

ZAŠTITA MREŽA U INTERNETU (neki aspekti)

Uvod

- ◆ Kao što smo naveli u ORM1, zaštita mrežnih komunikacija je funkcija koja obuhvata praktično sve nivoe protokol steka.
- ◆ Na zaštitu se u ranoj fazi razvoja Interneta (70te i početak 80tih) vrlo malo obraćala pažnja.
- ◆ Sa ogromnim porastom mreže tokom 90tih (pre svega u pogledu korisnika mreže) kao i novim primenama Interneta (napr. Elektronsko poslovanje i bankarstvo), problem zaštite je naglo dobio na značaju.

- ◆ Zato možemo reći da je zaštita mreža u Internetu:
- ◆ (1) veoma važna (zato što informacija u Internetu ima veliku vrednost), i
- ◆ (2) složena (kao što smo rekli obuhvata sve nivoe protokola steka, a osim toga i tehničke detalje operativnog sistema i korišćenih aplikativnih programa).

Zaštita mreže

- ◆ Zaštita mreže (*network security*) i zaštita informacije (*information security*) treba da onemogući neautorizovanom korisniku pristup štićenoj informaciji ili usluzi (*service*).
- ◆ Moraju se štititi i fizički i apstraktni resursi.

Zaštita fizičkih i apstraktnih resursa

- ◆ Fizička zaštita:
 - ◆ (a) magnetnih medijuma
 - ◆ (b) računara
 - ◆ (c) kablova
 - ◆ (d) konvertora protokola
- ◆ Zaštita apstraktnih resursa je složenija i uključuje:
 - ◆ (a) integritet podataka
 - ◆ (b) raspoloživost podataka
 - ◆ (c) privatnost (kripto zaštita)
 - ◆ (d) ograničen pristup info. (npr. samo neka polja sloga)

Potreba za informacionom politikom

- ◆ Organizacija mora da definiše svoju politiku, koja obuhvata sledeća pitanja:
- ◆ (1) kome je dopušten pristup pojedinim delovima informacije,
- ◆ (2) pravila predstavljanja informacije drugima, i
- ◆ (3) kako organizacija reaguje na narušavanje ovih pravila.

Odnos informacionih politika

- ◆ Ponekad informacione politike različitih organizacija mogu biti u suprotnosti.
- ◆ Npr. organizacija A može dati informaciju organizaciji B, ali ne i C. Ako B da informaciju organizaciji C, ona narušava politiku organizacije A.

Mehanizmi za zaštitu

- ◆ Mehanizmi za zaštitu informacije u Internetu se mogu podeliti u tri široka skupa:
- ◆ (1) prvi se fokusira na probleme *autorizacije*, *autentifikacije*, i *integriteta*.
- ◆ (2) drugi se fokusira na problem *privatnosti*, i
- ◆ (3) treći se fokusira na problem *raspoloživosti* kontrolom pristupa.

Mehanizmi autentikacije

- ◆ Autentikacija = verifikacija identifikacije
- ◆ Npr. mnogi serveri odbijaju zahtev ukoliko ne potiče od autorizovanog korisnika.
- ◆ Da bi proverio autorizovanost, server mora znati identitet klijenta.
- ◆ U jednoj, slaboj, varijanti autentifikacije, administrator specificira spisak važećih IP adresa klijenata.
- ◆ Nedostatak ove varijante: lako se zaobilazi u prolaznim konvertorima protokola.
- ◆ Napadač može da imitira autorizovanog klijenta, a isto tako može da imitira i servera.

Pored potrebe za verifikacijom identiteta klijenta postoji i potreba za verifikacijom identiteta servera

- ◆ Klijenti se suočavaju sa istim problemom kao serveri.
- ◆ Npr. u sistemu elektronske pošte, klijent je zadužen da pošalje poštu udaljenom serveru.
- ◆ Ukoliko poruka sadrži osetljivu informaciju, klijent treba da verifikuje da zaista komunicira sa serverom kom je poruka namenjena.

Simetrični krypto system

- ◆ Korišćeni termini:
- ◆ Izvorni tekst (plaintext) P
- ◆ Ključ (key) k je parametar procesa šifrovanja
- ◆ Šifrovani tekst (cyphertext) C
- ◆ Metod šifrovanja (Encryption method) E
- ◆ Metod dešifrovanja (Decryption method) D
- ◆ Važi: $C = E_k(P)$, $P = D_k(C)$
E i D su matematičke funkcije koje imaju dva ulazna parametra: izvorni tekst (u slučaju E) odnosno šifrovani tekst (u slučaju D) i ključ

- ◆ Kriptoanaliza je oblast koja se bavi razbijanjem šifarskih metoda
- ◆ Nauka koja se bavi metodama šifrovanja (obuhvata pored ostalog i kriptoanalizu) je kriptologija
- ◆ Važno pravilo je da su metodi E i D javni, a k je tajni (Kerckhoff-ovo pravilo)
- ◆ Mnogo puta se pokazalo da se pokušaj da se E i D drže u tajnosti ne isplati (security by obscurity)
- ◆ Tako da se podrazumeva da kriptoanalitičar poznaje E i D

- ◆ U načelu se može reći da za dati E, vreme za razbijanje C pretragom prostora ključeva eksponencijalno zavisi od dužine ključa
- ◆ Dužina ključa se izražava u bitima

Kripto sistem javnog ključa (asimetrični)

- ◆ Jedan oblik poverljive usluge je kripto sistem javnog ključa (public key encryption system).
- ◆ Svaki učesnik dobija dva ključa:
 - ◆ (a) javni (public)
 - ◆ (b) tajni (secret)
- ◆ Zaštićen prenos poruke obezbeđuje sledeća procedura:
 - ◆ (1) pošiljalac šifruje poruku svojim tajnim ključem
 - ◆ (2) primalac dešifruje poruku javnim ključem pošiljaoca
- ◆ U gornjem slučaju oba učesnika mogu biti sigurni da je drugi učesnik autentičan.

Mehanizmi privatnosti

- ◆ Šifrovanje može da reši i problem privatnosti.
- ◆ Ako je poruka namenjena samo jednom primaocu:
- ◆ (1) pošiljalac šifruje poruku javnim ključem primaoca
- ◆ (2) primalac dešifruje poruku svojim tajnim ključem
- ◆ Da bi se autentifikovao pošiljalac a istovremeno obezbedila i privatnost, poruka se šifruje 2 puta:
- ◆ (1) pošiljalac prvo šifruje poruku svojim tajnim ključem, a zatim primaocčevim javnim ključem
- ◆ (2) primalac prvo primenjuje svoj tajni ključ, a zatim javni ključ pošiljaoca.

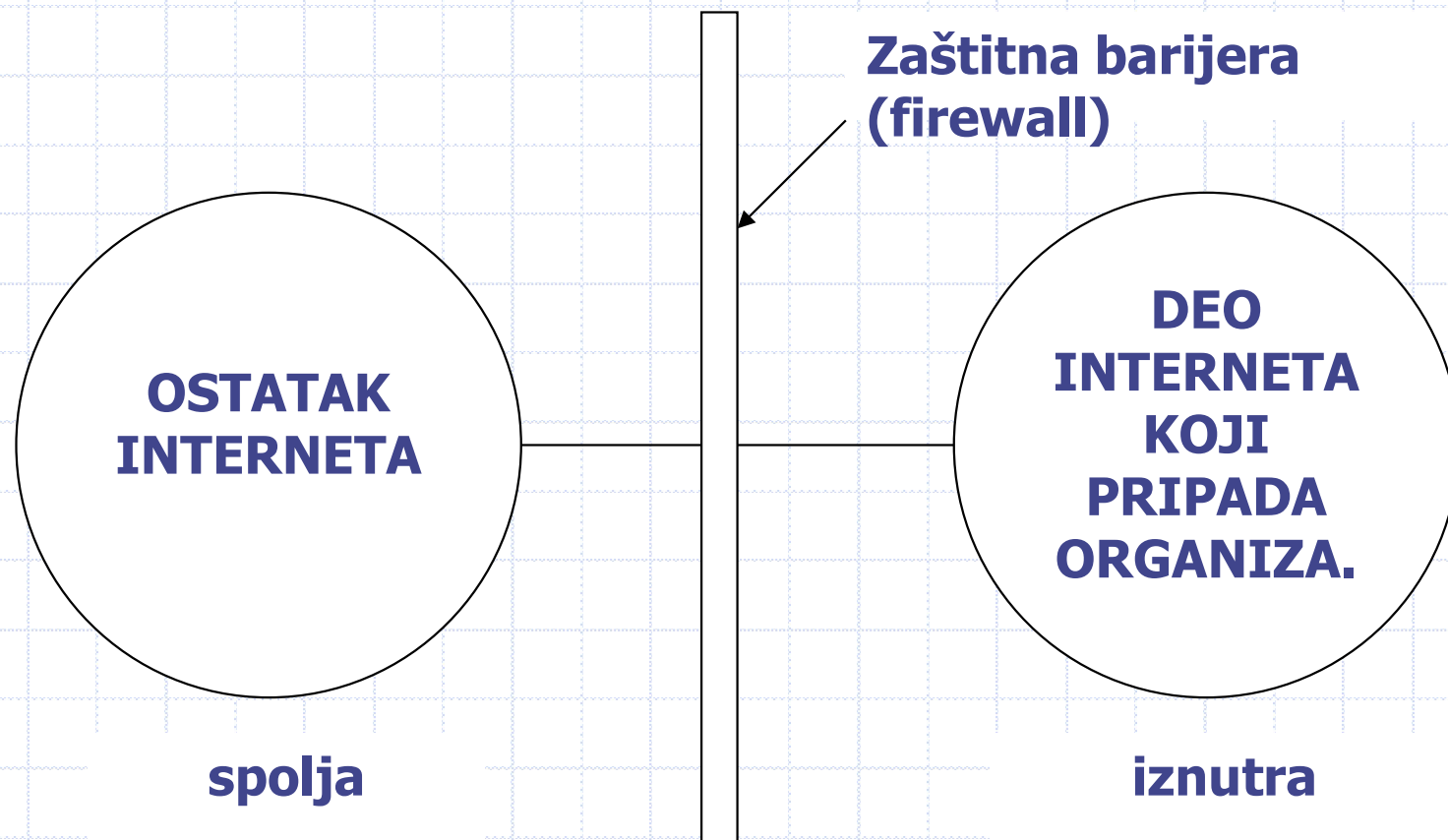
- ◆ Kripto sistem javnog ključa rešava neke važne probleme, ali da bi uspešno funkcionisao u praksi, potrebno je rešiti problem infrastrukture – odnosno kako da dve strane sigurno razmene javne ključeve.
- ◆ U protivnom napadač se može postaviti u komunikaciji između dve strane i proslediti svoj javni ključ strani A, dekriptovati saobraćaj od A svojim tajnim ključem i enkriptovati javnim ključem B.
- ◆ Čega dve strane A i B nisu svesne.

- ◆ Zato su razvijeni sistemi infrastrukture Public Key Infrastructure (PKI)
- ◆ Ovi sistemi omogućuju da se kroz sertifikat veže javni ključ za ime korisnika.
- ◆ Kada se desi da neki par javni/tajni ključ više nije siguran (napr. razbijen tajni ključ) potrebno je izvršiti opoziv sertifikata.

Zaštitne barijere (firewall) i pristup Internetu


- ◆ Jedan aspekt zaštite mreže u Internet okruženju je kontrola saobraćaja između mreže i javnog Interneta, tj. sprečavanje neželjenih komunikacija.
- ◆ To se realizuje kroz:
 - ◆ (1) ograničenja na mrežne topologije,
 - ◆ (2) postavljanje međustepena za prihvatanje-odašiljanje informacije, i
 - ◆ (3) filtriranje paketa.
- ◆ Ovo obezbeđuje tzv. *zaštitna barijera (firewall)*.

Koncept zaštitne barijere



Višestruke veze i njeni najslabiji delovi

- ◆ Velike organizacije mogu imati više mreža.
- ◆ Te mreže se priključuju na Internet preko više zaštitnih barijera.
- ◆ Sve ove zaštitne barijere moraju koristiti identična ograničenja pristupa.
- ◆ Aksiom "najslabije karike u lancu" (eng. "weakest link axiom"): Sistem je zaštićen u meri u kojoj je zaštićen njegov "najslabiji deo".

- 
- ◆ Aksiom najslabije karike je jedan od osnovnih i važi uvek kada zaštita nekog objekta (u ovom slučaju mreže) ima više paralelnih segmenata (paralelnih komunikacionih puteva sa okruženjem).

Realizacija zaštitne barijere

- ◆ Teorijski, zaštitna barijera blokira neželjenu komunikaciju između računara unutar organizacije i spolja.
- ◆ U praksi, detalji zavise od:
 - ◆ (1) mrežne tehnologije
 - ◆ (2) kapaciteta veze
 - ◆ (3) saobraćaja
 - ◆ (4) politike organizacije

Realizacija barijere zahteva fizičke komponente velike brzine

- ◆ U zavisnosti od veličine štićene mreže i količine saobraćaja, može biti potrebna velika procesorska snaga.
- ◆ Datagrami se moraju pregledati brzinom koja dopušta potpuno iskorišćenje veze sa Internetom.
- ◆ Datagrami ne smeju biti zakašnjeni da ne bi došlo do nepotrebnih ponovnih slanja istih datagrama (retransmisija).
- ◆ Današnje barijere poseduju mehanizme brzog filtriranja datagrama.

Filtri na nivou paketa

- ◆ Filtri paketa omogućavaju filtriranje (tj. blokiranje) određenih paketa.
- ◆ Npr. svih paketa koji dolaze sa određene adrese, ili paketa koje koristi određena aplikacija.
- ◆ Sledi primer specifikacije filtara. U primeru, konvertor protokola koji filtrira paketa povezuje zaštićenu mrežu sa ostatkom Interneta.

Primer specifikacije filtara datagrama

(Priključak br. 1 se povezuje na zaštićenu mrežu, a priključak br. 2 na ostatak Interneta.)

Paket stiže na priklj.	IP adr. izvora	IP adr. odredi .	Protokol	Prolaz izvora	Prolaz odredi .	Aplikaci.
2	*	*	TCP	*	21	FTP
2	*	*	TCP	*	23	TELNET
1	128.5.*.*	*	TCP	*	25	E-MAIL
2	*	*	UDP	*	43	WHOIS
2	*	*	UDP	*	69	TFTP
2	*	*	TCP	*	79	FINGER

Način specifikacije filtara paketa

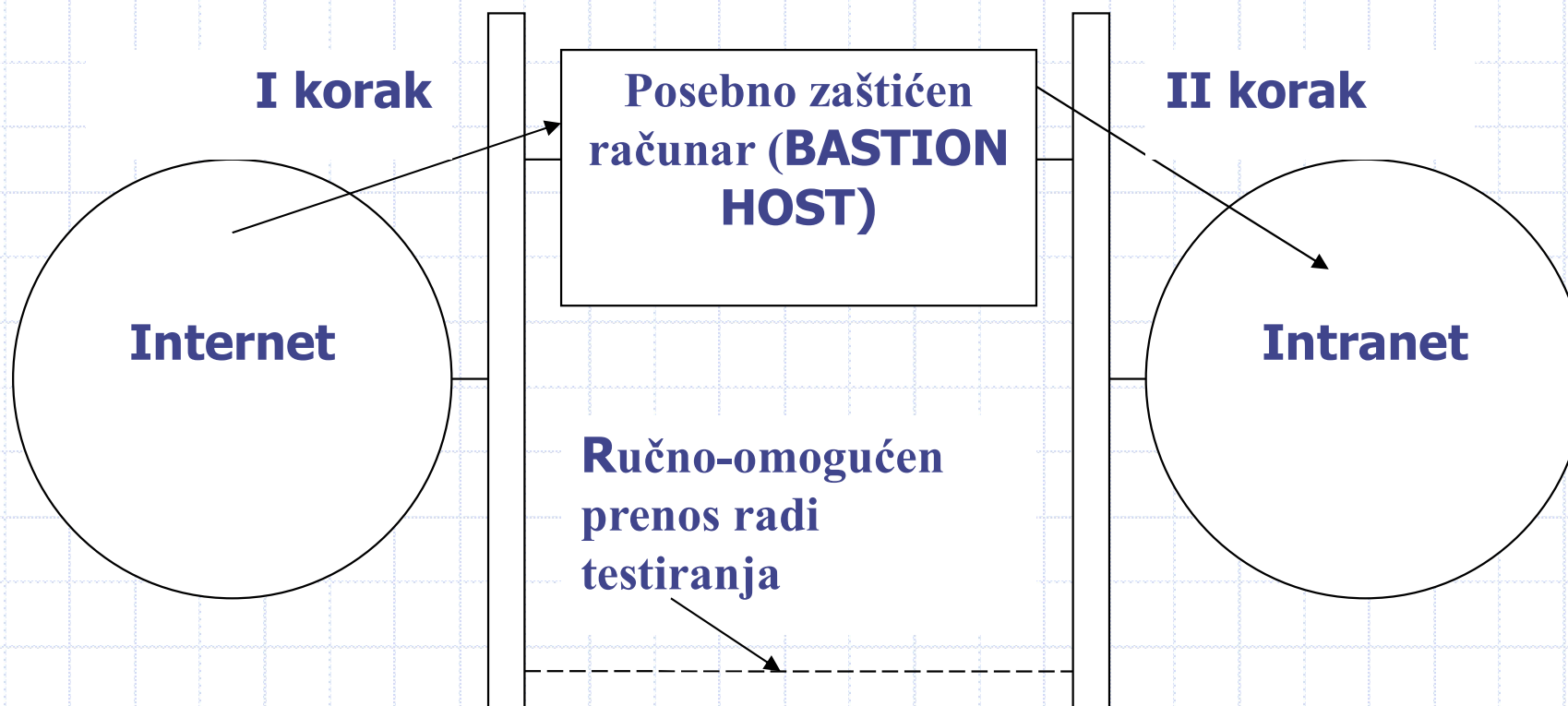
- ◆ Gornja šema specifikacije se pokazala kao nepraktična.
- ◆ Zato se primenjuje obrnut pristup: umesto specifikacije saobraćaja koji treba blokirati, specificira se deo saobraćaja koji je dopušten.

Pristup uslugama kroz zaštitnu barijeru

- ◆ Siguran pristup spoljnim uslugama moguć je samo kroz posebno zaštićen računar – “BASTION HOST”.
- ◆ U ovom pristupu formiraju se dve barijere:
- ◆ (1) spoljnja, koja blokira sav saobraćaj osim:
 - ◆ (a) datagrama čije odredište su serveri na zaštićenom računaru, i
 - ◆ (b) datagrame za klijente na zaštićenom računaru.
- ◆ (2) unutrašnja, koja blokira sav saobraćaj, osim datagrama koji potiču sa zaštićenog računara.
- ◆ Sledi ilustracija ovog koncepta.

Ilustracija uloge zaštićenog računara

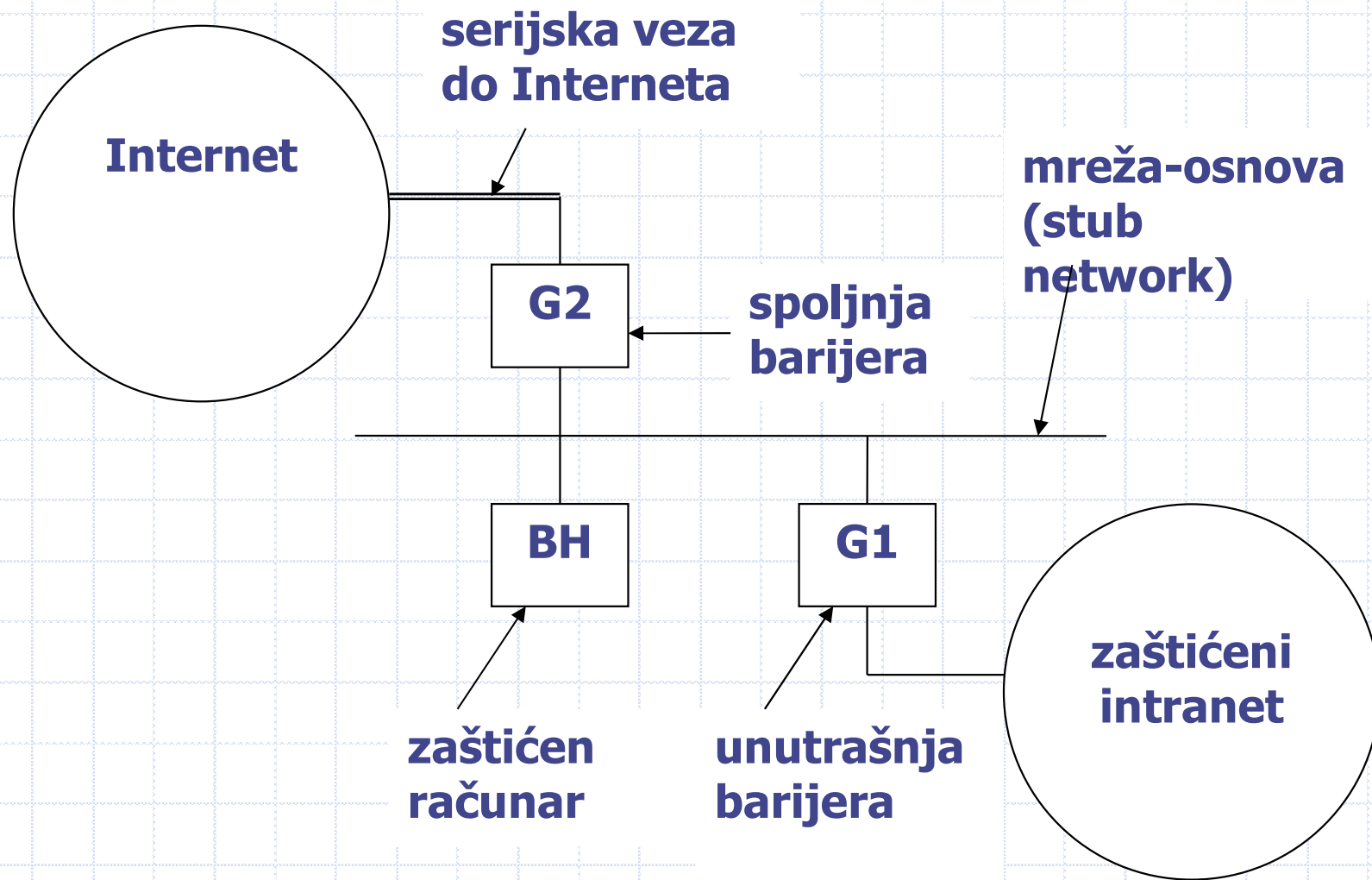
(Npr. prenos datoteke ide u 2 koraka: (a) Internet -> BastionHost i
(b) Bastion Host -> Intranet)



Detalji arhitekture zaštitnih barijera

- ◆ Unutrašnja i spoljna barijera se realizuju sa dva odvojena konvertora protokola, G1 i G2.
- ◆ Mreža koja povezuje intranet i Internet sa posebno zaštićenim računarom naziva se mreža-osnova (stub network).
- ◆ Sledi ilustracija.

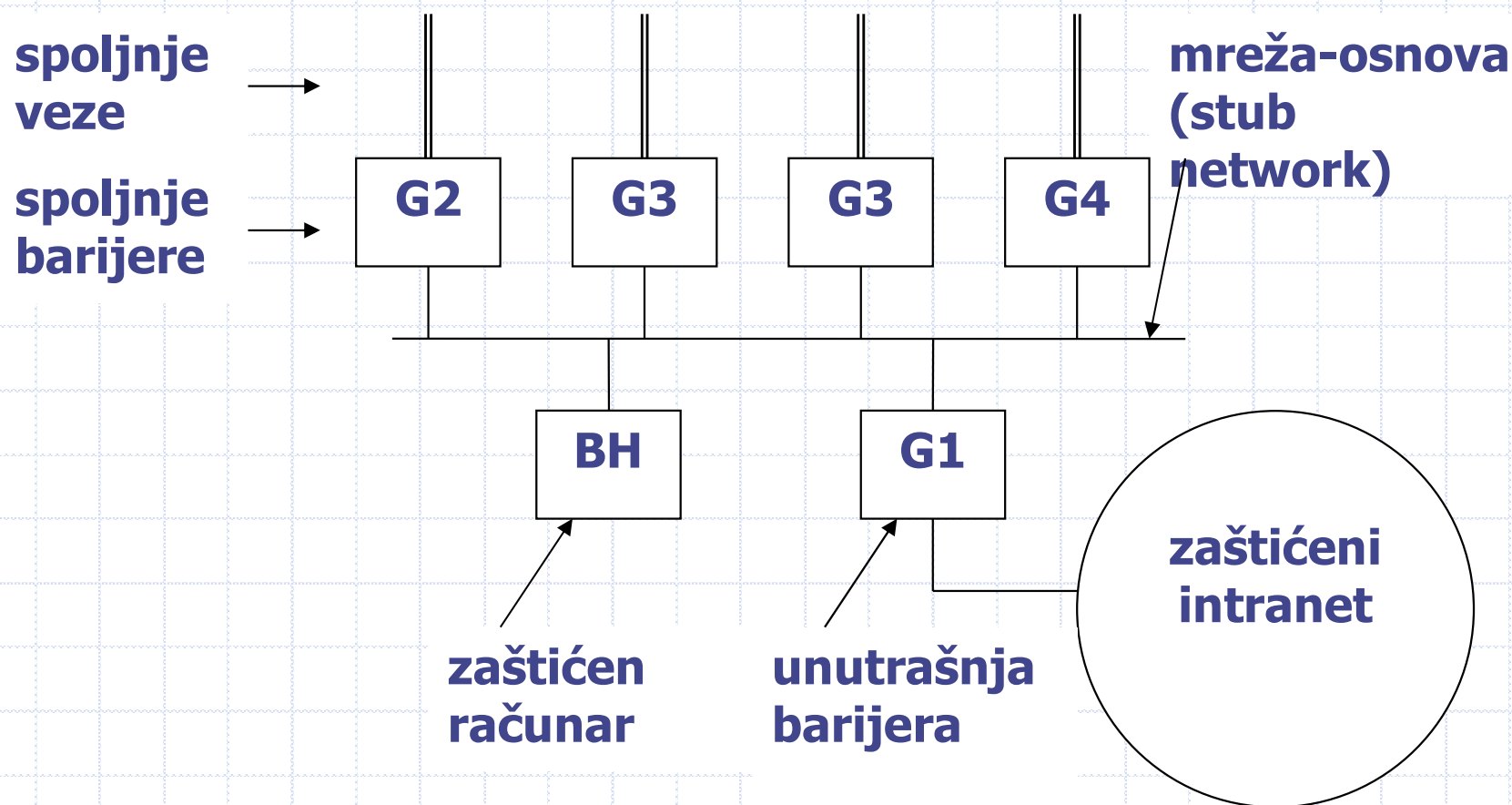
Ilustracija detalja arhitekture meže-osnove (stub network)



Arhitektura zaštitnih barijera za pristup ka više mreža


- ◆ Da bi se sprečio neželjeni tok podataka između spoljnjih lokaliteta (sajtova), nužno je napraviti mrežu-osnovu sa po jednim konvertormom protokola za svaku spoljnju vezu.
- ◆ Mreža-osnova, u tom slučaju, povezuje posebno zaštićen računar sa intranetom i drugim udaljenim lokalitetima.
- ◆ Jedna od spoljnjih veza može da vodi i do ISP-a.
- ◆ Sledi ilustracija.

Zaštitne barije prema više mreža



Vrste zaštitnih barijera

- ◆ Paketski filter – poredi svojstva paketa (adrese, prolaze, protokol) sa listom pravila i na osnovu pravila odlučuje da li se paket propušta ili odbacuje
- ◆ Barijera na nivou sesije – circuit level firewall. Prati TCP uspostavu veze i filtrira ne individualne pakete, već TCP veze
- ◆ Barijera na aplikativnom nivou – application level gateway firewall – na pr. Web zastupnik sa barijerom

- 
- ◆ Transparentna barijera – radi na L2 i ne predstavlja mrežni hop za povezane uređaje. Ipak ima uobičajene provere paketa.
 - ◆ Personalna barijera

Kako radi barijera sa pamćenjem stanja veze ?

- ◆ Prati TCP saobraćaj i kada detektuje da je prošla uspostava u tri koraka, dodaje pravilo koje propušta saobraćaj na toj TCP vezi
- ◆ Kada detektuje FIN segment ili nakon isteka vremenske kontrole, briše dato pravilo

Ponašanje mrežne barijere

- ◆ Za pakete koje odbacuje, barijera ima dve mogućnosti:
 - Da ih odbije, šaljući TCP RST ili ICMP port unreachable
 - Da ih samo tiho odbaci, u kom slučaju pošiljalac ne zna šta se desilo sa paketom

Dodatne opcione funkcije mrežne barijere

- ◆ Usmeravanje
- ◆ NAT
- ◆ VPN čvor
- ◆ AAA (Authentication, Authorization, Accounting)
- ◆ Deep packet inspection
- ◆ Integracija sa IPS

Primer mrežne barijere

- ◆ Iptables – barijera za linux OS
- ◆ Iptables je program u korisničkom prostoru linux OS, koji omogućuje da se konfiguriraju pravila filtriranja mrežne barijere u jezgru linux OS

Primeri komandi za iptables

- ◆ Iptables -L
- ◆ Izlistava pravila

- ◆ Iptables -A OUTPUT -p tcp -d 192.168.30.0/24 – dport 25 -j ACCEPT
- ◆ Dozvoljava izlazni TCP saobraćaj za datu mrežnu adresu i određeni prolaz

- ◆ iptables -A INPUT -i eth0 -s 203.0.170.70 -j DROP
- ◆ Zabranjuje dolazni saobraćaj sa date adrese

- ◆ `iptables -A INPUT -p tcp --dport 52005 -m iprange --src-range ADDR1-ADDR2 -j ACCEPT`
- ◆ Dozvoljava dolazni TCP saobraćaj ka portu 52005 sa zadatog opsega IP adresa od ADDR1 do ADDR2

- 
- ◆ Iptables -D INPUT 5
 - ◆ Brisanje 5. pravila za dolazni saobraćaj



◆ Ip6tables je za IPv6

Zaštita na mrežnom nivou steka

- ◆ IP security (IPsec) je radni okvir (framework) za primenu više različitih algoritama i usluga zaštite.
- ◆ Iako je na nivou IP protokola, orijentisan je na uspostavu veze (jer se i zaštita obično odnosi na pojedine veze za koje se definiše ključ). U IPsec se veze nazivaju Security Associations (SA).
- ◆ Za rad sa ključevima IPsec koristi Internet Key Exchange (IKE) protokol.

- ◆ IPsec ima dva režima:
- ◆ Transportni - u kom se dodaje novo zaglavlje odmah iza standardnog IP zaglavlja
- ◆ Tunelski – u kom se ceo datagram enkapsulira. Objašnjeno u predavanju o VPN gde se ovaj režim inače i koristi.

Zaštita web saobraćaja

- ◆ Sredinom 90-tih se pojavio The Secure Sockets Layer (SSL) – protokol za uspostavljanje zaštićenih veza u web saobraćaju
- ◆ U protokol steku se nalazi između transportnog i aplikativnog nivoa
- ◆ Kada HTTP koristi SSL, naziva se HTTPS (Secure HTTP) i obično koristi port 443
- ◆ Može da koristi različite kriptografske algoritme. U najjačoj varijanti koristi trostruki DES sa tri različita ključa.

- ◆ SSL ima dva dela: uspostavljanje i korišćenje sigurne veze.
- ◆ Uspostavljanje: A (web klijent) šalje zahtev za uspostavljanje sigurne veze.
- ◆ Tokom razmene poruke A autentifikuje B korišćenjem njegovog javnog ključa, a B autentifikuje A najčešće korišćenjem korisničkog imena i lozinke.
- ◆ Takođe A izgeneriše premaster ključ i pošalje ga B šifrujući ga njegovim javnim ključem. Iz premaster ključa obe strane naknadno izračunavaju ključ sesije koji će se dalje koristiti za šifrovanje komunikacije.

- ◆ Najšire korišćena je verzija 3 SSL.
- ◆ Krajem 90-tih se pojavio Transport Layer Security (TLS), koji je IETF standard i koji zamenjuje SSL.
- ◆ TLS je opisan u posebnoj prezentaciji
- ◆ Najčešće web pregledači podržavaju oba, kod HTTP/1.1 pokušavaju prvo da uspostave zaštićenu vezu korišćenjem TLS, i ako ne uspe, prelaze na SSL (to se naziva SSL/TLS).

Intrusion

- ◆ skup akcija sa ciljem narušavanja integriteta, poverljivosti ili dostupnosti resursa

Intrusion detection system

- ◆ sistem čiji je cilj da otkrije da li se u nadziranom računarskom sistemu dogodio, ili se možda događa, ili će se možda dogoditi napad
- ◆ Uočavaju se dve dvrste ovih sistema: host IDS i network IDS.
- ◆ HIDS nadzire jedan računar praćenjem sistemskih zapisa (pristup sistemskim resursima od strane pojedinih procesa itd), a NIDS nadzire mrežu analizom saobraćaja.

Poređenje HIDS i NIDS sistema

◆ Prednosti NIDS:

- Ne zahtevaju promene na računarima u mreži koju štite (HIDS se instalira na računaru koji štiti)
- Otkazi na računarima u mreži koja se štiti ne utiču na NIDS

◆ Prednosti HIDS:

- Imaju pristup detaljnijim informacijama nego NIDS
- Niži nivo lažnih alarma nego NIDS

◆ I jedni i drugi imaju problem sa opsegom vidljivosti (visibility scope). Tako NIDS u komutiranom Eternetu vide samo saobraćaj na segmentu mreže na kom se nalaze.

◆ NIDS takođe imaju problem sa saobraćajem koji je enkriptovan i sa velikom brzinom saobraćaja u savremenim mrežama.

Podela prema metodi detekcije

- ◆ Metoda zasnovana na potpisima
- ◆ Metoda zasnovana na detekciji anomalija

Metoda zasnovana na potpisima (signaturama)

- ◆ IDS sadrži bazu potpisa i pretražuje mrežne pakete (u slučaju NIDS) i traži poklapanje njihovog sadržaja sa nekim od potpisa iz baze.
- ◆ Osnovno ograničenje je što ne prepoznaju nove vrste napada – za svaki napad je potrebno da postoji potpis u bazi.
- ◆ Kod NIDS je potrebno da analizira i sadržaj informacionog dela paketa (Deep Packet Inspection).
- ◆ Važno je korišćenje brzih algoritama za poređenje stringova, da NIDS ne bi izgubio korak sa saobraćajem na mreži.

snort

- ◆ Open source NIDS koji koristi potpise
- ◆ U širokoj upotrebi već desetak godina

Metoda zasnovana na detekciji anomalija

- ◆ Ova metoda pretpostavlja formiranje modela normalnog ponašanja sistema, da bi IDS detektovao odstupanje od toga.
- ◆ Stoga obično zahtevaju fazu treninga – formiranja modela normalnog ponašanja
- ◆ Otvoreno pitanje je izbor parametara funkcionisanja nadziranog sistema koji se prate, kao i metrika za detekciju odstupanja.
- ◆ Ove metoda obično ima viši nivo lažnih alarma nego metoda zasnovana na potpisima.

Intrusion Prevention Systems (IPS)

- ◆ Za razliku od IDS, uključuju i reakciju na napad koji je detektovan
- ◆ Analogno kao kod IDS, postoje IPS koji štite računar (HIPS), i oni koji štite mrežu (NIPS)

Napadi odbijanjem usluge (DoS)

- ◆ Denial-of-Service napadi predstavljaju ozbiljan problem u Internet okruženju, naročito pogađaju poslovanje preko Interneta
- ◆ Cilj ovih napada je da prekinu ili značajno uspore funkcionisanje Internet poslužioca (najčešće web sajta, ali može biti u pitanju i DNS, pošta...) koji je meta napada
- ◆ Ovi napadi se mogu realizovati na različitim nivoima protokol steka

Neke vrste DoS napada

- ◆ Uočavaju se napadi na propusni opseg (bandwidth attacks), kod kojih se smanjuje mrežna dostupnost Internet poslužioca koji je meta napada
- ◆ Takođe se uočavaju i napadi iscrpljivanjem resursa (resource starvation attacks).

Napadi iscrpljivanjem resursa

- ◆ Primer su XML dokumenti koji sadrže duboko ugnježdene šeme – u tom slučaju radi se o DoS napadu na aplikativnom nivou
- ◆ Varijanta ovog tipa napada je kada računari šalju veliki broj paketa koji zahtevaju izvršenje kriptografskih operacija (koje su obično vrlo zahtevne po pitanju potrebnih resursa) – primer je u WiMAX mrežama, gde je moguć ovakav napad na MAC podnivou 2. nivoa, slanjem niza paketa koji zahtevaju autentikaciju

DDoS

- ◆ DoS napadi se vrlo često realizuju kao distribuirani (DDoS) napadi.
- ◆ U tom slučaju postoji skup n napadača, $n > 1$
- ◆ Obično su napadači računari koji su povezani na Internet a putem rač. virusa ili nekog drugog zlonamernog programa su dospeli pod kontrolu organizatora napada. Takvi računari učestvuju u napadu bez znanja njihovih legitimnih vlasnika. Nazivaju se zombi računari (zombies).

Refleksija (reflected DDoS)

- ◆ Kod ovakvih napada, računari koji učestvuju u napadu šalju pakete podataka ka računaru reflektoru (koji nije pod kontrolom napadača).
- ◆ Pri tom su podaci o izvoru paketa falsifikovani (spoofed source address), i postavljeni tako da ukazuju na metu napada.
- ◆ Reflektor šalje pakete odgovora ka meti napada i opterećuje mrežne resurse na putanji ka meti.

Preplavljanje SYN paketima (SYN Flood)

- ◆ Jedan od najpoznatijih DDoS napada.
- ◆ Napadači započinju uspostavljanje TCP veza (3 way handshake), ali pri tom ne realizuju sekvencu otvaranja do kraja (ne šalju ACK na SYN ACK koji stigne od servera).
- ◆ Na taj način resursi koje server zauzima za otvaranje TCP veze ostaju zauzeti i nagomilavaju se i tako se smanjuje radni kapacitet servera.

Amplification attacks

- ◆ Zasnovan na korišćenju adrese za difuznu emisiju (broadcast). Primeri:
- ◆ smurf napad – slanjem ICMP echo request paketa na broadcast adresu. Adresa izvorišta je pri tom lažno postavljena i pokazuje na metu napada.
- ◆ Fraggle napad – slično kao smurf, samo koristi UDP echo umesto ICMP echo.


Prevenција i odbrana od DoS

- ◆ Tradicionalne metode se oslanjaju na mrežne barijere, IPS sisteme, usmerivače i razne druge sisteme koji filtriraju saobraćaj
- ◆ Novije metode se oslanjaju na kriptografske puzle, kojima se pravi balans između opterećenja na klijentu i serveru – klijent da bi započeo izvršenje usluge na serveru mora da reši zadatak (puzle) koje su računski zahtevne.
- ◆ Čak i ovaj metod nije dovoljno uspešan kod napadača koji imaju na raspolaganju veliki distribuirani sistem za lansiranje napada, jer takav napadač mnogo brže rešava zadatak nego prosečan klijent.

Ransomware

- ◆ Napadač instalira na napadnuti računar program koji enkriptuje deo sistema datoteka na tom računaru, i tako onemogućuje njegovo korišćenje od strane legitimnog vlasnika.
- ◆ Napadač ucenjuje legitimnog vlasnika i traži otkup da bi dekriptovao sistem datoteka

- ◆ d – datoteka
- ◆ $\{d\}_k$ – datoteka šifrovana simetričnim algoritmom sa ključem k (koristi se simetrični algoritam zbog brzine)
- ◆ Napadač generiše par ključeva ($\text{pri}(\text{RM})$, $\text{pub}(\text{RM})$) kojima šifruje k . RM – računar meta
- ◆ $\{k\}_{\text{pub}(\text{RM})}$ – šifrovani ključ
- ◆ Privatni ključ $\text{pri}(\text{RM})$, koji je potreban za dešifrovanje k , se šifruje javnim ključem napadača $\text{pub}(N)$
- ◆ $\{\text{pri}(\text{RM})\}_{\text{pub}(N)}$

- 
- ◆ Napadač tipično radi eksfiltraciju dela sadržaja sistema datoteka napadnutog računara, sa ciljem učenjivanja legitimnog vlasnika računara sa objavljivanjem tog sadržaja, kao i sa ciljem dalje prodaje tog sadržaja

Homomorfna enkripcija

- ◆ Osnovni mehanizam zaštite podataka u današnjim računarskim mrežama je enkripcija
- ◆ U novije vreme, primene kao što su računarstvo u oblaku ili elektronsko glasanje su pojačale interes za homomorfnu enkripciju
- ◆ Problem kod tradicionalne enkripcije je da u potpunosti sprečava pristup podacima, što je vrlo nefleksibilno
- ◆ Za brojne primene je potrebno omogućiti da se izvrši neka operacija nad podacima ali da se oni pri tom ne dekriptuju

- ◆ Homomorfna enkripcija je vrsta enkripcije koja omogućava da se obrađuje kriptovani sadržaj, bez dekripcije (bez poznavanja ključa)
- ◆ Današnje homomorfne šeme podržavaju najčešće jednu operaciju
- ◆ Primer: aditivna šema koja omogućuje sabiranje glasova kod elektronskog glasanja. $C_i = \text{Enc}(M_i)$ su enkriptovani glasovi. Brojanje se vrši korišćenjem homomorfne enkripcije i dobija se $C = \text{Enc}(M_1 + \dots + M_n)$. Rezultat može da dekriptuje samo nadležno telo.

- ◆ Potpuno homomorfna šema bi omogućila enkriptovani upit na Internet pretraživaču pri čemu bi pretraživač izvršio upit bez da ga dekriptuje.