Glava 7: Zaštita mreže

- Principi zaštite mreže:
  - Kriptografija
  - Autentikacija
  - Integritet poruke (digitalni potpis, sertifikaciono tijelo)
- Zaštita u praksi:
  - *Firewall* i *Intrusion Detection System (IDS)*
  - Zaštita na nivoima aplikacije, transporta, mreže i linka

Glava 7

Šta je zaštita mreže?
Operativna zaštita: *firewall* i IDS

Šta je zaštita mreže?

Povjerljivost: samo pošiljalac i prijemna strana treba da "razumiju" sadržaj poruke
- Pošiljalac kriptuje poruku
- Prijemna strana dekriptuje poruku

Autentikacija: pošiljalac i prijemna strana žele da uzajamno potvrde svoje identitete

Integritet poruke: pošiljalac i prijemna strana žele da poruka nije promijenjena u prenosu a da se to ne detektuje

Pristup i dostupnost: servisi moraju biti dostupni i pristupačni korisnicima

Ko može biti napadnut?

- Pojedinci
- Web pretraživači/serveri za elektronske transakcije (on-line kupovine,⋯)
- Klijent/server on-line bankarstva
- DNS serveri
- Ruteri koji razmjenjuju ažurirane tabele rutiranja
- Web kamere
- …

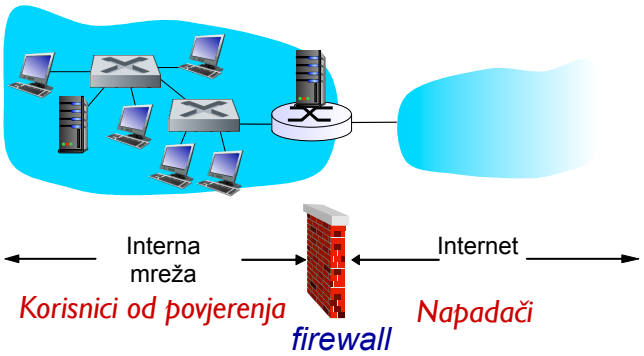
Koje su vrste napada?

- *prisluškivanje:* presrijetanje poruka
- Aktivno *ubacivanje* poruka u komunikaciju
- *Lažno predstavljanje:* lažiranje izvorišne adrese ili bilo kojeg drugog polja paketa
- *Otimanje:* "otmica" komunikacije u toku uklanjanjem jedne strane u komunikacije i zauzimanjem njenog mjesta
- *Onemogućavanje servisa*: sprječavanje da korisnici koriste neki servis (preopterećenje resursa,…)

Firewall

firewall

Izoluje internu mrežu od Interneta, dozvoljavajući da neki paketi prolaze a neki ne



Zašto firewall?

Sprečava DoS napade:

- SYN *flooding*: napadač uspostavlja veliki broj lažnih TCP konekcija ne ostavljajući slobodne resurse za stvarne konekcije

Sprečava ilegalne modifikacije/pristup internim podacima

- Napadač mijenja internet stranicu

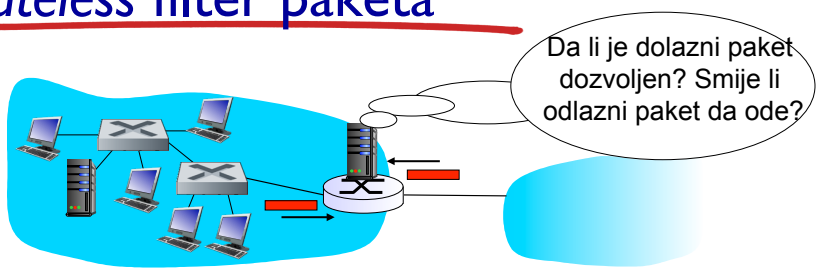
Dozvoljava samo autorizovni pristup unutrašnjosti mreže

- Skup autentifikovanih korisnika/hostova

Tri tipa firewall-a:

- *Stateless* filter paketa
- *Stateful* filter paketa
- Aplikacioni *gateway*

Stateless filter paketa



- Interna mreža je povezana na Internet preko *router*-a koji je istovremeno i *firewall*
- ruter *filtrira paket po paket,* odlučujući o prosleđivanju/ odbacivanju paketa na bazi:
  - izvorišne IP adrese, destinacione IP adrese
  - TCP/UDP izvorišnih i odredišnih brojeva portova
  - Tipa ICMP poruka
  - SYN i ACK flagova u zaglavlju TCP segmenta

Stateless filtriranje paketa: primjeri

- *primjer 1:* blokiraj dolazne i odlazne IP datagrame sa vrijednošću polja *protocol field* = 17 i sa ulaznim ili izlaznim portom 23
  - *rezultat:* sve dolazne i odlazne TELNET konekcije i UDP saobraćaj su blokirani
- *primjer 2:* blokiraj dolazne TCP segmente sa ACK flagom jednakim 0.
  - *rezultat:* sprječavanje eksternih klijenata da uspostave TCP konekcije sa internim klijentima, ali je dozvoljeno internim klijentima da uspostavljaju TCP konekcije.

Stateless filtriranje paketa: još primjera

Politika	*Firewall Setting*
Nema pristupa Webu preko Interneta.	Odbaci sve odlazne datagrame koji sadrže segment sa brojem destinacionog porta 80.
Nema dolaznih TCP konekcija osim na javni Web server.	Odbaci sve dolazne TCP SYN segmente osim za IP adresu XXX.XXX.XXX.XXX, port 80
Spriječi da Web radio "proguta" kapacitet linka prema Internetu.	Odbaci sve dolazne UDP segmente osim DNS i *router broadcast*-a.
Spriječi da se interna mreža koristi za *smurf* DoS napad.	Odbaci sve ICMP pakete poslate na "broadcast" adresu (npr. YYY.YYY.YYY.YYY).
Spriječi da interna mreža bude "*tracerouted*"	Odbaci sve odlazne ICMP TTL expired poruke

Access Control List

ACL: tabela pravila, primijenjena "top to bottom" na dolazne paketa: parovi (akcija, uslov) pairs.

akcija	Izvorišna adresa	Adresa destinacije	protokol	Izvorišni port	Odredišni port	flag bit
dozvoliti	222.22/16	van 222.22/16	TCP	> 1023	80	Bilo koji
dozvoliti	van 222.22/16	222.22/16	TCP	80	> 1023	ACK
dozvoliti	222.22/16	van 222.22/16	UDP	> 1023	53	---
dozvoliti	Van mreže 222.22/16	222.22/16	UDP	53	> 1023	----
odbiti	sve	sve	sve	sve	sve	sve

Stateful filtriranje paketa

- prati status svake TCP konekcije
  - Prati uspostavljanje konekcije (SYN) i raskidanje (FIN): utvrđuje da li dolazni i odlazni paketi "imaju smisla"
  - Aktivira *timeout* za neaktivne konekcije na *firewall*-u: ne prihvata nove pakete

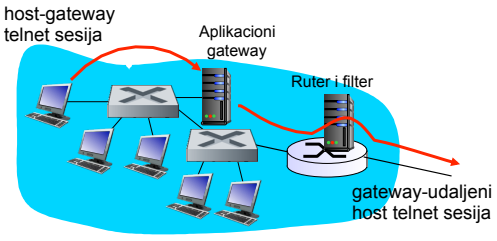
Stateful filtriranje paketa

ACL je proširena da ukazuje na potrebu provjere stanja konekcije prije prihvatanja paketa

akcija	Izvorišna adresa	Adresa destinacije	protokol	Izvorišni port	Odredišni port	flag bit	Provjera veze
dozvoliti	222.22/16	van 222.22/16	TCP	> 1023	80	Bilo koji	
dozvoliti	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	X
dozvoliti	222.22/16	van 222.22/16	UDP	> 1023	53	---	
dozvoliti	Van mreže 222.22/16	222.22/16	UDP	53	> 1023	----	X
odbiti	sve	sve	sve	sve	sve	sve	

Aplikacioni *gateway*

- Filtrira pakete prema sadržaju podataka aplikacija kao i IP/TCP/ UDP polja.
- *Primjer:* dozvoliti odabranim internim korisnicima telnet prema spolja



1. Zahtijeva da svi korisnici telneta moraju proći kroz gateway.
2. Za autorizovane korisnike, gateway uspostavlja telnet konekciju prema destinaciji. Gateway igra ulogu relay-a između svije konekcije.
3. Ruter blokira sve telnet konekcije koje ne potiču od gateway.

Ograničenja firewall-a, gateway-a

- *IP spoofing:* ruter ne može znati da li podaci dolaze od stvarnog izvora
- Ako više aplikacija traži specijalni tretman, svaka mora imati svoj gateway
- Software klijenta mora znati kako da kontaktira gateway.
  - Npr. mora postaviti IP adresu proxy servera u Web pretraživaču
- Filteri obično koriste politiku sve ili ništa prema UDP
- *kompromis:* stepen komunikacije sa svijetom, nivo zaštite
- Mnogi dobro zaštićeni sajtovi su i dalje meta napada

Intrusion detection system (IDS)

- *deep packet inspection:* posmatra sadržaj paketa (npr., upoređuje sadržaj paketa sa bazom sadržaja poznatih virusa)
- Provjerava korelaciju među više paketa
  - Skeniranje portova
  - Mrežno mapiranje
  - DoS napad

Intrusion detection systems

Više IDS-ova: različiti tipovi provjere na različitim lokacijama