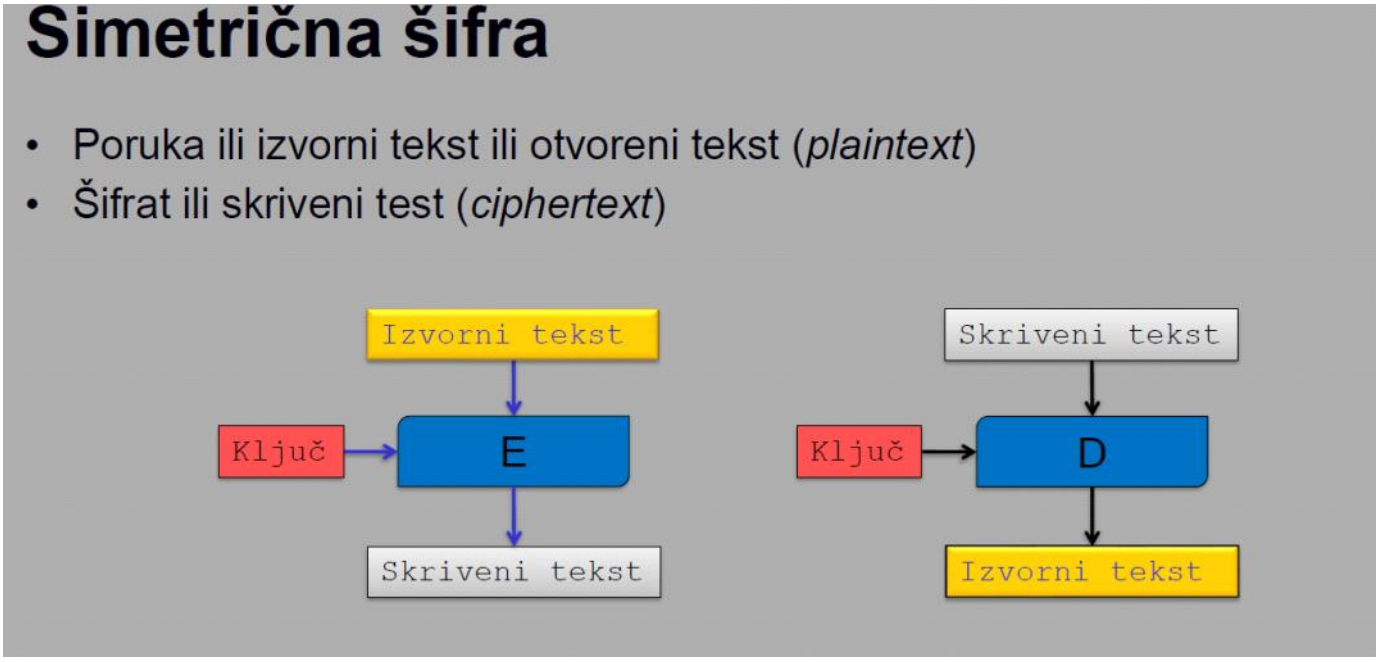
2. kritografija

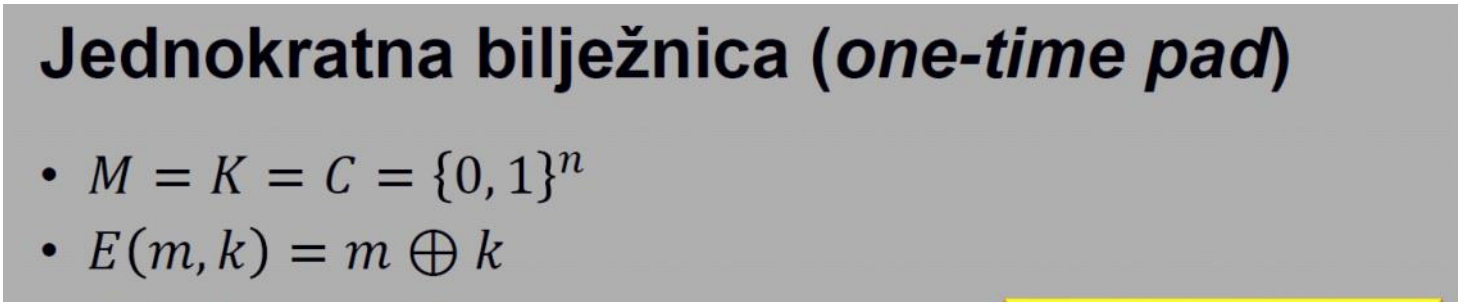
Friday, February 11, 2022 2:23 PM



Klasicne kriptografija --> cezar, supstitucijska, gruba sila

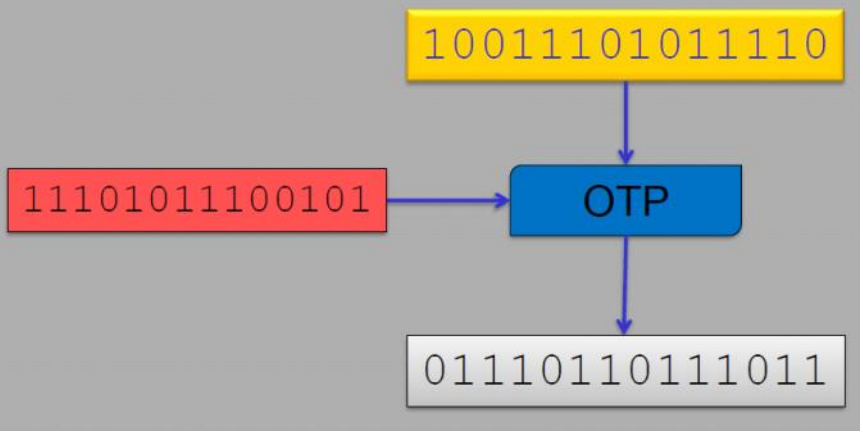
Simetricne sifre





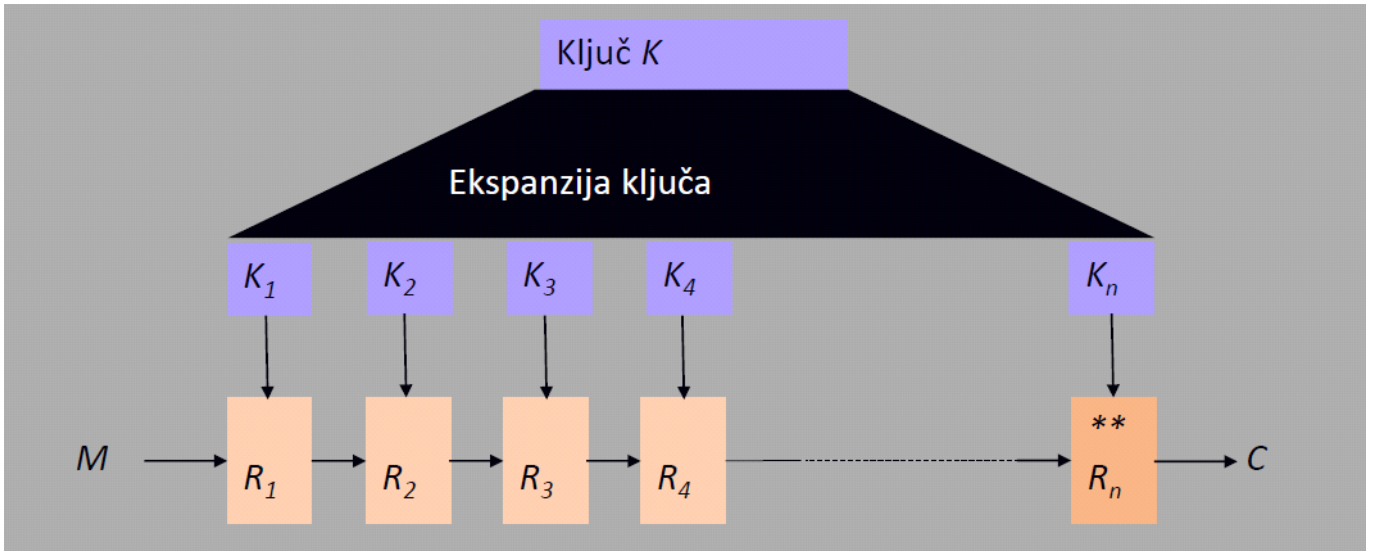
Jednokratna bilježnica (*one-time pad*)

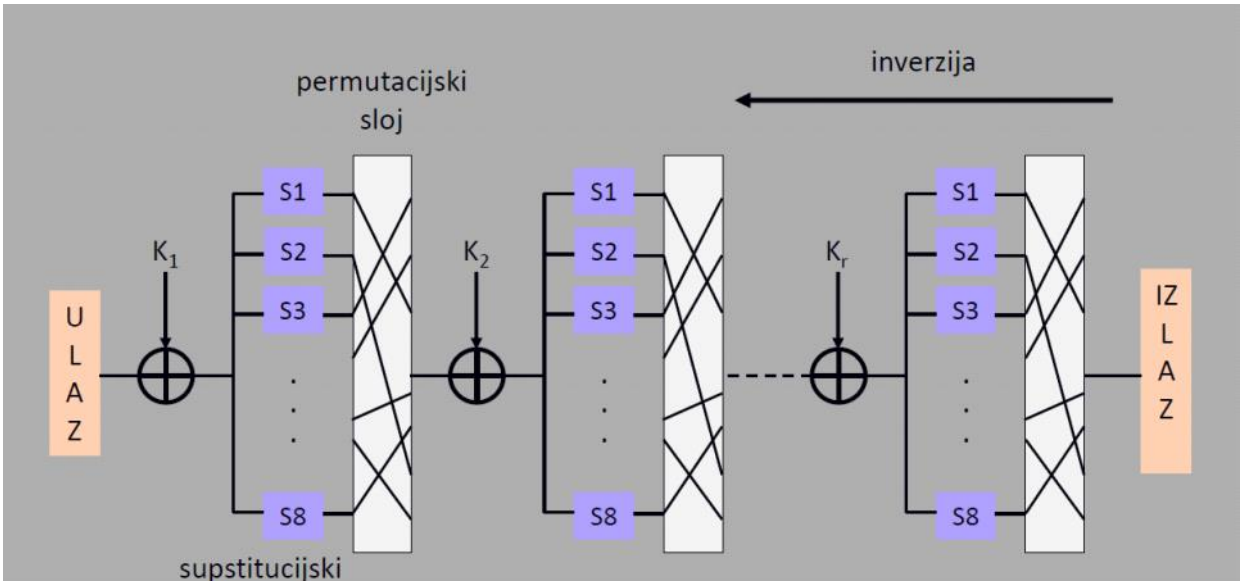
- $M = K = C = \{0,1\}^n$
- $E(m,k) = m \oplus k$
- $D(c,k) = c \oplus k$

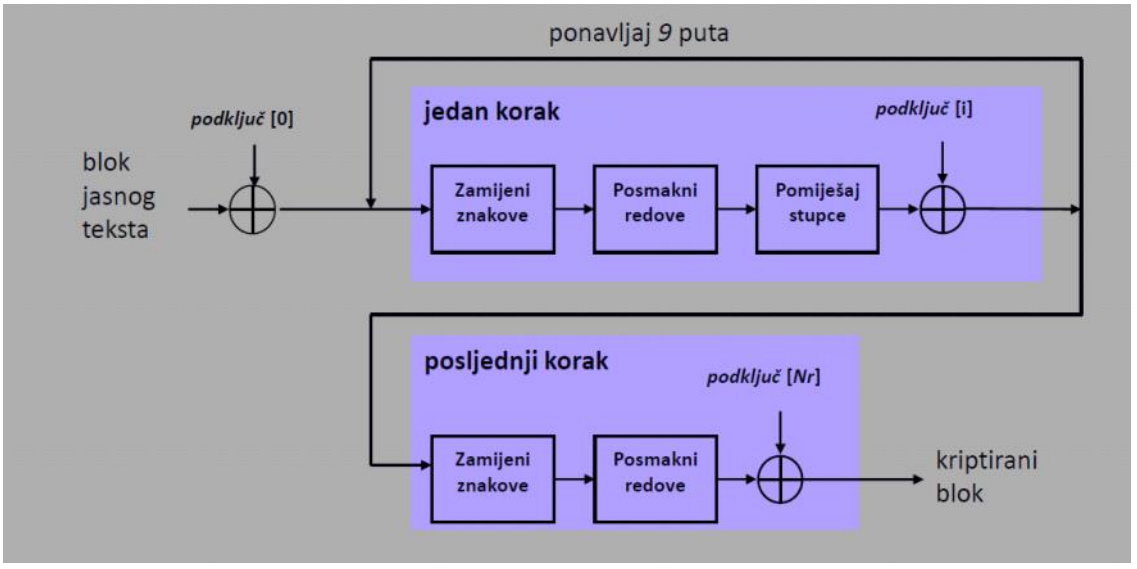


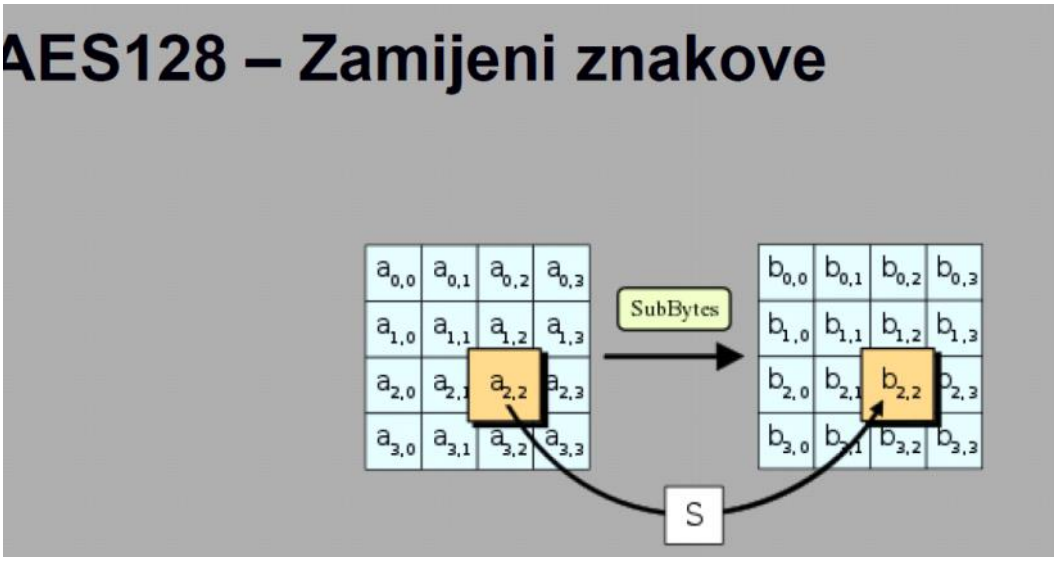
Jednokratna bilježnica – nedostatci

- Ključ mora biti jednako velik kao i poruka!
- Ključ se smije koristiti najviše jednom!
  - $c_1 = m_1 \oplus k$
  - $c_2 = m_2 \oplus k$
  - $c_1 \oplus c_2 = m_1 \oplus m_2$

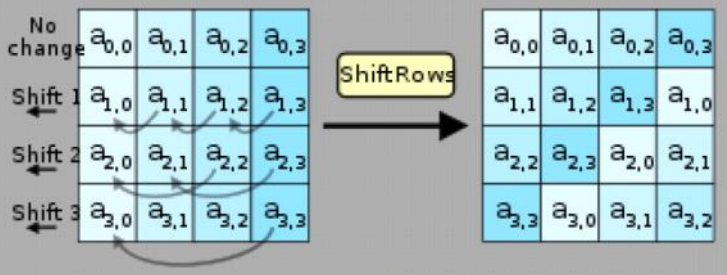



permutacijski
sloj
inverzija
S1
S2
S3
S8
K1
K2
Kr
ULAZ
IZLAZ
supstitucijski


ponavljaj 9 puta
podključ [0]
blok
jasnog
teksta
jedan korak
podključ [i]
Zamijeni
znakove
Posmakni
redove
Pomiješaj
stupce
posljednji korak
podključ [Nr]
Zamijeni
znakove
Posmakni
redove
kriptirani
blok

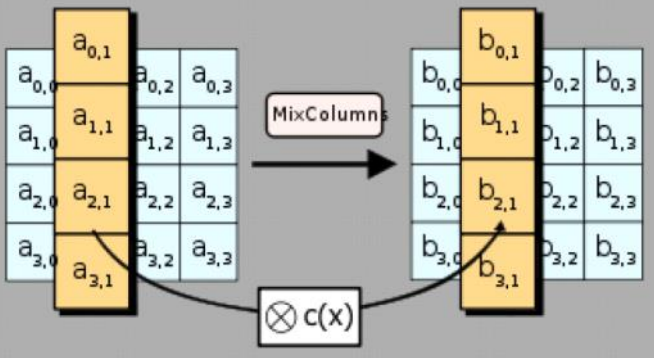

AES128 – Zamijeni znakove
SubBytes
S

AES128 – Posmakni redove



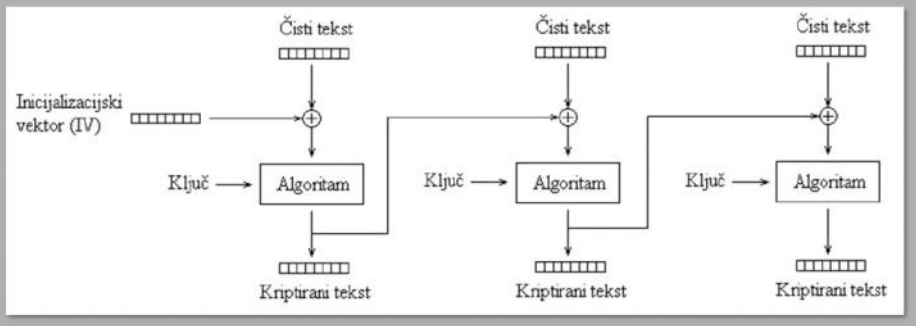
Izvor: wikipedia.org

AES128 – Pomiješaj stupce

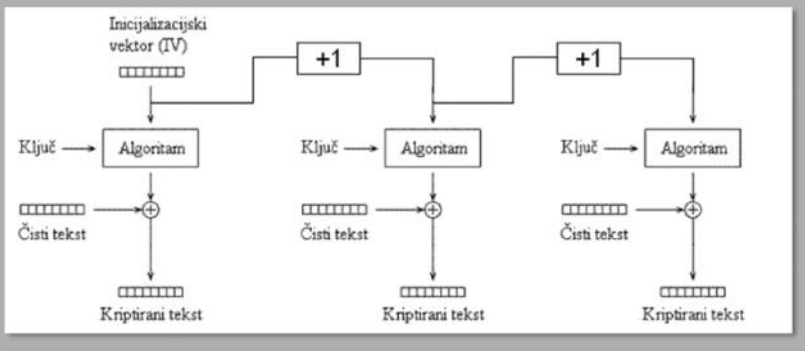


Izvor: wikipedia.org

Načini šifriranja CBC – *Cipher Block Chaining*

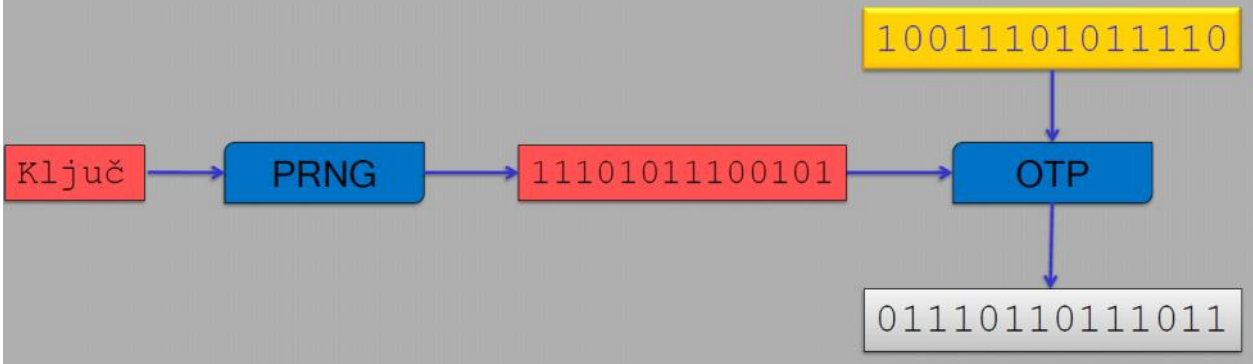


Načini šifriranja CTR – *Counter Mode*



Protočna šifra (*stream cipher*)

Generator pseudoslučajnih brojeva na temelju ključa generira niz bitova koji se XOR-a s izvornim tekstom

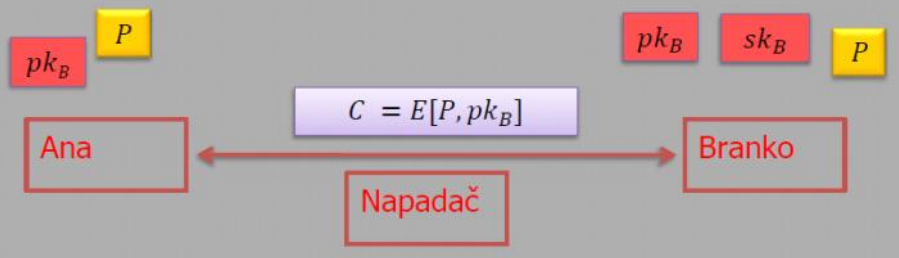


- Kriptografska funkcija sažetka H je *otporna na kolizije* ako je praktički nemoguće pronaći dvije različite poruke x i y takve da vrijedi $H(x) = H(y)$.

Hash funkcije – napad grubom silom

- Algoritam:
  1. Izaberi slučajnu poruku m
  2. Izračunaj $h = H(m)$ i zapamti par (h, m)
  3. Ako smo već vidjeli (h, m') gdje je $m' \neq m$ onda smo gotovi
  4. Skoči na korak 1.
- Iz paradoksa rođendana (*birthday paradox)* slijedi da je, u očekivanju, potrebno oko $1.2 * 2^{\frac{n}{2}}$ iteracija da se pronađe kolizija.

- Encrypt-and-MAC: $E(m, k_1), M(m, k_2)$
  - SSH, generalno nesigurna konstrukcija
- MAC-then-Encrypt: $E(m \,||M(m, k_2), k_1)$
  - Stare verzije TLS-a, 802.11i, može biti nesigurno, POODLE napad (CVE-2014-3566)
- Encrypt-then-MAC: $c = E(m, k_1), M(c, k_2)$
  - IPSec, TLS nakon verzije 1.2



Nedostaci RSA

Primjer 2

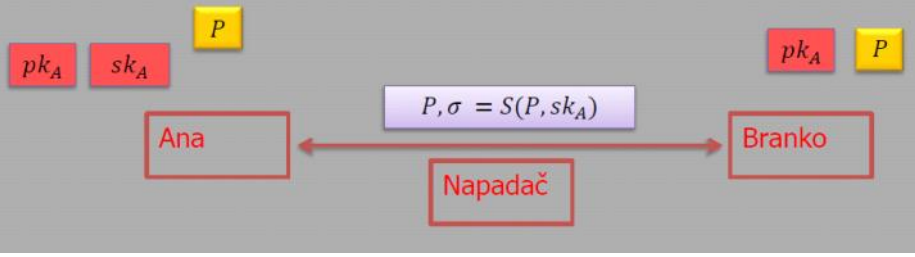
- Kriptiramo datoteku
  - Datoteka se sastoji se od n bajtova $b_1, b_2, \dots, b_n$
  - kriptiramo svaki bajt zasebno $c_k = E(b_k, pk)$
  - šaljemo $c_1, c_2, \dots, c_n$ Wi-Fi mrežom

- Napadač može za svaki mogući bajt $b = 0, 1, \dots, 255$ izračunati $c = E(b, pk)$
- Kada vidi $c_1, c_2, \dots, c_n$ lagano nalazi $b_1, b_2, \dots, b_n$

Ako je algoritam enkripcije deterministički onda sustav kriptiranja javnim ključem nikako ne može biti siguran!

Javni i tajni ključevi

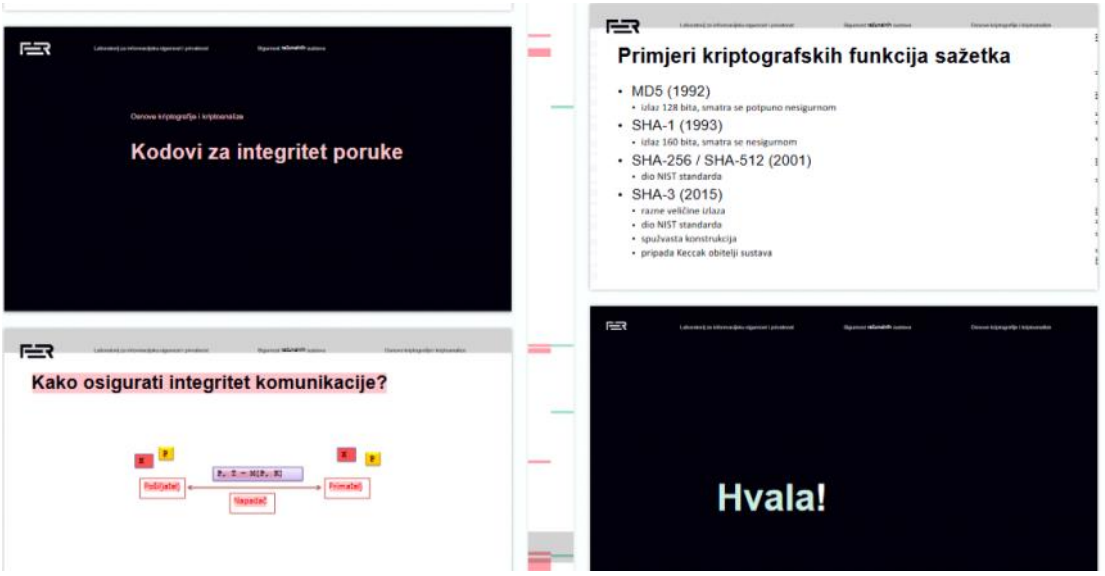
- Stara ideja: Svatko ima dva ključa
  - Javni ključ pk_A: Javno poznat (npr. telefonski imenik)
  - Privatni ključ sk_A: Poznat samo Ani
  - Ana *generira* potpis svojim privatnim ključem sk_A
  - Branko *provjerava* potpis Aninim javnim ključem pk_A



Side kanali --> sve sto nije direktno gledanje bitova (potrosnja energije, gledanje cacha, ubacivanje gresaka)

Deterministicki --> nema nista slucajno

izbaceni kodovi za integritet



Simetricna --> na temelju istog kljuca se enkriptira i dekriptira kljuc

Blok sifra --> AES

otp ne stiti integritet ka niti jedna sifra sama po sebi

Modovi --> ecb, cbc, ctr

Stream cipheri (protocne) --> Salsa20, xora izvorni tekst sa random kljucem, alternativa aesu

Hasevi --> digitalni potpisi, proof of work, provjera softwera (MD5, SHA-3)

Integritet poruka --> HMac (mac pomocu hasha)
Povjerljivost i integritet --> Encrypt then MAc, jedan paket --> AES- GCM

RSA --> kriptiranje javnim kljucem

e zovemo *javni eksponent*
d zovemo *privatni eksponent*
N zovemo *modul*
Otvoreni i skriveni tekst su brojevi u $\mathbb{Z}_N$

3. Ranjivosti

Saturday, February 12, 2022 3:49 PM

Kerckhoff pristup --> dijelit kriptografske zakljucke

SDLC (software dev life cycle) --> dizajn, implementacija, uvodenje u potrebu, upravaljanje, odrzavanje, uklananje

Rukovanje ranjivostima --> ne uvest, otkrit, ispravit, uklonit

Ranjivosti --> dizajn (dodatno stavljanje autentifikacije, autorizacije)
implementaciji (nultog dana {nitko za njih ne zna osim onog tko ih otkrio}) <-- sprecavanje (edukacija, testrainje, revizija)
<-- sprecavanje (staticka analiza {izvornog koda}
dinamicka(izvrsavanje koda,
ponasanje, razliciti ulaze)
<---sprecavanje (formalne)

OWASP TOP 10 --> zastita web aplikacija
CWE TOP 25 --> kategorije slabosti

Ranjivosti nastaju zbog --> pogreske proizvodaca, neispravno koristenje

Sprecavanje ranjivosti --> rucno pregledavanje i testiranje, koristenje alata
Otkrivanje ranjivosti --> automatizirano (trazenje svih ranjivosti, lazno pozitivni i negativni), rucno (kada se zna vec koja je ranjivost, filtriranje laznih, ogranicenja ljudi)

Implementacijske ranjivosti u upotrebi --> izrada patcheva koja to ispravlja, izdavanje upozorenja, workaroundi (gasi internet, blokiraj port)

ShellCode --> pisana u asembleru, pokrene neke stvari
CVE --> katalog ranjivosti

CVSS --> izracun ozbiljnosti ranjivosti {0-10, korak = 0.1}

3 komponentne racunanja --> bazna (nacin pristupa, kompleksnost, CIA)
--> vremenska (parametri se s vremenom mijenjaju)
--> okruzenje

Trazenje ranjivosti --> ljudi koji traze ranjivosti, reward programi

Trziste ranjivosti --> prodaja na crnom trzistu, sigurnosnim tvrtkama

4. Prijetnje i izvori prijetnji

Saturday, February 12, 2022 6:10 PM

Primjeri prijetnji --> pogadanje kriptografskog kljuca,
overflow servera,
lazni email,
DDoS napad (ogranicen router),
napjanje prestane raditi,
ucjenjivacki zlocudni kod (ransomware)

Agent prijetnje --> subjekt koji prevodi prijetnju
Izvor prijetnje --> potaknuo je prijetnju
Napad --> kombinacija izvora , namjere (prijetnje) i posljedice

Podjela izvora prijetnji --> a) prirodni b) ljudski

a) Prirodni izvor prijetnji --> pozar, poplava, potres
b) Namjerni ljudski izvor
--> vanjski (ovisi o znanju i ovlasti izvoru prijetnje), unutarnji (covjek koji ode iz firme i zna sve sifre)

Namjerni vanjski izvori prijetnji karakteristike --> raspolozivi resursi
--> motivi i ciljevi
--> ustrajnost
--> ljudski resuri i sposobnosti

Izvori prijetnji

Napredne ustrajne prijetnje APT (planiranje i provodenje dugotrajno)--> hrpu para, ljudi, cilj odreden drzavnim interesom --> primjer --> Stuxnet (napad na Iransku elektranu), SolarWinds (napad na niz drugih tvrtki) --> Cozzy bear
Kiberneticki kriminalci (motiv zarada, ustrajnost srednja) --> vrste (tradicionalne, omogucio kiberneticki prostor)
--> Zarada (krada, prodaja, ucjenjivanje, prijevare) --> ochko123, kobobface gang
Haktivisti --> nisu uporni, nemaju kompentencija i resursa, trude se biti vidljivi

Pojedinacni napadaci
Gray, Black White Hacks --> velike vjestine
Script kiddies --> ne znaju nista, znatizalja ili slava

Automatizirane probe (vise spam nego ozbiljno, laka zastita)

a) Skener koji trazi ranjive servise
b) Crvi koji mogu zaraziti druga racunala

Cyber Kil chain --> istrazi, naouruzaj, isporci, iskoristi, instaliraj, uspostavi, djeluj
MITRE ATT&CK --> taktika { cilj}, tehnika {kako} , procedura {tehnika provodenja}
Drustveni injzinering
Korisnik je najslabiji, instalacija zlocudnog koda {phising, spear phising}

Atribucija --> tko stoji iza napada <-- prikirvanje { vpn, tor}
Model prijetnje --> **koga** zlimo sprijeciti da ucini **sto**

5 zlocudni kod

Wednesday, February 16, 2022 11:35 PM

(def) **Zlocudni kod** --> Zlocudna funkcionalnost --> sklopovlje, firemware koja je ubacena u sustav radi sttetnih ciljeva

Klasifikacija zlocudnog koda --> nacin sirenja (cd, usb)
--> nacin pokretanja (samostalno, preko klijenta)
--> monolitni
--> platforma (os, aplikacija)
--> perzistentni i neperzistentni
--> prikrivanje (dio aplikacije --> trojan, dio os-a --> rootkit)
--> funkcionalnost (backdoor, rat, cryptominer, dropper)

Virus --> ubaci se u izvrsni kod (pokrece se njihovim pokretanjem)
Crvi --> siri se putem mreze
Downloader --> zlocudni kod koji skida i instalira neki drugi zlocudni kod
Dropper --> zlocudni kod koji sadrzi drugi zlocudni kod te ga postavlja na kompromitirano racunalo
Logicka bomba --> kada je uvjet ispunjen, desi se nesto
Spyware --> izvlaci podatke
Alat za udaljen pristup --> nije nuzno zlocudni kod
Trojan --> pretvara se da je neka korisna funkcija
Ucjenjivacki kod --> ucjenjivanje vlasnika, najcesce sifriranje podataka diska

Forma --> (exe, dll), (linux --> elf) , powershelll, Ms Office (makroi u visual basicu)
PDF --> sadrzi js, ranjivost u pdf readeru,
Mobilna --> trojan aplikacija,
Web --> js

C&C server --> kod se javlja negdje na Internet, napadac moze upravljati, lako otkriti ali tesko napadaca

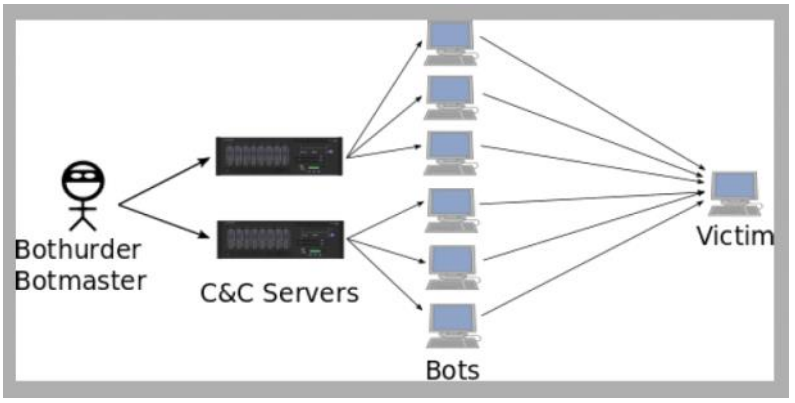
Zastita --> odgovorno ponasanje, AV (anti virusna podrska) , dinamicka analiza maila, blokiranje C&C posluzitelja

Indikator kompromitacije (IOC) <-- podaci koji omogucavaju detekciju zlocudnog koda --> (podaci u registryju, IP adrese zlocudnog koda, hash file-a) <-- brz nacin utvrdivanja je li nesto zarazeno

Reverzno inzinjerstvo --> stavljanje u sandbox i pracenje rezultata, analiza u debuggeru, staticka analiza (Ghidra) --> decompaileri

Virus total --> detekcija zlocudnog koda

Dinamicka analiza --> zasticena okolina, specificni os
Botnet --> skup zarazenih pc-a kojima upravlja botmaster, izvrsava neki kod



Http, P2P protokoli

Primjeri : Mariposa, Emotet

Upotrebe --> overflow zrtava, spam, skupljanje lokalnih podataka

Razvoj zlocudnog koda --> od pocetka(APT- ovi)
--> kit za izradu

NCO --> prodaje spijunsku opremu

6. kontrola pristupa

Thursday, February 17, 2022 12:44 AM

Autentifikacija --> provjera identitena
Autorizacija --> moze li subjekt obaviti odredenu operaciju

Metode autentifikacija --> necemu sto znamo (pass), sto jesmo (fingerprint) , ono sto imamo (stick)

1Fa--> najcesca, nedovoljna
2FA --> sve vise se prelaze, visoka zastita
MFA --> rijetko koristena

Primjeri authentifikacije --> pass, fraze, otp (one time pass), smart card, biometrija

Pass --> ono sto znas, niz znakova, najstariji mehanizam

Provjera --> upisi username, dostavi u bazu, provjeri
Ranjivosti --> presretanje, los odabir znakova passworda (brute force, dictioanry), iste lozinke, krada, obnavljanje

Zastita --> sto vise random, ne dijeliti, zastititi prijenos

Sigurna pohrana --> lozinka + seed koji stvara sazetak

Sprecavanje online pogadanja --> vrijeme cekanja, blokiranje racuna

Jednokratne (OTP) --> 4 i vise znamenke po nekom algoritmu (standardi TOTP, HOTP)

Implementacije --> tokeni za internet, mobilnne, program na pc-u

Dijeljene tajne --> i jeda i druga strana dokazuju poznavanje
Fraze --> dulje su i nije na njih vezan username

Lozinke i 2FA --> dodaje se 2fa koja se salje nezavisnim kanalom

Pametna katrica --> ono sto imamo (kartica) i ono sto znamo (pin)
--> privatni kljuc na kartici, javni kljuc poznat, kartica potpisuje podatke

Biometriske --> ne moze se mijenjati

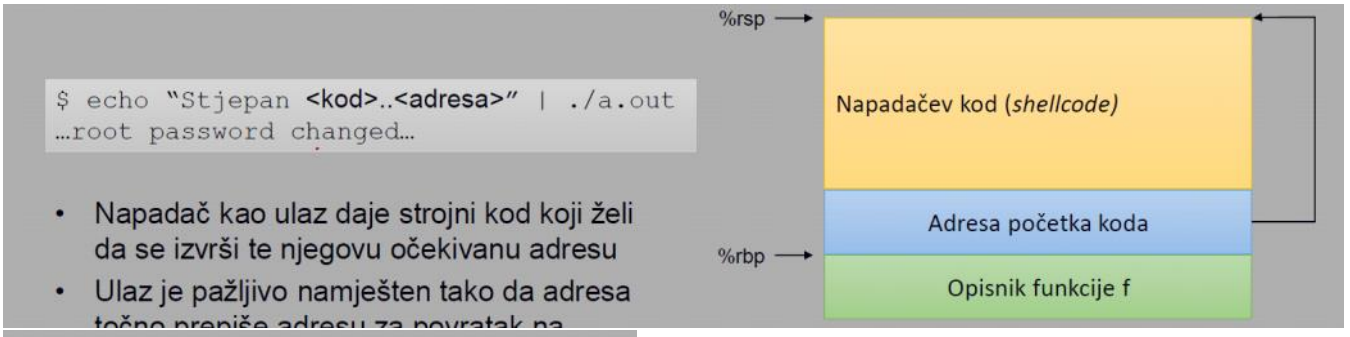
Autorizacija bazirana na dozvolama --> sta ko smije radit (generalno se se odbija)

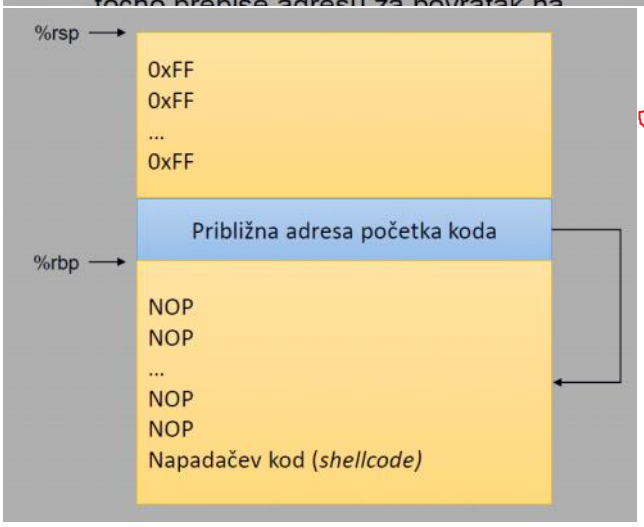
Autorizacija bazirana na ulogama --> prava se grupiraju u uloge a uloge na subjekte

Ranjivosti i napadi

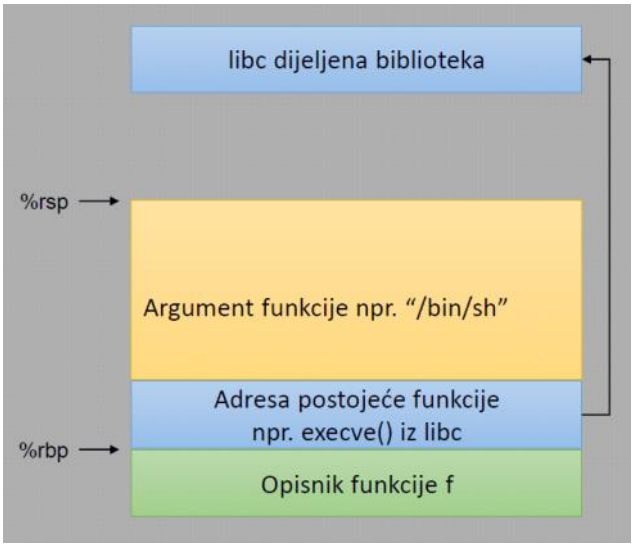
Saturday, February 19, 2022 2:35 PM

Provjera sintakse --> ispravne velicine (buffer overflow), ispravno formatiran (injection napad)
Provjera semantike --> ima li smisla (HeartBeat <-- dohvat sadrzaja zaporke, kljuceva (OpenSSL))





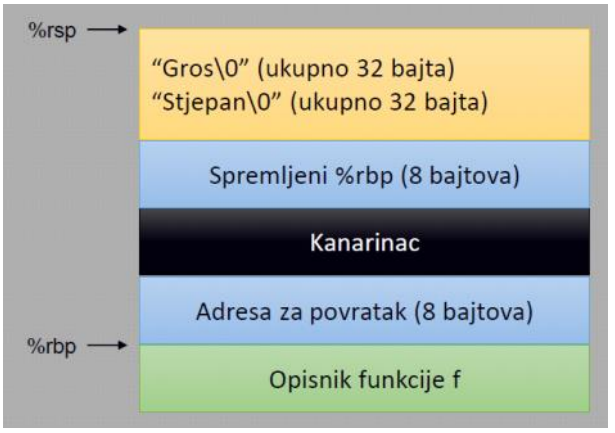
Buffer overflow --> napad (pogadanje adresa)
obrana --> write xor execute, non sled --> instrukcije koje nista ne rade,



Zaobilazenje NX bita
return to libc napad

obrana --> randomizacija memorijskog prostora

Obrana --> stavi kanarinca da se zastiti adresa za povratak



Ostale ranjivosti --> heap overflow, integer overflow, string format

Obicno programiranje --> razumne okolnosti, razumni ulazi za razumne izlaze

Defenzivno programiranje --> nerazumne okolnosti, nerazumni ulazi, ne smije se ponasati nerazumno

Potreban je paranoican pristup prilikom --> interakcije s korisnikom, formiranja pretpostavki o okolnostima

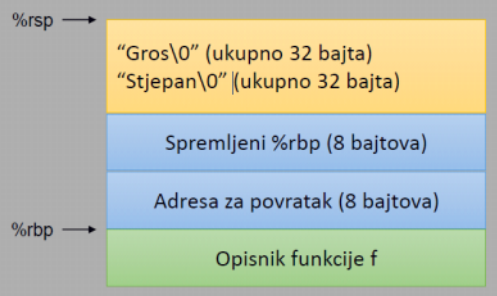
Buffer overflow napadi --> morris crv, code red crv

Normalno izvršavanje

```c
#include <stdio.h>

int main() {
  char ime[31 + 1], prezime[31 + 1];
  scanf("%s %s", ime, prezime);
  printf("%s, %s", prezime, ime);
  return 0;
}
```

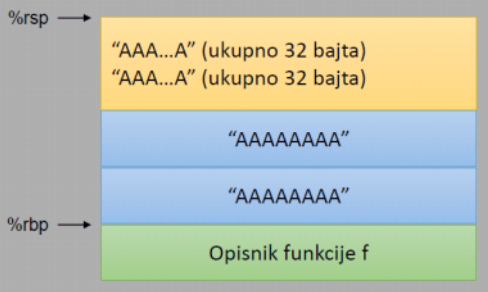
```
$ echo "Stjepan Gros" | ./a.out
Stjepan Gros
```



Prelijevanje međuspremnika

```
$ echo "Stjepan A<80 puta>" | ./a.out
Segmentation fault (core dumped)
```

- Prepisali smo adresu za povratak na stogu!
- Nakon instrukcije `ret` program je pokušao nastaviti izvršavanje na adresi koja odgovara nizu znakova „AAAAAAAA" (0x4141414141414141)!



obrana --> ne koristiti c

Sigurnost prog. podrske

Saturday, February 19, 2022 3:32 PM

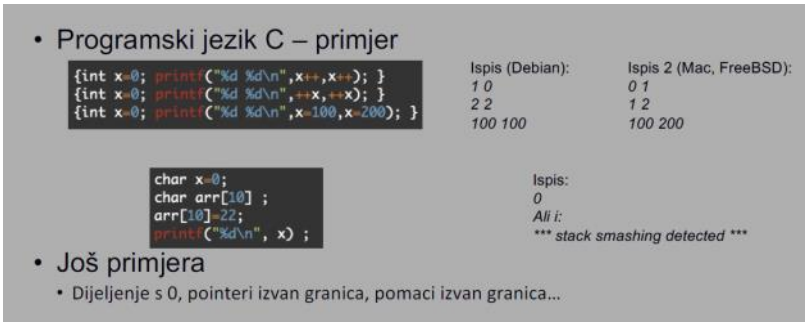
Taksonomija pogreska --> namjerne(zlonamjerne i nezlonamjerne) , nenamjerne (granicni uvjeti, logicke pogreske, provjera valjanosti)

Nezlonamjerne pogreske --> buffer overflow , nepotpuna provjera ulaznih parametara, sinkronizacija provjere i pristupa

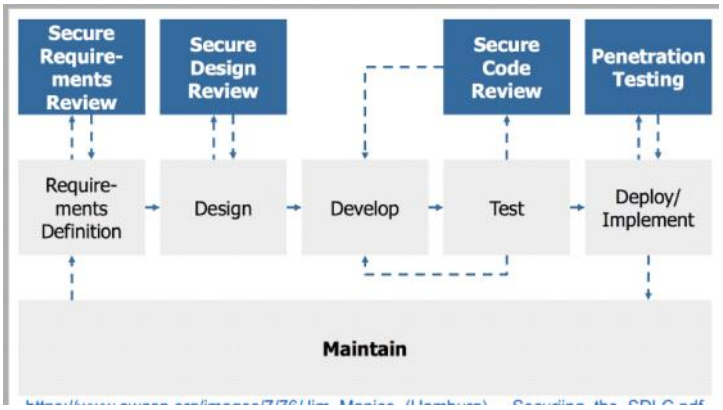
Staticka analiza --> izvroni kod
Dinamcika analiza --> binarni kod

Strongly typed --> pazi umjesto nas

Slabo tipizirani --> C, C++
Djelomicno tipizirani --> Python, Ruby
Strogo tipizirani --> Java, C#, Rust (pazi o tipovima, baca gresku prilikom izvodenja/prevoditelja



Zivotni ciklus zahtijeva



Koraci prije implementacije

--> sto osigurati (osnovni i dodatni sigurnostni zahtijevi)
--> profil napadaca (protiv koga se borimo)
--> identifikacija entiteta (sto treba stititi)
--> postavljanje arhitekture (osiguranje sigurnosnih zahtijeva)

Smjernice za siguran dizajn

Minimizacija prostora za napad--> funkcionalnosti otvaraju propuste, umetanje koda

Sigurne pocetne postavke --> generirane lozinke kod registracije (uvesti velika mala slova, duljina 8)

Najmanja prava --> wordpress (sto manje da ne unisiti sve)

Princip obrane u dubinu --> dvorac ima vise barijera, vise neovisnih mehanizama koji stite istu stvar

Sigurno ispadanje --> elektronska brava (sto kada nestane struje?)

Ne vjerujte vanjskim uslugama --> podaci se salju u vanjski CRM koji ima sigurnsne ranjivost

Razdvajanje zaduzenja --> svako ima svoje zaduzenje

Izbjegavanje sigurnosti prikrivanjem --> bolje da je open source da sto vise ljudi to validira

Jednostavna sigurnost --> ne dodavat slozenost, sve radit na najjednostavniji moguci nacin

Ispravne sigurnosne zakrpe --> ne zuriti sa popravkom

OS

Operacijski sustav --> skup programa koji povezuju sve dijelove racunala

Razdvajanje

dijeljenje --> procesi se ne vide, pr. --> public/private, pristup na vise razina

Ovlasti na linuxu --> u {owner}, g {group}, o,a {other, everyone} <--- akcije --> r {citanje} w {write} x {pokretanje} - {bez ovlasti}

prvi znak {d - direktorij, l- link na datoteku} , prva 3 znaka user, druga 3 group, 3 other

x da mos uc, r izlistat

cmhod 655 file.txt
chown user:group file.txt --> mijenja vlasnika

Sandboxing --> memorija (user space(korisnicki programi, sve sto nije kernel), kernel space (jezgra sustava)), izolacija sumnjivih programa, standard na Mac i iOS, ostalo docker kontenjeri

Apple --> dev mora napisat sta njihova aplikacija koristi
Namespace u linuxu --> sta tko kome moze pristupit, seccomp(ne moze pozivati sistemske fje osim osnovnih), firejail, docker
Windows --> user access control, win10 prava izolacija i brisanje nakon koristenja

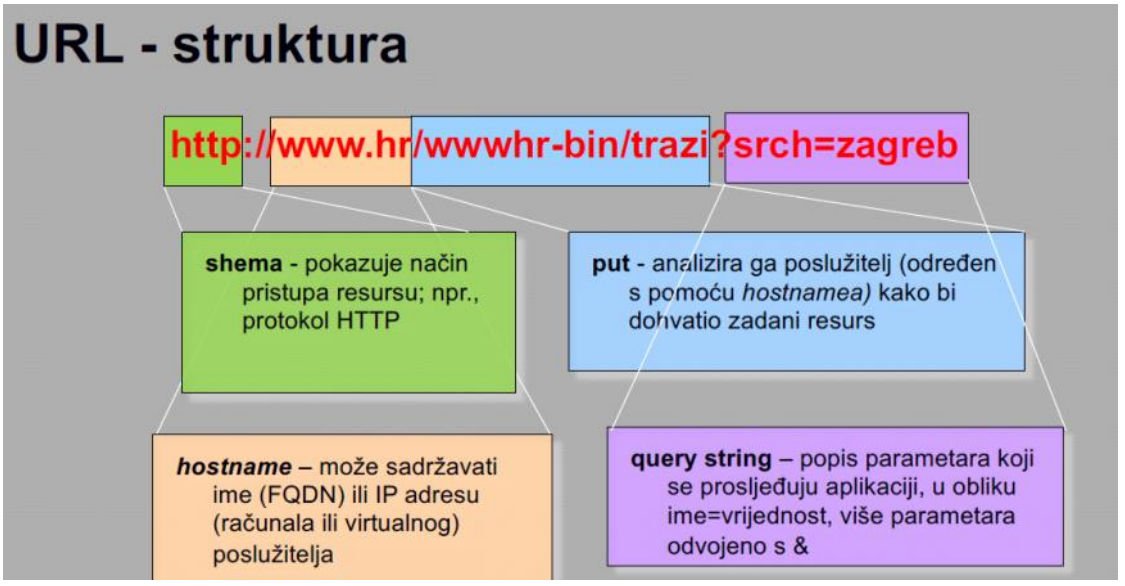
Sifriranje boot diska --> prije boota se mora upisat sifra da se otkljuca disk
BitLocker --> nacini rada 1.Transparent operation mode --> TPM- pohrnanjen u sklopovlju, 2. lozinka, 3.usb key mode
Linux --> dm-crypt i luks

Sigurnost web aplikacija

Saturday, February 19, 2022 5:38 PM

Posljedice na klijentu --> botnet, keyloggeri, krada podataka
Posljedice na serveru --> ukradeni brojevi kreditnih kartica, podataka (rupe --> XSS, SQL injection)

HTTP
Rjesenja stateless stanja -->
--> sessions, obrazci, parametri kao dio URl-a
--> nije sifrirana



Ranjivosti web aplikacija

A1 Injection --> ubacivanje SQL naredbi, promjena baze podataka

1. (taut)izraz koji je u svakom slucaju istina
2. (ilegal)doznat strukturu tablica i baze
3. (injekcija)slijepo pikamo naredbe
4. (upit)union --> upit koji povezuje vise naredbi

```
//moguci nacin...
$query  = "SELECT first_name, last_name FROM users WHERE user_id =
                                    'bilo_sto' OR '1'='1';";

//dakle upisujemo:
                                     bilo_sto' OR '1'='1

//ili samo:
SELECT first_name, last_name FROM users WHERE user_id = '1' ORDER BY 1#';
SELECT first_name, last_name FROM users WHERE user_id = '1' ORDER BY 2#';
SELECT first_name, last_name FROM users WHERE user_id = '1' ORDER BY 3#';

SELECT first_name, last_name FROM users WHERE user_id = '' LIKE '%';
```

preporuke --> paziti na or, Or, oR, OR, ne prikazat greske, koristit framework koji o tom vodi racuna, pohranjene procedure

A2 Losa autentifikacija

Cilj --> pogodit ime i pass od usera ili ukrat session id

User credentials

Brute force(alati) , lozinke iz rjecnika (slabe lozinke), vertikalni napadi (cijeli dict za jednog usera), horizontalni napadi (pogadanje imena usera)

Zastita --> captcha, login attpemt, filtirranje adresa, poruke pogreske ne otkrivati, token umjesto cookie-a, httpOnly (js ukrade cookie kroz browser), trajanje cookie-a

Lose poruke o greskama --> sto manje informacija

Dupliciranje lozinki --> iste lozinke na vise mjesta

ID

Nastajanje
kada se korisnik prijavi generira se, server ga salje korisniku, korisnik salje serveru

Alternativa --> token

Sigurni cookie --> HTTPOnly - sprecava se krada putem XSS-a
--> Expires

Izbjegavanje --> viseautentifikacija , novi session id, cuvanje lozinki, minimalne ovlasti

A3 Nesigurna pohrana osjetljivih podataka

ucinci --> pristup privatnim podacima, sramocenje tvrtke, nezadovoljstvo korisnika
problemi --> **slabi kljuc, zastarjeli algoritam sifriranja,** pohrana i prijenos plain text
rjesenja --> **verifikacija arhitektura, pratiti ranjivosti za kriptoalgoritme**, zastita (sifriranje podataka, baze)

A4 XEE --> Xml injection, aplikacije koje parsiraju xml

rjesenje --> validacija xml-a

A5 Losa kontrola pristupa --> napadac pokrece funkcionalnosti i usluge na koje nema pravo

npr /user/getAccs promijeni u /admin/getAccs i ima pristup
?acct = 6065 u 6066 i ima podatke tog korisnika

izbjegavanje --> verificirati arhitekturu(na svakom sloju), implementaciju (autorizacija, url zasticen)
, eliminacija referenci(?file=1 --> Report1.xls)

A6 Lose sigurnosne postavke --> source mora biti javan, paziti na libraryije, dozvole nad datotekama

plugin za wordpress ima ranjivosti, .htaccess daje pregled direktroija

izbjegavanje --> **pentestovi, audit, .htaccess datoteka**, skrivena pohrana web aplikacije

.htaccess --> konfiugracijska datoteka, filtirranje ip adresa, listanje direktroija, filtriranje datoteka, zabrana pristupa direktoriju i kritcnim datotekama

A7 XSS --> ubaci se js u browser koji ukrade cookie

Same origin policy --> ako fer da cookie, samo on smije dobit nazad taj cookie

problem --> sjediste s vise poddomena

reflektirani --> napadac salje zrtvi link na koji ona klikne, salje se na server, on vrati, cookie se salje napadacu
pohranjeni --> stavio u bazu skriptu, korisnik ude i ukrade mu se cookie (kao unos forme)

obrana --> **post umjesto get-a, httpOnly**, kodirati i izbjeci <>{}

A8 Nesgiurna deserializacija --> web vjeruje serializiranom objektu i ne provjerava ga

rjesenje --> ne vjerovati svemu od korisnika, potpisivati

A9 Ranjive komponente --> apache, nodejs
rjesenje --> pratit patcheve, noovotkrivene ranjivosti, koristene komponente, sigurnosne politike i omotace

A10 Nedovoljan nadzor --> upisat u logove propale pokusaje, pametan nadzor

rjesenje --> log monitoring, app firewall

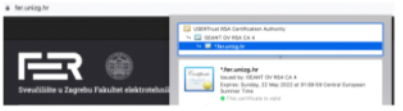
Laboratorij za informacijsku sigurnost i privatnost Sigurnost računalnih sustava Sigurnost web aplikacija

Malo o protokolu HTTP

- *stateless* - ne održava stanje
  - računala ne moraju održavati informacije o korisnicima
  - problem: web-aplikacija mora održavati takve podatke
- rješenja:
  - postavljanje i slanje cookieja
  - korisničke sjednice (*sessions*)
  - skrivene varijable (unutar obrazaca)
  - parametri kao dio URL-a
    - /index.php?session_id=some_unique_session_code).
- komunikacija nije šifrirana

URL, "lokot" i sigurnost

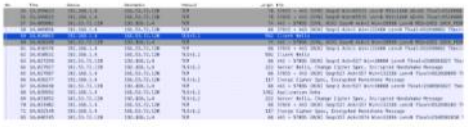
- Lokot u pregledniku
  - Autentifikacija poslužitelja – sve treba biti zaključano/zeleno
    - Kada koristimo HTTPS, svaki poslužitelj weba treba imati važeći certifikat
    - Preglednik provjerava taj certifikat i zaključava"zazeleni" lokot ako je sve u redu
      - Izdavatelj certifikata je na popisu „trusted" CA
      - Certifikat je važeći
      - Certifikat nije na CRL!



Što u tom slučaju vidi preglednik?

- Certifikat je provjeren i u redu

Što se ipak vidi u nižim slojevima?



- Zašto je ovo važno?
  - Elementi / tehnike za autentifikaciju (npr. Tokeni, kolačići sa identifikatorima sjednice) su šifrirani
  - Čitava komunikacija (podaci) su šifrirani – vidi se IP adresa

Laboratorij za informacijsku sigurnost i privatnost Sigurnost računalnih sustava Sigurnost web aplikacija

"*IDN Homographic Attack*"

- IDN - *internationalized domain name*
- URL može sadržavati unicode znakove
  - Podrška za različita pisma (npr. ćirilica)
  - Problem: ćirilično 'a' (U+0430) izgleda slično latiničnom 'a' (U+0061)
- Važno: certifikat / lokot su „zeleni" – (i trebaju biti)
  - Korisno za phishing napade!

Mrezna sigurnost 1

Saturday, February 19, 2022 11:59 PM

Presretanje, prisluskivanje--> preuzima se informacija izmedu tocaka a i b

Prekidanje --> onemogucimo komunikaciju

Promjena --> promjena, unistenje informacije

Umetanje --> ubaci zlonamjerne informacije
Ponavljanje --> ubacivanje prethodne informacije

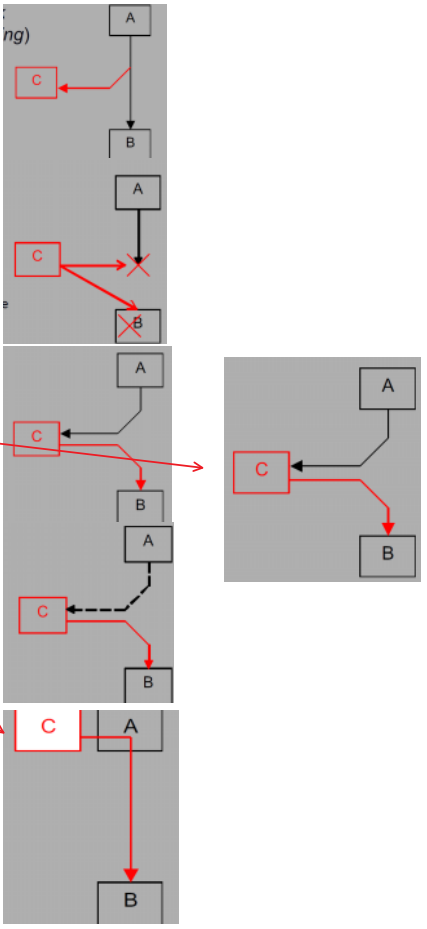
Lazno predstavljanje --> napad se predstavlja kao korisnik

Man in miidle MITM --> sve prethodno navedeno

Ranjivosti --> fizicka, protokol, implementacija, konfiguracija

Ranjivosti protokola

ARP, Ethernet, IP, TCP, UDP --> ne jamci se osiguranje sigurnostnih zahtjeva

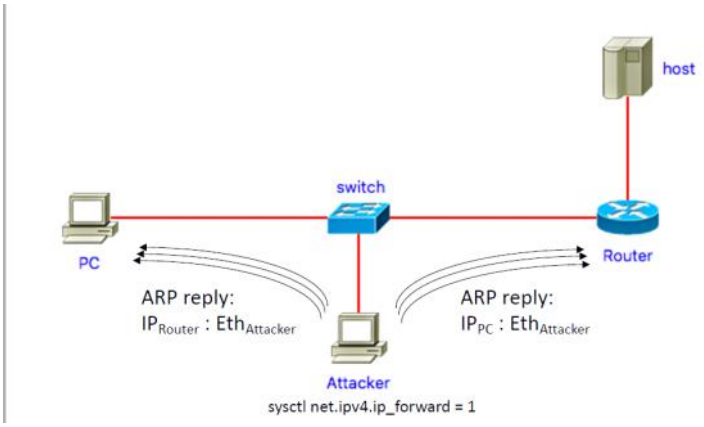


ARP

- 32 bit IP u 48 Ethernet(MAC) adrese

- A salje ARP svima, B odgovara porukom ARP odziv

napad --> nema autentifikaciju, lazno preslikavanje, promjena, ometanje, prisluskivanje prometa



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

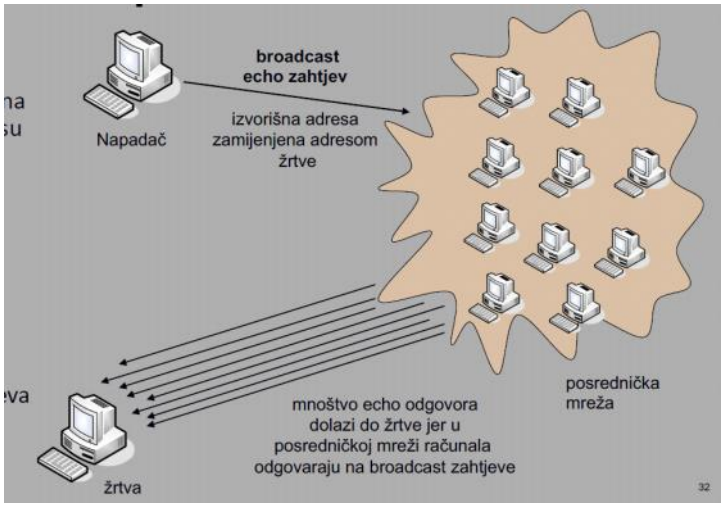
IP

podaci nisu zasticeni --> izmjena polja, laziranje source IP adresa
Spoofing --> lazna adresa posiljatelja (DDos)
zastita --> **filtriranje neispranih izvorisnih** adresa

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

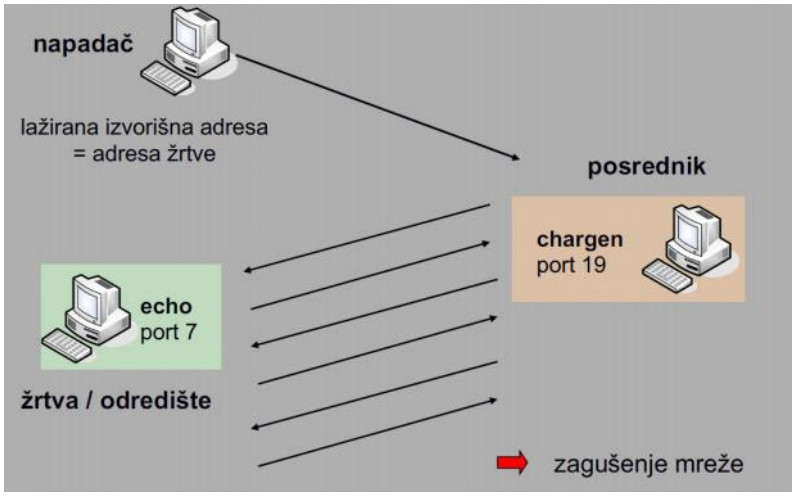
- nuzan za IPv6

Poboljsanje sigurnosti na mreznom sloju

--> IP nema zastite
-->opcija --> kriptiranje i zastita (VPN)

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)
udp amlification i refelction --> lazna izvorna adresa, odziv sadrzi vise podataka od upita
DNS 54 puta
NTP 556 puta
SNMP 650 puta

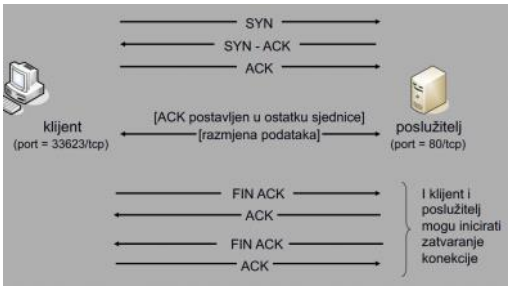


TCP

- spojni transportni protokol
- pouzdan

- SYN dogovaranje početnih brojeva pri uspostavi veze
- FIN završeno slanje podataka
- ACK broj potvrde je postavljen

SEQ redni broj prvog okteta u korisnickim podacima
ACK potvrduje da su svi podaci do tog oketa primljeni
URG urgent pointer
PSH predavanje podataka aplikaciji
RST resetira vezu



- pouzdan - potvrda, nema dupliciranja, slaze pakete

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

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

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

Zaštita od RST i FIN napada

- TCP MD5/AO
- (Ručno) ograničenje maksimalne veličine prozora
  - Napadač u tom slučaju mora napraviti više pokušaja
- Ograničenje slijednog broja u RST segmentima
  - Dodatno slanje ACK segmenta
- Druga rješenja koja modificiraju ponašanje TCP-a

ICMP napadi na protokol TCP

- ICMP je mrežni protokol
  - Na temelju podataka iz višeg sloja se obavlja demultipleksiranje
    - Zaglavlje mrežnog sloja i prvih 64 bita višeg sloja [RFC793]
    - Što više podataka, ali manje od 576 okteta [RFC1812]
- Konkretni napadi
  - ICMP poruke o greškama uzrokuju prekid veze
  - Port ili protokol nedostižni, fragmentacija potrebna a DF bit postavljen
  - ICMP poruka o zakrčenju (ICMP Source Quench)
- Zaštita prijenosnog sloja

Sigurnosna rješenja

- TCP-MD5 (RFC2385) / TCP-AO (RFC5925)
  - Uglavnom za zaštitu protokola BGP
    - BGP koristi i TTL zaštitu
  - Valjani RST, kada nema druge strane, će biti ignoriran
  - Problematično zbog dijeljene tajne, kripto-algoritmi usporavaju poslužitelje/usmjernike,
  - TCP MD5 zamijenjen s TCP AO jer koristi problematičan algoritam, nema zaštite od ponavljanja, ne podržava IPv6, zamjena dijeljene tajne je problematična (nema načina signalizacije promjene dijeljene tajne)
- IPsec – lako potpuno, nije skalabilno rješenje
- TLS

Mrezna sigurnost 2

Monday, February 21, 2022 9:47 PM

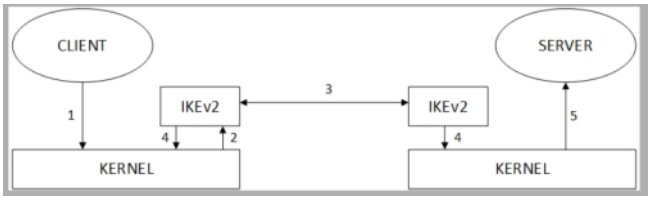
VPN --> privatna mreza nad javnom inrastrukturom

Rjesenja za VPN --> OpenVPN, WireGuard, IPSec

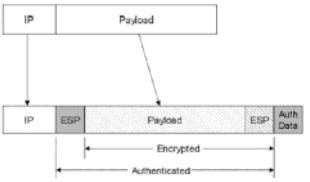
PPTP --> lako saznati podatke, nije siguran

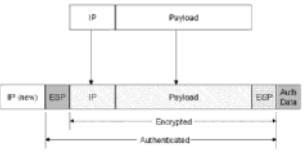
Vrste VPN-a --> Site to Site (private i zasticene nad routerima)
Remote access (uredaj i router)

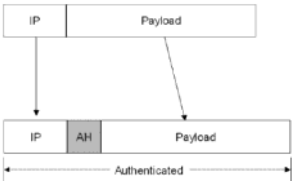
IPsec --> protokol za krajnje tocke i razmjenu informacija (spaja 2 ili vise mreza, spaja 2 racunala)
Osnove arhitekture
tunelski ili prijenosni nacin
autentifikacija kroz certifikat, dijeljene tajne ili eap
ponasanje kranjih tocaka definirano bazama SPD i SAD
SPD --> sto treba zastititi
SAD --> kako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

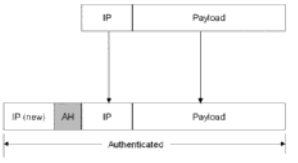


primjer rada IKE i ESP/AH









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

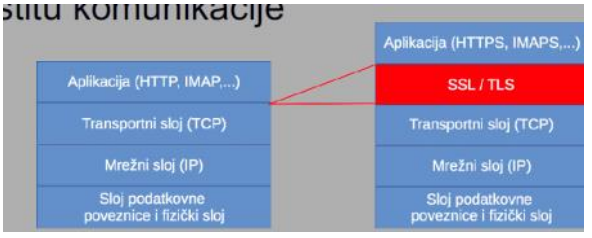
Digitalni Certifikati

Simetricne sifre --> jedan tajni kljuc
Asimetricna sifra --> javan dostupan svima i privatan samo vlasniku

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

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



TLS

- zastita komunikacije

Aplikacije koje koriste TLS --> https, smtp, pop3, imap4

HTTP +TLS --> klijent inicira handshake preko protokola record
na portu 443

Osnovna funckionalnost

-potdvrda identitea servera i i zastita tajnosti i autenticnosti koumunikacije CAuth

Presretanje - vlastiti CA i instalacija na klijentska racunala
- skidanje zlocudnog koda

Napadi --> heartBlead (ranjivost openSSL implementacije)
--> SSL Stripping <-- problem kod prvog pristupa
--> BEAST <-- predvidiljiv

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

DDos

- nije samo za mrezni sloj (memorija, cpu, disk)
- teska obrana
- posljedice katastrofalne

napadi --> preplavljivanja (lazni UDP, icmp, DNS, VoIP overflow)
--> preplavljivanje koje iskoristava karakteristika protokla (SYN, SYN ACK , ACK PUSH ACK, RST/FIN overflow)
--> DNS, NTP amplification

zastita --> na strani zrtve <-- ako je napad temeljen na udp moguce blokirati ga

--> komunikacijski put (suradnja s ISP-om)

Mrezna sigurnost 3

Monday, February 21, 2022 10:41 PM

Aplikacijski sloj

- port 1 do 65k (netstat pokazuje portove)

Udaljeno otkrivanje aplikacija
- pokusaj prisupa aplikaciji (preko weba ili telneta)

TCP skeniranje
- SYN skeniranje(salje se SYN i ceka se odgovor, ako nema odgovora ne znamo kakava je situacija), TCP connect (ako nije ukljucen filter)
  FIN skeniranje (sigurno se moze znati da nema nicega, vraca se RST inace ignore), skeniranje framgentacijom (izbjegavanje detekcije)

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

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)

Mail server

MTA - mail transfer agent
MUA - mail user agent

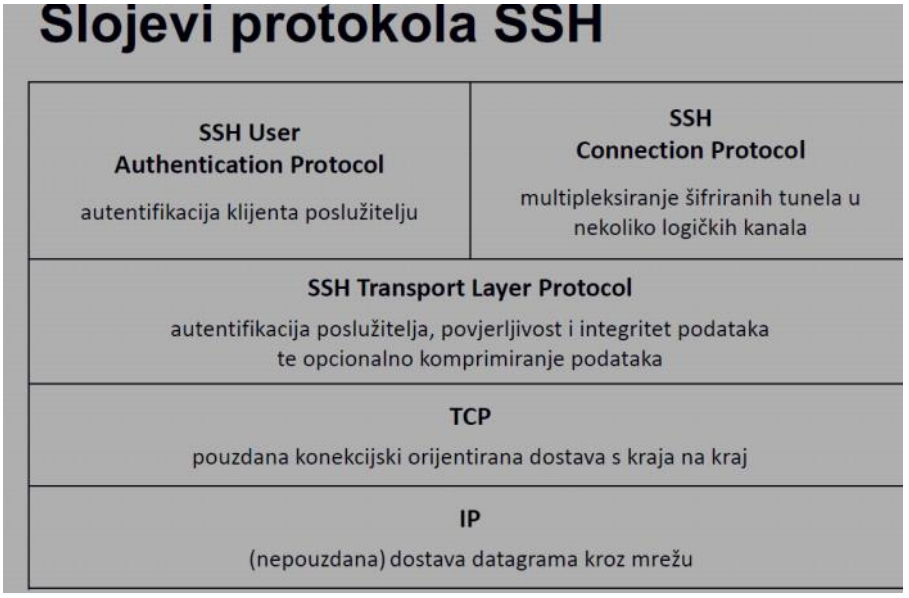
- integrirano rjesenje (groupware) --> MS Exchange
- nesiguran, potrebna nadogranja

FTP

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

SSH

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



dogovara nacin razmjene kljuceva, simetricni/asimetricni algoritam sifriranja, autentifikaciju i sazetka

Autentifikacija klijenta na SSH

- asimetricna kriptografija, prijava uz username i password

Transport Layer
- nacin razmjene kljuceva, asimetricni alg. sifriranja, simetricni alg sifriranja

Usluge --> ssh client, ostvarivanje VPN-a, prijenos datoteka

Problemi na SSH --> tajni kljuc nije zasticen lozinkom, popis racunala i javnih kljuceva, zamjena i povlacenje kljuceva

DNS

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

<-- rjesenje
prijetnje --> 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

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 **DNSSEC** --> salje se izvorni i potpisan podatak DNS sec nadopuni 41/67
Problemi <-- ne osigurava povjerljivost, ne stiti od DDoS napada

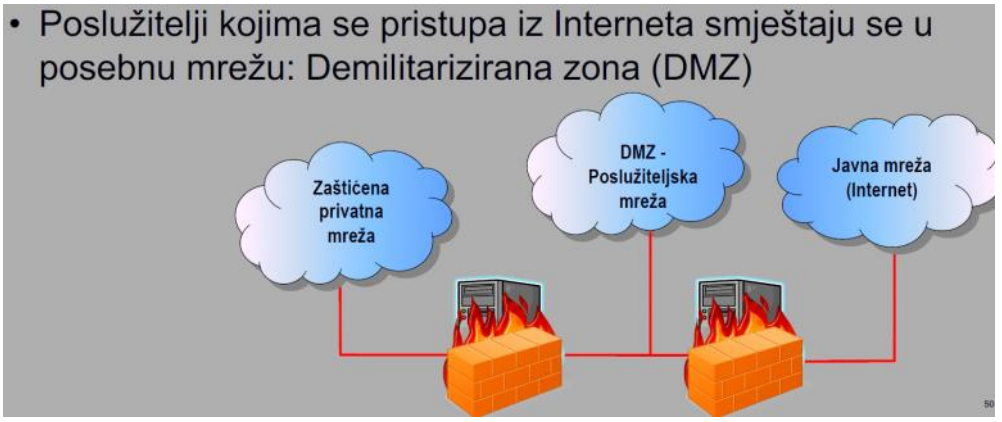
Zloupotrebe --> autorizacija i autentifikacija na temelju domene, raspodjela osjetljivih podataka

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

FIrewall

- smjesten izmedu 2 mreza
- provjera pakete sa pravilima

NAT --> zasebna funkcinalnost, nije za sigurnost



lanci --> lista pravila u kojima se definiraju pravila

packet filter --> blokira pakete na temelju (TCP, UDP), port, TCP flag (SYN , ACK), ranjiv na spofing

Statefull inspection --> pamte se stanja , prati se slijed sesije

iptables chains --> input, output, fowared, prerouting, postrouting (accept - paket se prihvaca, drop - paket se odbacuje, reject - kao drop ali salje icmp request)

genericki uzorci --> p (protocol), s (src), d (dst) , i (interface), o (out interface), m state (establishet, related)

Firewall Napomena --> nije rjesenje sigurnosti

Proxy --> spaja se na lokalni server, bolji nadzor mreznog promea

Sustavi za detekciju upada

IDS

- sustav za detekciju uljeza
- anomalije u sustavu
- podjele
    1. prema mjestu nadzora
        - NIDS --> podatke s mreze, HIDS <-- podatke s racunala
    2. nacinu rada
        - pravila ili anomalije
    3. Sustav za pervernciju upada
        - IPS, dodatna pravila na firewall
    4. Otkrivanje ranjivosti u mrezi
        - skeniranje mreznih raspona
        - penetracijska ispitivanja

- problemi s brzinama (10G+), sifriranom komunikacijom
- implementacije SNORT, BRO

Wifi

Tuesday, February 22, 2022 12:24 AM

Osnovna svojstva
- koriste elektromagnetske valove za prijenos podataka

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

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

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

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

Zadnje predavanje

Tuesday, February 22, 2022 12:38 AM

Digitalna forenzika --> grana forezinckih znanosti
Digitalni dokaz --> digitalni podatak koji pozudano podrzava ili opovrgva hipotezu
Racunalna forenzika --> forenzika samo racunala

- policija koristi forenziku, tvrtke, institucije

provodenje digitalne forenzike --> integritet i autenticnost
izazovi --> kriptografija, apple cloud, veci kapaciteti memorije

Upravljanje sigurnoscu
- ciljan, sustava i kontinuiran pristup

Upravljanje rizicima

- uvid u ogranizaciju
- fokus na problem, ranjivost

Upravljanje rizicma --> procjena (skala od 1 do 5), ovladavanje, pracenjje, identifikacija(pronaci rizike) i tako u krug

4 pristupa za rizik --> uklanjanje, prijenos, umanjenje, prihvacanje

Revizije --> bitna komponenta, elementi provedbe (intervijui, uvid u stanje)

Norme --> ISO 27001, 27002
--> NIST
--> DSS (kreditne kartice), CIS, ITIL

Rukovanje incidentima

- planiranje unaprijed
- upravljanje incindetom --> prepoznati,analizirati i sprijeciti
- rukovanje incidentom --> akitivra nastankom incidenta

Svrha rukovanja incidentima --> smanjenje stete, brz i efikasan oporavak, osiguranje sustava

CERT --> zastita, detekcija i odgovor na incidente
SOC --> analizira detekcije

CTI --> obavjestajni rad u kibernetickom prostoru
- proces i rezultat tog procesa(znanje)

- odnos (binarni kod) podatak -(karakteristika koda) informacija -(karakeristika napadaca) znanje
- razine --> strateska operativna, takticka, tehnicka

OSINT --> (open source inteligence) prikupljanje informacija <-- Linkedin, Twiter, Stackoverflow

Strojno ucenje

napad na Alexu, Siri, autonomna vozila, koristi se tamo gdje nema smisla

Privatnost --> prikrivanje podataka, tko ima uvid u nase podatke <-- narusavanje (krada, ucjena, javna sramota)

Anonimnost --> prikrivanje tko je objavio informacije <-- narusavanje (IP adrese, Web cookie)

Incognito --> ne pamte se lozinke, cokkie, jos je vidljiva IP adresa, nema prijava

Anonimizirajuci Web browser --> proxy --> da se ne vidi tko si i sta si, curenje cookie-a, IP adresa, ne znamo jel biljeze ili ne IP adrese

VPN --> skriva IP, ne cuva podatke IP adresa

Mreza Tor --> ulazni, releji, izlazni cvorovi

- nudi skriveni server umjesto klijenta

problemi --> latencija, kriminal, ISP moze blokirati ako se vrti izlazni cvor

Dark web --> droga, pornografija