SVEUČILIŠTE U ZAGREBU
Fakultet elektrotehnike i računarstva

Diplomski studij

Sigurnost komunikacija

Ak. godina 2022./2023.

Sigurnost aplikacijskog sloja

Creative Commons

- **slobodno smijete:**
  - **dijeliti** — umnožavati, distribuirati i javnosti priopćavati djelo
  - **remiksirati** — prerađivati djelo
- **pod sljedećim uvjetima:**
  - **imenovanje**. Morate priznati i označiti autorstvo djela na način kako je specificirao autor ili davatelj licence (ali ne način koji bi sugerirao da Vi ili Vaše korištenje njegova djela imate njegovu izravnu podršku).
  - **nekomercijalno**. Ovo djelo ne smijete koristiti u komercijalne svrhe.
  - **dijeli pod istim uvjetima**. Ako ovo djelo izmijenite, preoblikujete ili stvarate koristeći ga, preradu možete distribuirati samo pod licencom koja je ista ili slična ovoj.

U slučaju daljnjeg korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom na ovu internetsku stranicu. Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava. Ništa u ovoj licenci ne narušava ili ograničava autorova moralna prava.

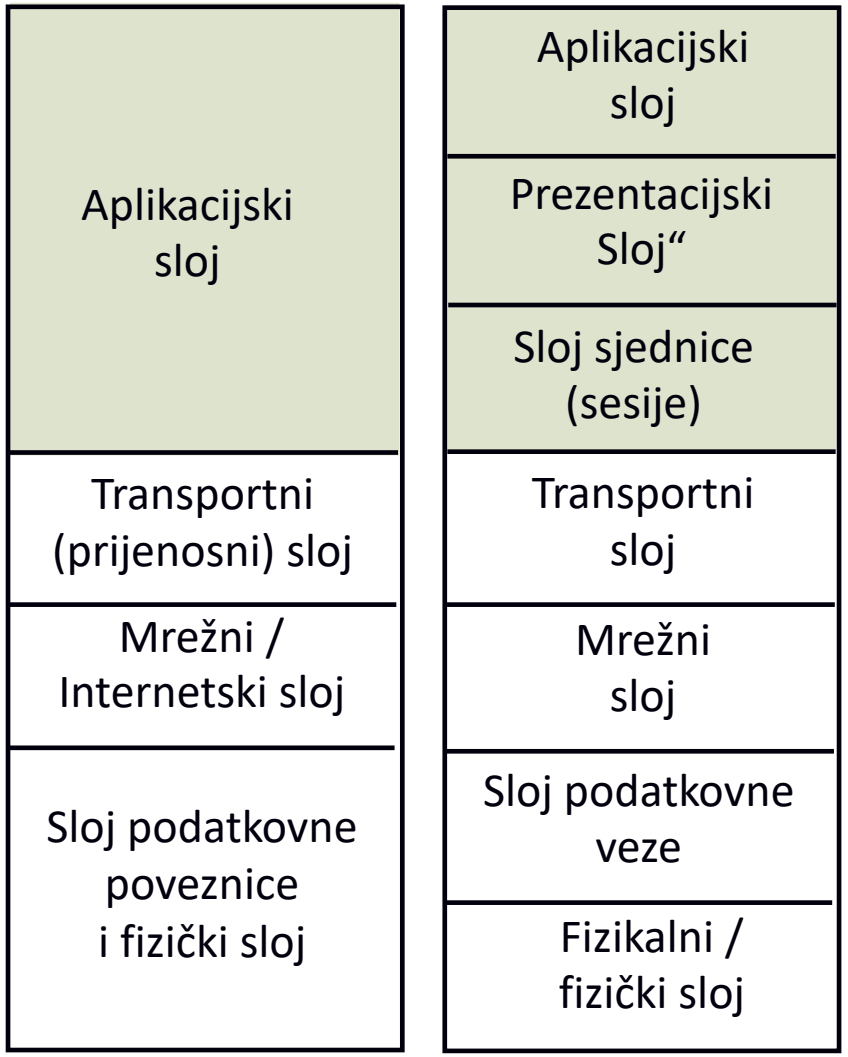
Tekst licencije preuzet je s http://creativecommons.org/.

Sadržaj

- općenito o aplikacijskom sloju
- metode otkrivanja aplikacija na mrežnim čvorovima
- česti sigurnosni problemi s aplikacijama
- aplikacije za udaljeni rad

Općenito o aplikacijskom sloju

- mnoštvo različitih aplikacijskih protokola
  - ne smije se miješati pojam aplikacije i aplikacijskog protokola
  - najčešći model usluge klijent-poslužitelj
- aplikacijski protokoli za prijenos koriste kombinaciju komunikacijskog protokola i dobro poznatih pristupa (engl. well known ports)
  - IETF aplikacijski protokoli imaju rezerviran pristup
    - korisnici aplikacija mogu koristiti i druge ako žele
  - vlasnički aplikacijski protokoli nemaju rezerviran pristup



Vidljivost aplikacija na mrežnom čvoru (1)

- Poslužiteljske aplikacije osluškuju zahtjeve na dobro poznatim pristupima
  - Pristupi su brojevi od 1 do 65535 (za svaki prijenosni protokol: TCP, UDP, SCTP, …)
- Administrator (ili običan korisnik) na nekom računalu korištenjem odgovarajućih alata može dobiti popis:
  - Pristupa na kojima čeka neka aplikacija
  - Poslužiteljskih aplikacija koje osluškuju zahtjeve
  - Popis statusa veza (uspostavljene ili bilo koje drugo stanje)
- Na Unix / Linux / Windows OS-u alat je netstat
  - Ima i mnoštvo drugih sa i bez grafičkog sučelja

Vidljivost aplikacija na mrežnom čvoru (2)

- Primjer (izvršavanje na Linuxu)

```
$ netstat -an4
Active Internet connections (servers and established)
Proto Recv-Q Send-Q   Local Address           Foreign Address         State
tcp        0      0   0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0   127.0.0.1:38245         0.0.0.0:*               LISTEN
tcp        0    172   31.147.204.44:22        161.53.19.9:61407       ESTABLISHED
tcp        0      0   31.147.204.44:22        95.168.116.4:43619      ESTABLISHED
udp        0      0   0.0.0.0:5555            0.0.0.0:*
```

Udaljeno otkrivanje aplikacija

- Temeljni način udaljenog otkrivanja aplikacija je skeniranje pristupa kako bi se utvrdilo koji su otvoreni
  - Najjednostavnija metoda skeniranja je pokušaj pristupa aplikaciji
  - Može se obaviti aplikacijom (Web preglednik u slučaju Weba) ili, općenitije, telnet aplikacijom u slučaju protokola TCP
- Otvoren pristup znači da je neka aplikacija prisutna
  - Samo na temelju te informacije se ne može znati koja aplikacija je prisutna.
- Potrebno je dodatno prikupljanje informacija kako bi napadač otkrio aplikaciju, i njenu verziju
  - Točna verzija je potrebna radi pronalaženja potencijalnih ranjivosti

Otkrivanje aktivnih TCP aplikacija (1)

- Pokušaj uspostave veze (engl. TCP connect)
  - Najjednostavnija metoda koja uspostavlja u potpunosti vezu te ju odmah prekida
  - Moguće korištenje specifičnih alata ili generičke telnet naredbe
  - Upostava veze -> postoji aplikacija na pristupu, RST ne postoji
- TCP SYN skeniranje
  - tzv. poluotvoreno skeniranje (engl. half-open scanning)
  - Šalje se SYN te gleda odgovor
    - SYN+ACK znači da aplikacija sluša, čeka uspostavu veze na danom pristupu
    - RST znači da na danom pristupu ne čeka nikakva aplikacija
- U oba slučaja, ako nema odgovora tada negdje na putu postoji nekakav filter i ne znamo kakva je situacija

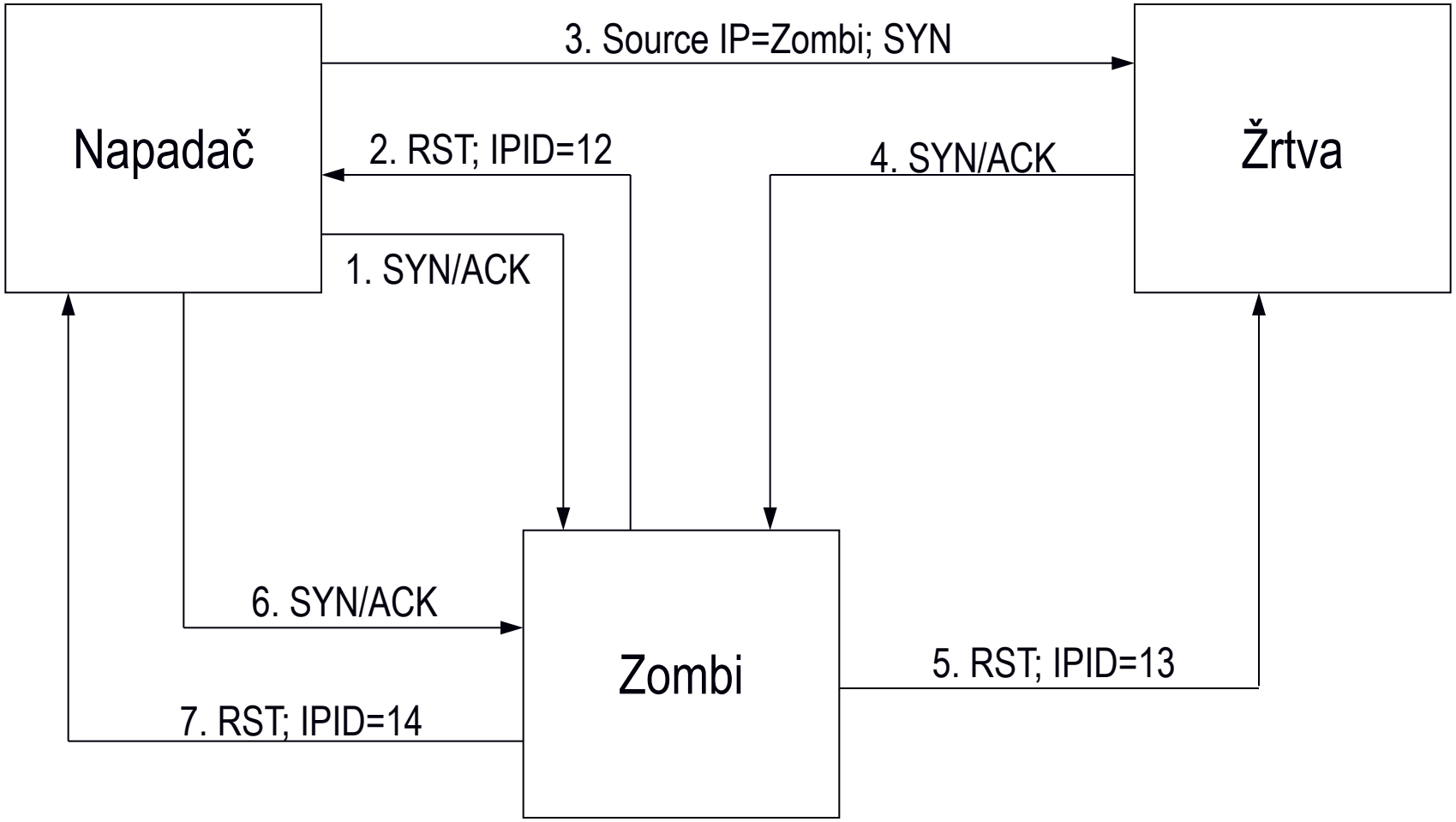
Otkrivanje aktivnih TCP aplikacija (2)

- TCP FIN skeniranje
  - Šalje se segment s FIN zastavicom. U slučaju da nema ničega na pristupu, vraća se RST, u suprotnom se zahtjev ignorira
  - Određene implementacije u oba slučaja šalju RST segment
  - Sigurno možemo znati samo da nema ničega na pristupu
- Skeniranje s fragmentacijom (engl. fragmentation scanning)
  - Nije posebna vrsta skeniranja već mehanizam izbjegavanja detekcije
  - Fragmentiranjem IP paketa u kojemu je TCP segment otežava se detekcija skeniranja

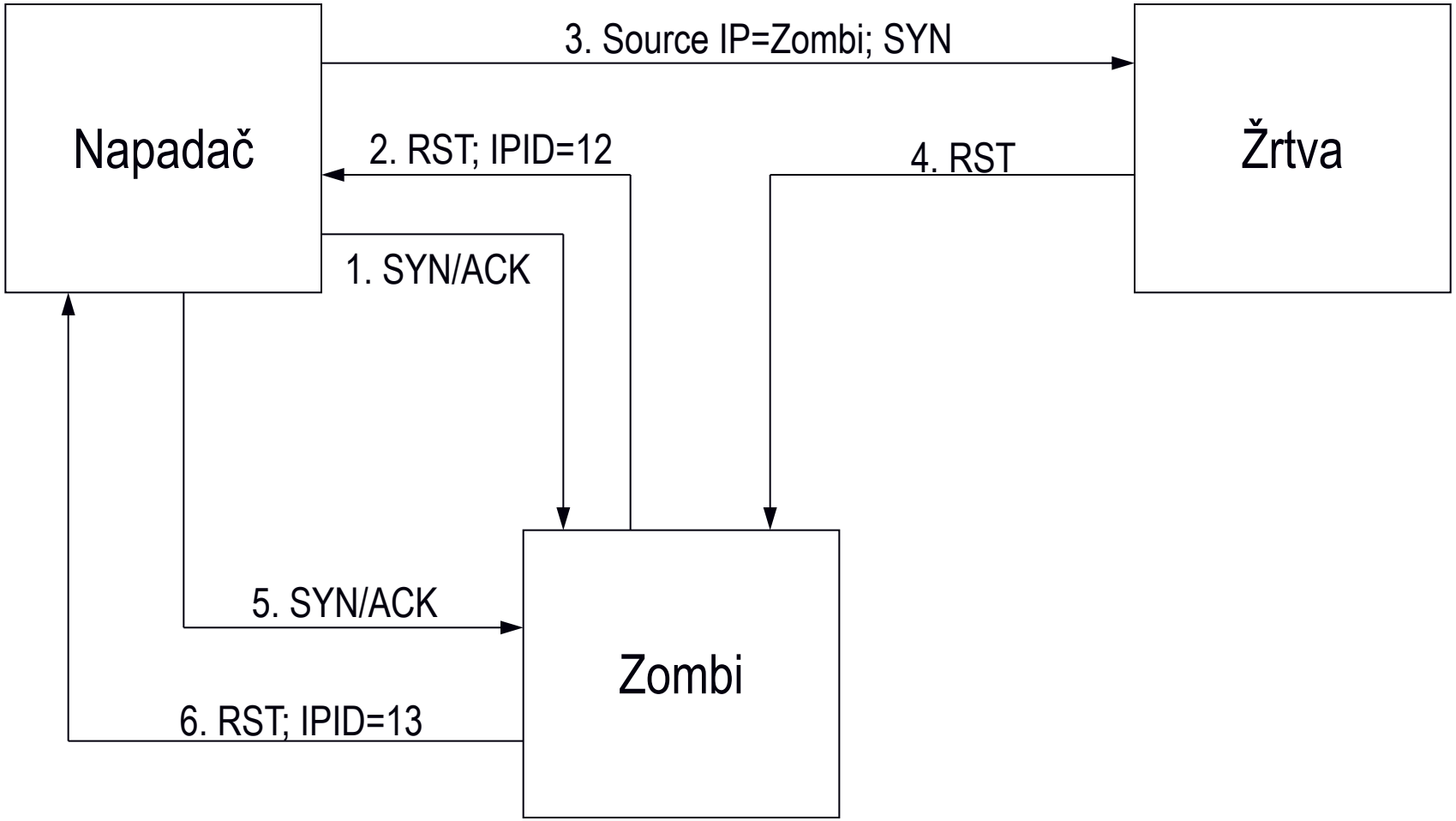
Prikrivanje izvora skeniranja

- sva prethodna skeniranja otkrivaju lokaciju napadača
- „Idlescan” je način skeniranja korištenjem treće strane (tzv. zombi)
- očekivanja od zombija
  - mala količina prometa koju generira
  - predvidivi identifikator IP paketa (polje ID)
- ideja skeniranja
  - utvrđuje se trenutni ID koji zombi koristi
  - šalje se paket pri čemu je kao izvorišna adresa naveden zombi
  - ponovo se utvrđuje korišteni ID i na temelju toga određuje rezultat skeniranja

„Idlescan”: ako je port otvoren



„Idlescan”: ako je port zatvoren



Skeniranje UDP porta (1)

- Slanje (praznog) UDP datagrama
- Za zatvoren pristup pristižu poruke “ICMP port unreachable”
  - Osim ako je negdje na putu instaliran filter
- Kada je pristup otvoren ne šalje se nikakav odgovor
  - Pod pretpostavkom da poslužitelj ignorira poruke koje nisu ispravno formatirane i nisu primljene u ispravnom redoslijedu
  - Ako se ne dobije ICMP poruka pretpostavlja se da je port otvoren
    - Što baš ne mora biti slučaj…

Skeniranje UDP porta (2)

- Potencijalni problemi za napadača
  - UDP je nepouzdan te je potrebno pokušati nekoliko puta kako bi bili sigurni da nije došlo do gubitaka (posljedica je također da nema odgovora!)
  - Neki operacijski sustavi ograničavaju brzinu slanja ICMP poruka (RFC 1812, 4.3.2.8)
    - Generiraju ograničen broj ICMP poruka u sekundi
- Vrlo spora tehnika skeniranja

Poteškoće sa skeniranjem za napadača

- Relativno velik broj pristupa po čvoru
  - Mora balansirati brzinu i detaljnost kako bi izbjegao otkrivanje
  - Skeniranje samo određenog podskupa pristupa
- Potencijalno velik broj čvorova koje je potrebno skenirati
  - 254 u slučaju mreže s mrežnom maskom 24
- Ako je između cilja i napadača filter ne vraćaju se odgovori i nije moguće znati je li port otvoren ili ne
- Ako je neki port otvoren ne znači da se tamo nalazi očekivana aplikacija

Detekcija aplikacija i operacijskog sustava

- Kako bi napadač mogao iskoristiti aplikaciju koja sluša na nekom pristupu mora znati koje ranjivosti ima
  - Poznavanjem točne verzije aplikacije i koristeći baze ranjivosti može pripremiti napad na aplikaciju
  - Slično vrijedi i ako traži novu ranjivost
  - Određene aplikacije izvršavaju se na više operacijskih sustava pa je dobro znati i koji je operacijski sustav korišten
- Napad je moguć i na operacijski sustav, za što je potrebno također znati točnu verziju operacijskog sustava
  - „OS fingerprinting”

Detekcija aplikacije

- Napadač se spaja na port
  - Neke aplikacije objavljuju svoju verziju u pozdravnim porukama koje šalju odmah po spajanju
  - Koristeći očekivani protokol pokušava komunicirati s aplikacijom
    - Na taj način utvrđuje da pretpostavljena aplikacija čeka na pristupu
  - Moguće je na temelju konverzacije s aplikacijom utvrditi verziju
- Problemi za napadača
  - Ako aplikacija ne objavljuje svoju verziju/tip ili objavljuje neku generičku ili lažnu verziju
  - Na aplikacije se stavljaju zakrpe (patch) koje ne mijenjaju prijavljenu verziju aplikacije
  - Funkcionalnosti iz novijih verzija se dodaju na starije (a s njima i ranjivosti) pri čemu se također ne mijenja prijavljena verzija

Otkrivanje vrste i verzije operacijskog sustava

- „OS fingerprinting”
  - Norme i specifikacije protokola ne definiraju apsolutno svaki detalj ponašanja implementacije
    - Kada se implementira protokol odabire se različita ponašanja – slučajno ili namjerno
    - Iz verzije u verziju također se nadograđuje mrežni stog te mu se mijenja ponašanje
  - Detekcija OS-a temelji se snimanju ponašanja njegova mrežnog stoga te usporedbi s bazom poznatih operacijskih sustava
  - Detekcija nije u potpunosti pouzdana, tj. uvijek postoji mogućnost pogreške
    - snimljenom ponašanju odgovara više operacijskih sustava!

Primjer alati za skeniranje: nmap

```
# nmap -O 31.147.204.44
Host is up (0.0011s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.4

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.93 seconds
```

Česti sigurnosni problemi s aplikacijama

- pogađanje vjerodajnica i drugih informacija
  - najčešće pogađanje grubom silom
  - neispravno rukovanje lozinkama
- korištenje nezaštićene komunikacije
- ranjivosti u aplikaciji aplikacije koje omogućavaju njenu zloupotrebu

Napadi pogađanja grubom silom

- Pokušaj otkrivanja nepoznate ili tajne informacije upotrebom pogađanja (engl. brute force)
  - Najčešće se pogađaju lozinke
  - Pogađanje korisničkih imena, dijeljenih tajni,…
- Sve usluge (engl. services) koje omogućavaju prijavu putem mreže ranjive su na pogađanje
  - telnet, ftp, r* naredbe, ssh, http, snmp, …
- Napad pogađanja može biti „on-line” ili „off-line”
  - „on-line” uključuje interakciju s uslugom
  - „off-line” radi na ukradenim podacima

Zaštite od pogađanja grubom silom

- Ograničavanje pristupa usluzi
- Kvalitetne, jake lozinke (dobra entropija!)
  - Nametati ograničenja kompleksnosti lozinke
  - Koristiti fraze (passphrases) umjesto lozinki
- Ograničavanje broja pokušaja, zaključavanje
  - Ubacivanje kašnjenja između dva pokušaja
  - Nakon N pokušaja privremeno ili permanentno zaključavanje korisničkog računa
- Primjena jačih autentifikacijskih metoda (PKI, 2FA, …)
- Pohrana lozinki u šifriranom obliku ili u obliku sažetka
  - Zaštita od „off-line” pogađanja

Nekorištenje šifrirane komunikacije

- Mnogi protokoli šalju podatke preko mreže u čistom obliku
  - Snimanjem prometa moguće je ukrasti osjetljive podatke
  - Dosta često slanje lozinke preko mreže
- Mnogi aplikacijski protokoli su ranjivi na prisluškivanje
  - Posebno su kritični aplikacijski protokoli temeljeni na UDP-u
    - TLS se ne može koristiti, a DTLS nije toliko zaživio
- Zaštite
  - Šifriranje na nižim slojevima (IPsec, TLS)
  - Tuneliranje korištenjem aplikacije SSH ili neke slične metode
  - Korištenje autentifikacijskih protokola koji ne prenose lozinke preko mreže
  - Noviji protokoli razvijaju se s „ugrađenom” enkripcijom, npr. QUIC/HTTP3

Ranjivosti implementacija Internet usluga

- značajan broj infrastrukturnih usluga Interneta implementiran je u programskim jezicima C/C++
  - jezici niskog nivoa u kojima je vrlo lako uvesti ranjivost
- niz čestih ranjivosti – neki specifični za C/C++ a neki općeniti
  - preplavljivanje spremnika (engl. buffer overflow), pisanje van granica polja
  - problemi sa nizovima za formatiranje
  - dvostruko oslobađanje radne memorije (engl. double free)
  - pogreške u aritmetičkim operacijama („krivi” tipovi podataka)
  - ... i niz drugih

Posljedice ranjivosti

- infrastrukturne usluge dostupne su na Internetu
  - šaljući posebno formatirane zahtjeve napadač pokušava iskoristiti ranjivosti
  - određene ranjivosti nisu dostupne putem mreže već samo lokalno – tada se koriste za podizanje privilegija jednom kada se dobije pristup računalu
- usluge/aplikacije izvršavaju se s nekim privilegijama, često i administratorskima
  - ovladavanjem usluge napadač preuzima njene ovlasti, moguća potpuna kontrola poslužitelja na kojemu se izvršava usluga
- napadači iskorištavaju ranjivosti korištenjem tzv. „shellcode-a”
  - kratak kod, s vrlo specifičnim uvjetima rada, zadaća mu je pokrenuti nešto drugo – primjerice pokrenuti proces za udaljeni pristup

Neke općenite zaštite

- dobar dizajn programa sa uključenom sigurnošću od samog početka
- pisanje koda pazeći da se ne uvode ranjivosti
- izbjegavati izvršavanje Internet usluga s administratorskim ovlastima
  - postoje još dodatni mehanizmi ograničavanja prava procesa
- nadogradnja aplikacija čim se otkriju ranjivosti
  - CVSS je jedna korisna mjera za određivanje opasnosti od ranjivosti
- isključivati nepotrebne usluge
- ograničavati pristup uslugama

Primjer: Preplavljivanje spremnika

- mehanizam ranjivosti
  - programer alocira određenu količinu prostora za prihvat podataka s mreže
    - na stogu (stack overflow) ili na gomili (heap, heap overflow)
  - napadač namjerno šalje veću količinu podataka te se podaci moraju prepisati van predviđenog prostora – prepisuju nešto drugo
    - „nešto drugo” su nekakvi parametri na stogu, primjerice povratna adresa
  - po povratku iz funkcije izvršava se napadačev kod (shellcode)
  - napadačev kod izvršava neku akciju koja omogućava pristup napadaču
- zaštita
  - pažnja prilikom pisanja koda, korištene zaštitnih mehanizama, izbjegavanje nesigurnih funkcija
  - korištenje neizvršivog stoga i gomile

Poslužitelji elektroničke pošte

- Elektronička pošta koristi barem dva poslužitelja
  - MTA - Mail Transfer Agent (postfix, sendmail, qmail, …)
  - MUA - Mail User Agent / MDA - Mail Delivery Agent (dovecot, …)
- Danas je uobičajeno integrirano rješenje (tzv. groupware)
  - MS Exchange, Zimbra, Lotus Notes
  - Značajno povećana kompleksnost sustava što znači i vjerojatnije pogreške
  - Mogućnost korištenja jednostavnijeg posredničkog poslužitelja radi sigurnosti
- Poslužitelj elektroničke pošte direktno izložen na Internetu
  - Sprečavanje pristupa bi onemogućilo primanje elektroničke pošte
- Obavezna redovita nadogradnja

Usluga prijenosa datoteka (1)

- Originalno za tu namjenu bio je predviđen protokol FTP
  - File Transfer Protocol
- Jedna od primjena je anonimni „upload” i „download” datoteka
  - Neispravnim podešavanjem moguće je napadačima omogućiti postavljanje nedozvoljenih sadržaja, dohvat postojećih „skvirenih” datoteka, brisanje sadržaja, čitanje i pisanje direktorija na poslužitelju kojima se ne bi smjelo pristupiti
  - Napadači su znali razmjenjivati piratizirani materijal zloupotrebom anonimnih FTP poslužitelja
- Nema zaštitu komunikacije, prijenos lozinke preko mreže
  - Postoji ekstenzija FTPS, ali se ne koristi često

Usluga prijenosa datoteka (2)

- Protokol uključuje otvaranje zasebnih TCP veza!
  - Kontrolni kanal koristi jednu TCP vezu, za svaki prijenos podataka otvara se zasebna TCP veza
  - Otvaranje zasebne veze može biti u aktivnom i pasivnom modu
    - Aktivni način -> poslužitelj se spaja na klijenta
    - Pasivni način -> klijent se spaja na poslužitelj
- Povećava kompleksnost uređaja vatrozid/NAT
- Preporuka: izbjegavati
  - Alternativa SFTP/SCP
  - Ne koristiti anonimni pristup

Usluga nadzora mreže

- SNMP – Simple Network Management Protocol
  - udaljeni nadzor (i upravljanje) usmjernika, preklopnika, poslužitelja,...
  - nema kriptografsku zaštitu, koristi UDP
  - mogućnost DoS ili udaljenog izvođenja naredbi
- zaštita
  - provjeriti sve uređaje u mreži koji imaju omogućen SNMP (npr. SNScan)
  - onemogućiti SNMP na svima uređajima na kojima nije nužan
  - instalirati najnovije zakrpe, „firmware update”
  - promijeniti podrazumijevane „public” i „private community”
  - izolirati u zaseban VLAN te vatrozidom ograničiti pristup
  - koristiti SNMPv3

Udaljeni rad

- Najpoznatiji protokol: SSH
  - Zamijenio telnet, r naredbe (rsh, rlogin, rcp), ftp
  - OpenSSH – najpoznatija implementacija, otvorenog koda, Unix/Linux, Windows
  - PuTTY – poznati klijent na Windows operacijskom sustavu
  - WinSCP – za prijenos datoteka na Windows OS-ovima
- Postoje i komercijalne implementacije (SecureCRT)
  - U odnosu na OpenSSH jedina prednost je GUI sučelje

Slojevi protokola SSH

SSH User Authentication Protocol autentifikacija klijenta poslužitelju	**SSH Connection Protocol** multipleksiranje šifriranih tunela u nekoliko logičkih kanala
SSH Transport Layer Protocol autentifikacija poslužitelja, povjerljivost i integritet podataka te opcionalno komprimiranje podataka	
TCP pouzdana konekcijski orijentirana dostava s kraja na kraj	
IP (nepouzdana) dostava datagrama kroz mrežu	

SSH Transport Layer Protocol

- Dogovara način razmjene ključeva, asimetrični algoritam šifriranja, simetrični algoritam šifriranja, algoritam za autentifikaciju poruka i algoritam kriptografskog sažetka
  - klijent i poslužitelj razmijene uređene liste podržanih algoritama
  - odabire se prvi algoritam koji se nalazi na popisu klijenta, a ujedno je podržan od strane poslužitelja
  - ako se ne može pronaći zajednički algoritam, veza se prekida

SSH Transport Layer Protocol

- Autentifikacija poslužitelja korištenjem para ključeva (javni/privatni)
  - poslužitelj može imati više ključeva za različite asimetrične algoritme
  - više poslužitelja može dijeliti isti ključ
- Prilikom prvog spajanja klijentski program korisniku prikazuje sažetak poslužiteljskog ključa
  - Od korisnika se očekuje provjera ispravnosti sažetka kako bi se spriječio MITM
  - Nakon provjere korisnik bi trebao potvrditi ispravnost sažetka ključa (Leap of faith)
  - Klijentski program zapisuje ključ lokalno i više ga ne predočava korisniku, ali ga obavezno provjerava prilikom svakog spajanja
    ~/.ssh/known_hosts

Podržane autentifikacije klijenta

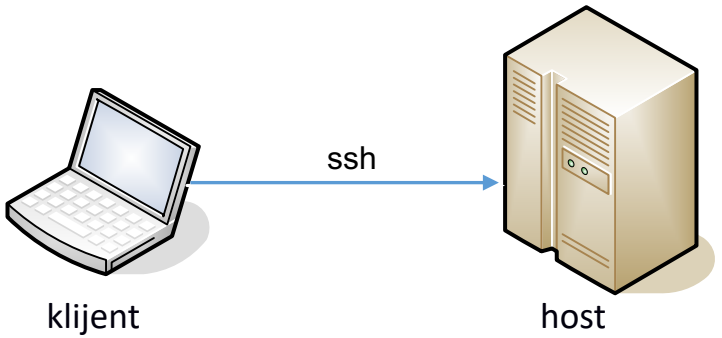
- Prijava upotrebom korisničkog imena i lozinke
- Upotreba asimetrične kriptografije
  - Klijent generira par javni-tajni ključ
  - Tajni ključ može i treba biti zaštićen lozinkom
  - Javni ključ instalira na svako računalo kojemu želi pristupiti (~/.ssh/authorized_keys)
- Podržano je još
  - PKI, Kerberos, PKCS11, integracija s PAM sustavom na Linuxu, 2FA, …

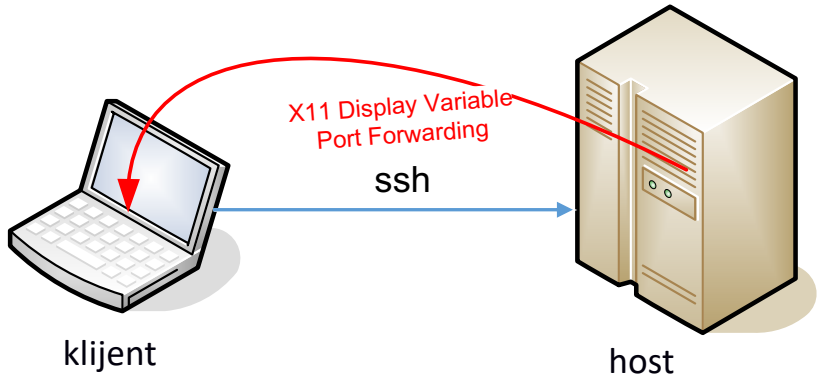
Usluge temeljene na protokolu SSH

- Udaljen rad (ssh klijent)
- Prijenos datoteka (scp i sftp klijenti)
- Tuneliranje Ethernet okvira ili IP datagrama
  - Ostvarivanje VPN-ova na drugom ili trećem sloju
- Prosljeđivanje (engl. forwarding) lokalnih i udaljenih pristupa
  - Spajanjem na lokalni pristup otvara se veza na udaljenom računalu prema nekom drugom pristupu/IP adresi (prosljeđivanje lokalnog pristupa)
  - Spajanjem na pristup udaljenog računala otvara se veza na neki pristup lokalnog računala (prosljeđivanje udaljenog pristupa)

Načini korištenja

- udaljeni pristup:
  `ssh user@host`
- interaktivna naredba:
  `ssh -t user@host naredba`
- X11 naredba:
  `ssh -X user@host Xnaredba`
- za verzije novije od OpenSSH 3.8p1:
  `ssh -Y user@host Xnaredba`

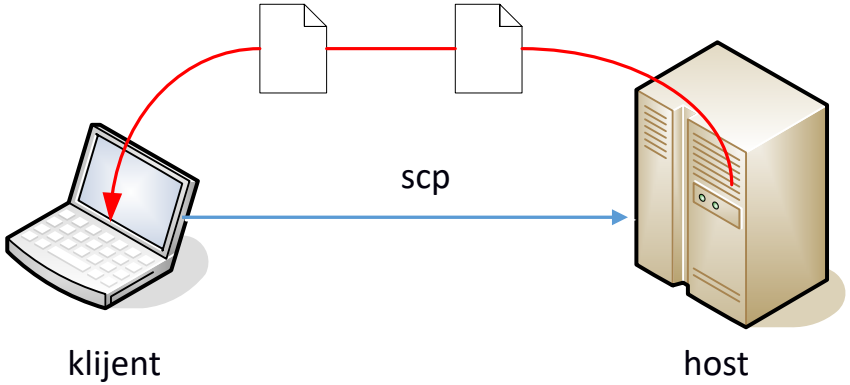




Kopiranje datoteka

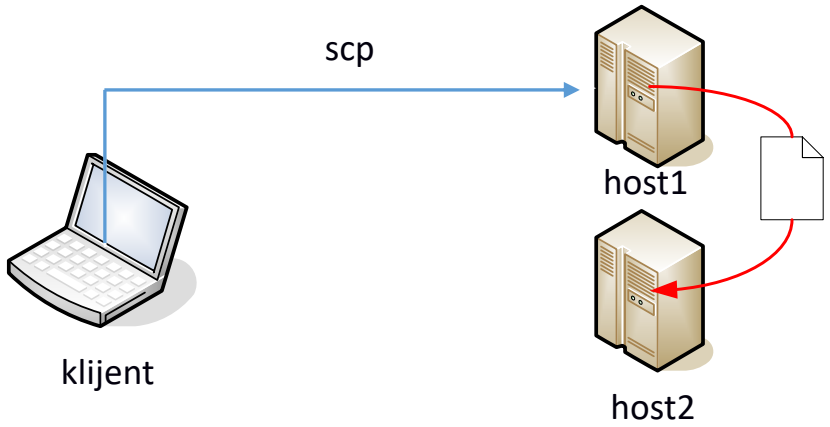
- kopiranje na lokalno računalo:

```
scp user@host:src_path dest_path
```



- kopiranje na udaljeno računalo:

```
scp src_path user@host:dest_path
```



- kopiranje s host1 na host2:

```
scp user@host1:src_path user@host2:dest_path
```

Host ključevi

- ključevi se koriste za verifikaciju autentičnosti udaljenog računala
- javni ključevi provjerenih računala:
  `/etc/ssh/known_hosts`
  `~/.ssh/known_hosts`
- poruka prilikom prvog spajanja

```
$ ssh mrepro.tel.fer.hr
The authenticity of host 'mrepro.tel.fer.hr (161.53.19.47)' can't be established.
RSA key fingerprint is SHA256:vV4ju0F3SbDzJa3g7SWEx8DRhg+7XP0r/c7+nMQzWBg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'mrepro.tel.fer.hr,161.53.19.47' (RSA) to the list of known hosts.
```

- sadržaj datoteke `~/.ssh/known_hosts`:

```
mrepro.tel.fer.hr,161.53.19.47 ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC+YGlJbtrzLhSy1qu+c6/38DRFGG0f/PPeiNtfReYIQ1CquiUU4rSCWeL7xQjtA5Kh
O/0Ej6vzkMr4k0ANsviDJ1NgweOUJNo/DVZv+YreNjm1EZH350O43CH17Eo5VphNi+5KdGeartpTESNt/Dv+ACtMGpra5Gg+
ELLaBkovG/YgzswTGdk+UZ4xA1ONg/4dEGF7dvYoXqqG9kpvmeZ+R37vKBRQJ8RT4U0J+YCJBsGcGi2FiIUMFdfyE/JUmH6Y5
aH5HwhM20e/2DQY6p7kMMjm2p6UaAbAUKrgyGEBPyO6tsuf6vopI7GVxGqeMN9EB0H4ve5J9AFoc5FouZKl
```

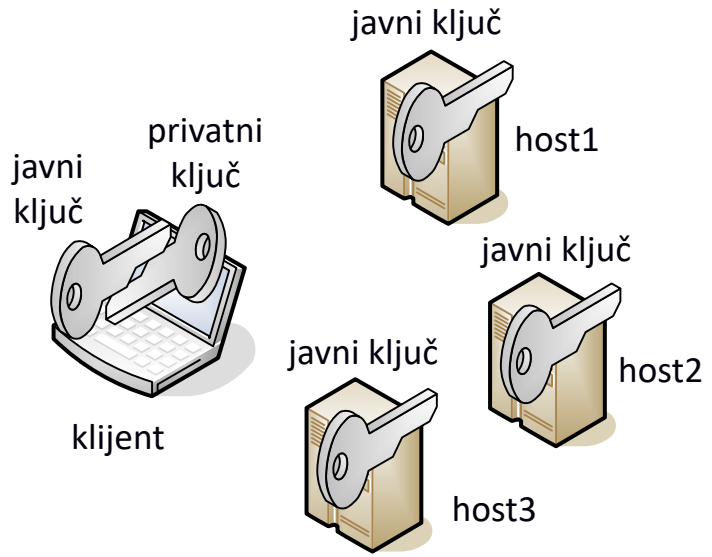
Korisnički ključevi

- autentifikacija korisnika računalu

RSA:
ključevi: `~/.ssh/id_rsa, ~/.ssh/id_rsa.pub`
`$ ssh-keygen -t rsa`

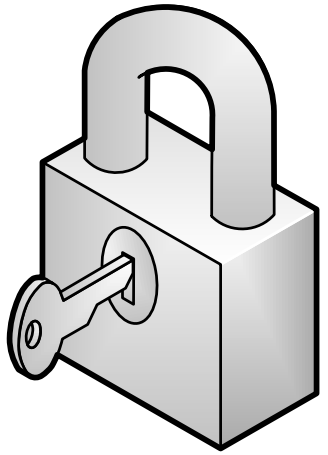
DSA:
ključevi: `~/.ssh/id_dsa, ~/.ssh/id_dsa.pub`
`$ ssh-keygen`

ECDSA:
ključevi: `~/.ssh/id_ecdsa, ~/.ssh/id_ecdsa.pub`
`$ ssh-keygen -t ecdsa`



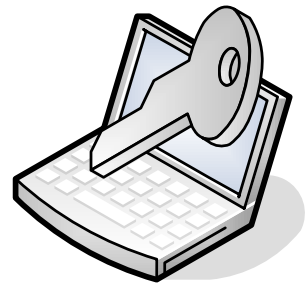
SSH agent

- SSH agent pohranjuje otključanu kopiju ključeva
  `$ eval `ssh-agent``
- u pravilu se pokeće automatski (startup)
- može se prosljeđivati na drugo računalo
- dodavanje ključeva:
  `$ ssh-add`



ssh-agent

privatni ključ

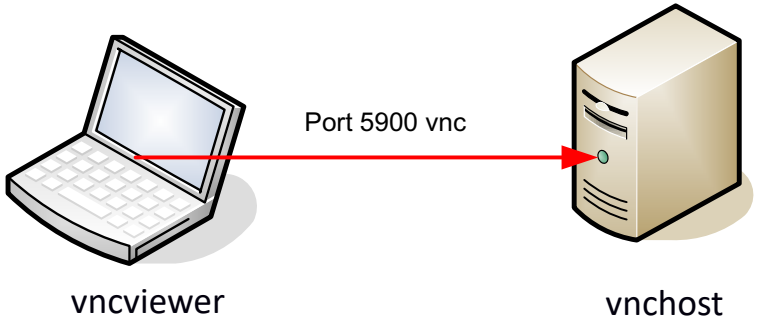


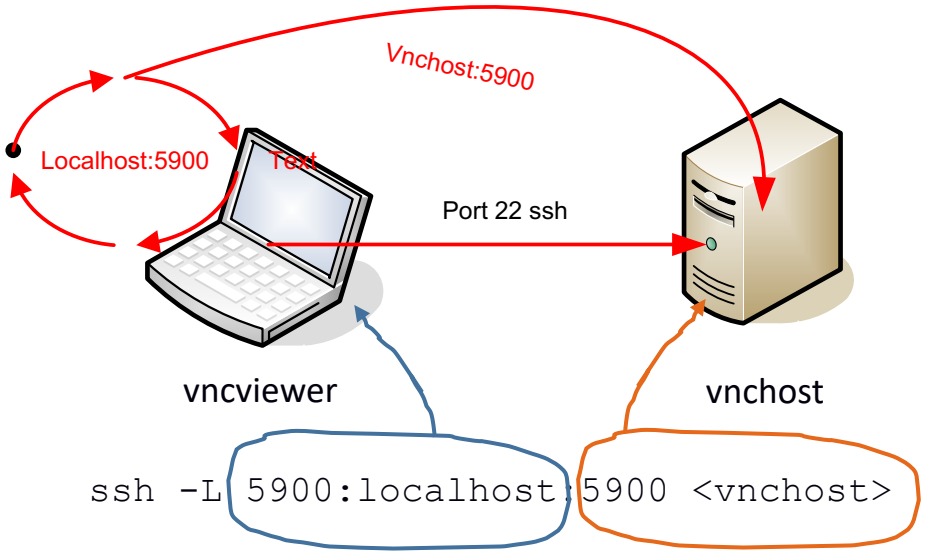
klijent

Port forwarding

- local forwarding:
  `ssh -L <localport>:<targethost>:<targetport> <ssh_host>`
- primjer - osiguravanje VNC komunikacije:

```
$ ssh -L 5900:localhost:5900 <vnchost>
$ vncviewer localhost
```





Mogući operativni problemi sa SSH

- Korisnik nije zaštitio tajni ključ lozinkom
  - Omogućava napadaču neometan pristup svim računalima na koje se može prijaviti bez lozinke
  - To je posebno kritično kada se pristupa administratorskim računima, i/ili se tajni ključ nalazi na slabije zaštićenim radnim stanicama administratora
- Popis računala i javnih ključeva
  - Omogućava napadaču enumeraciju računala bez velikog problema
  - U novijim verzijama pohranjuje se sažetak imena računala
- Zamjena i povlačenje ključeva je zahtjevna
  - Primjerice kada netko ode iz tvrtke