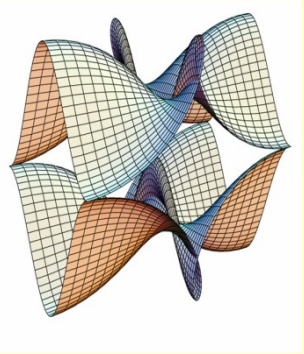
Sveučilište u Zagrebu
PMF – Matematički odsjek

MREŽE RAČUNALA
Predavanja 2022/2023



Poglavlje 25: Sigurnost u mrežama

Sastavio: Robert Manger
12.01.2015

Sigurna mreža i sigurnosna politika (1)

- Što je to *sigurna mreža*? Postoje razne definicije, na primjer:
  - To je mreža koja ne dopušta osobama izvana da pristupe računalima unutar naše organizacije.
  - To je mreža koja sprečava osobama izvana da mijenjaju informacije na web stranicama naše organizacije.
  - To je mreža koja osigurava povjerljivost komuniciranja, na primjer da e-mail poruku ne može čitati nitko osim pošiljatelja i primatelja.

Sigurna mreža i sigurnosna politika (2)

- Budući da nema jednoznačne definicije sigurne mreže, svaka organizacija mora definirati svoju *sigurnosnu politiku* (što treba dozvoliti, što treba spriječiti).
- Kod definiranja sigurnosne politike potrebno je naći kompromis između sigurnosti, jednostavnosti i cijene korištenja mreže.
- Treba odlučiti koji aspekti sigurnosti su za dotičnu organizaciju najvažniji, a koji se eventualno mogu zanemariti.

Neki aspekti sigurnosti

- *Integritet podataka*. Da li primatelj zaista dobiva podatke koje je poslao pošiljatelj, ili ih je netko putem promijenio?
- *Dostupnost podataka*. Da li ovlašteni korisnici mogu doći do podataka, ili ih netko u tome ometa?
- *Povjerljivost podataka*. Da li su podaci koji putuju mrežom zaštićeni od neovlaštenog čitanja?
- *Autentičnost podataka*. Da li podaci koje je dobio primatelj zaista potječu od navedenog pošiljatelja?

Čuvanje integriteta pomoću kriptiranja

- Tehnike za zaštitu podataka od slučajnog oštećenja (npr. kontrolni zbrojevi) ne osiguravaju integritet.
- Ako napadač namjerno mijenja podatke koji prolaze mrežom, on će također promijeniti i kontrolni zbroj.
- Zaštita od zlonamjernog mijenjanja podataka zasniva se na *kriptografskoj hash funkciji* i tajnom ključu koji je poznat samo pošiljatelju i primatelju.
- Pošiljatelj na osnovi sadržaja poruke i ključa računa vrijednost *H* hash funkcije i šalje je uz poruku.
- Primatelj ponavlja isti račun i provjerava da li je dobio istu vrijednost *H*.
- Napadač koji pokušava promijeniti poruku ne može na ispravan način promijeniti i *H* jer ne zna ključ.

Čuvanje dostupnosti pomoću lozinki

- Dostupnost podataka osigurava se tako da se neovlaštenim korisnicima spriječi nepotrebno zauzimanje računalnih ili mrežnih resursa.
- Jedan način zaustavljanja neovlaštenih korisnika je uvođenje lozinki za pristup resursima.
- Ako uvedemo lozinke, onda moramo paziti da se one ne šalju po mreži u nezaštićenom obliku, pogotovo ako je riječ o bežičnoj mreži.
- Npr, ako se korisnik prijavljuje za rad na drugom računalu pomoću Telnet, tada svatko tko prisluškuje promet na mreži može doznati njegovu lozinku.
- Danas postoje protokoli koji prenose lozinke u kriptiranom obliku, npr ssh umjesto Telnet.

Čuvanje povjerljivosti pomoću kriptiranja (1)

- Zaštita od neovlaštenog čitanja podataka koji putuju mrežom postiže se kriptiranjem.
- Neke od tehnologija za kriptiranje zasnivaju se na tajnom ključu koji znaju samo pošiljatelj i primatelj.
- Pošiljatelj koristi ključ da bi stvorio kriptiranu poruku koja putuje mrežom.
- Primatelj koristi isti ključ da bi dekriptirao primljenu poruku.
- Napadač koji prisluškuje komunikaciju ne zna ključ pa ne može izvući nikakvu informaciju iz kriptirane poruke.

Čuvanje povjerljivosti pomoću kriptiranja (2)

- Neka je *K* ključ, *M* poruka, a *E* kriptirana poruka. Cijeli postupak može se interpretirati kao primjena dviju funkcija *encrypt*( ) i *decrypt*( ):

  $E = encrypt\ (K, M)$,

  $M = decrypt\ (K, E)$.

- Druga funkcija je inverz prve funkcije:

  $M = decrypt\ (K, encrypt\ (K, M))$.

- Snaga opisane zaštite zasniva se na matematičkim svojstvima funkcije za kriptiranje.
- Pogađanje *M* na osnovi *E* bez znanja *K* predstavlja zadatak koji je suviše složen u računskom smislu.

Kriptiranje javnim ključem (1)

- Novije tehnologije za kriptiranje zasnivaju se na tome da se svakom korisniku pridruže dva ključa.
- Prvi ključ korisnik čuva kao svoju tajnu, a drugog objavljuje zajedno sa svojim imenom i prezimenom.
- Javni i tajni ključevi opet omogućuju povjerljivu komunikaciju.
- Bilo tko može pomoću javnog ključa *public_u1* određenog korisnika *u1* kriptirati svoju poruku, te ju poslati korisniku *u1*.
- Jedino korisnik *u1* može pomoću svog tajnog ključa *private_u1* dekriptirati poruku i saznati njen sadržaj.

Kriptiranje javnim ključem (2)

- Dakle sve zajedno izgleda ovako:

  M = *decrypt* (*private_u1*, *encrypt* (*public_u1*, *M*)) .
- Prednost korištenja javnog ključa je u tome što nema potrebe da pošiljatelj i primatelj razmjenjuju tajni ključ preko nesigurnog komunikacijskog kanala.
- Objavljivanje javnog ključa ne predstavlja sigurnosni rizik zahvaljujući matematičkim svojstvima korištenih funkcija.
- Naime, pronalaženje tajnog ključa na osnovi poznatog javnog ključa predstavlja zadatak koji je suviše složen u računskom smislu.

Osiguranje autentičnosti pomoću digitalnog potpisa

- Kriptiranje s dva ključa može se koristiti i u obratnom smjeru. Poruka kriptirana pomoću tajnog ključa može se dekriptirati pomoću pripadnog javnog ključa:

  $M = decrypt\ (public\_u1, encrypt\ (private\_u1, M)\ )$.

- Ovaj mehanizam služi za autentikaciju poruke i naziva se *digitalni potpis*.
- Da bi "potpisao" poruku, pošiljatelj je kriptira pomoću svog tajnog ključa. Primatelj dekriptira poruku pomoću pošiljateljevog javnog ključa.
- Primatelj je siguran da poruka zaista potječe od dotičnog pošiljatelja. Naime jedino taj pošiljatelj zna tajni ključ koji odgovara upotrebljenom javnom ključu.

Istovremeno osiguranje autentičnosti i povjerljivosti (1)

- Da bi se osigurala i autentičnost i povjerljivost, postupak kriptiranja potrebno je provesti dvaput.
- Poruka se najprije “potpisuje” kriptiranjem pomoću pošiljateljevog tajnog ključa *private_u1*. Takva kriptirana poruka se ponovo kriptira pomoću primateljevog javnog ključa *public_u2*:

  $X = encrypt(public\_u2, encrypt(private\_u1, M))$.
- Primatelj najprije dekriptira poruku pomoću svog tajnog ključa *private_u2*, a zatim je još jednom dekriptira pomoću pošiljateljevog javnog ključa *public_u1*:

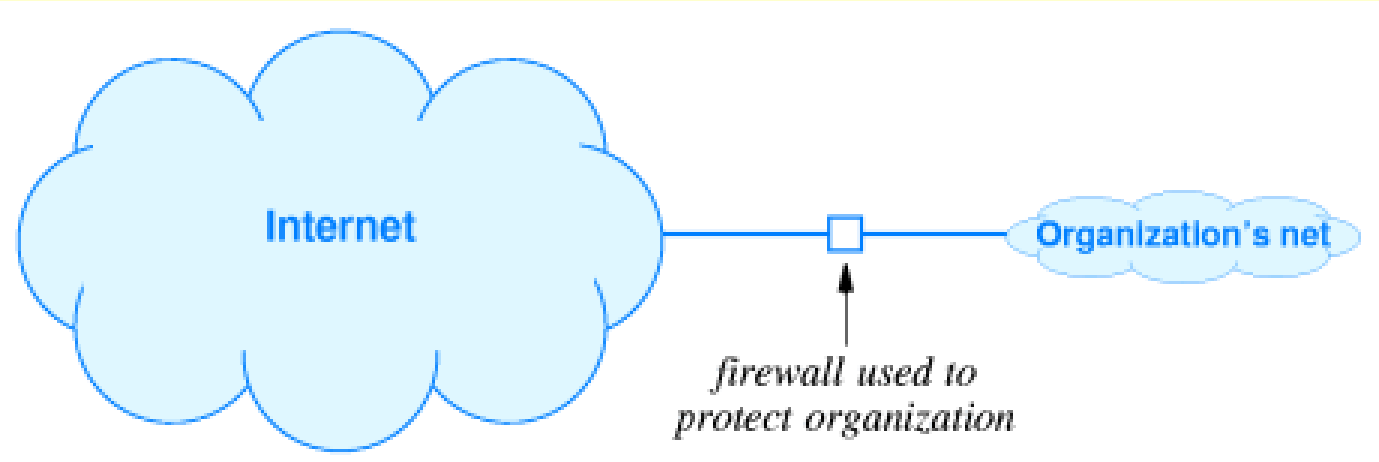
Istovremeno osiguranje autentičnosti i povjerljivosti (2)

$$M = decrypt\ (public\_u1,\ decrypt\ (private\_u2,\ X)\ )\ .$$

- Ako nakon ovog postupka primatelj dobije smislenu poruku, tada je sigurno da je ta poruka autentična i povjerljiva.
- Naime, jedino primatelj je mogao pročitati poruku jer samo on zna odgovarajući tajni ključ *private_u2* potreban za uklanjanje kriptiranja s *public_u2*.
- Također, jedino pošiljatelj je mogao poslati poruku jer samo on zna tajni ključ *private_u1* potreban za kriptiranje koje je uklonjivo s *public_u1*.

Korištenje vatrozida (1)

- Za još veći stupanj zaštite potreban je dodatni mehanizam koji se zove *Internetski vatrozid* (Internet firewall).
- Vatrozid je poseban uređaj (računalo), koje se smješta između unutarnje mreže neke organizacije i vanjskog interneta, i koje štiti unutarnju mrežu od prometa izvana.



Korištenje vatrozida (2)

- Da bi vatrozid obavljao funkciju, potrebno je da:
  - Sav ulazni promet prolazi kroz vatrozid.
  - Sav izlazni promet prolazi kroz vatrozid.
  - Vatrozid implementira sigurnosnu politiku i odbija promet koji krši tu politiku.
  - Sam vatrozid je otporan na sigurnosne napade.
- Osnovna zadaća koju obavlja vatrozid je *filtriranje paketa*. Administrator konfigurira vatrozid tako da on propušta samo pakete upućene na određene IP adrese i određene TCP portove.

Korištenje vatrozida (3)

- Na primjer, može se postići da vanjski subjekti mogu pristupati samo nekim (osiguranim) računalima unutar organizacije, te da pritom smiju komunicirati samo preko određenih portova (servisa).
- Druga zadaća koju obavlja vatrozid je pokretanje posebnih aplikacijskih programa koji se zovu *application-layer gateways* ili *proxies*.
- Na primjer, može se postići da zaposlenici unutar organizacije mogu dovlačiti datoteke s Interneta jedino posredstvom FTP proxy-ja na vatrozidu. Taj proxy najprije kontrolira da li je zaposlenikov zahtjev dozvoljen u smislu sigurnosne politike, zatim on dovlači datoteku s vanjskog Interneta i provjerava da u njoj nema virusa, na kraju on šalje datoteku zaposleniku.

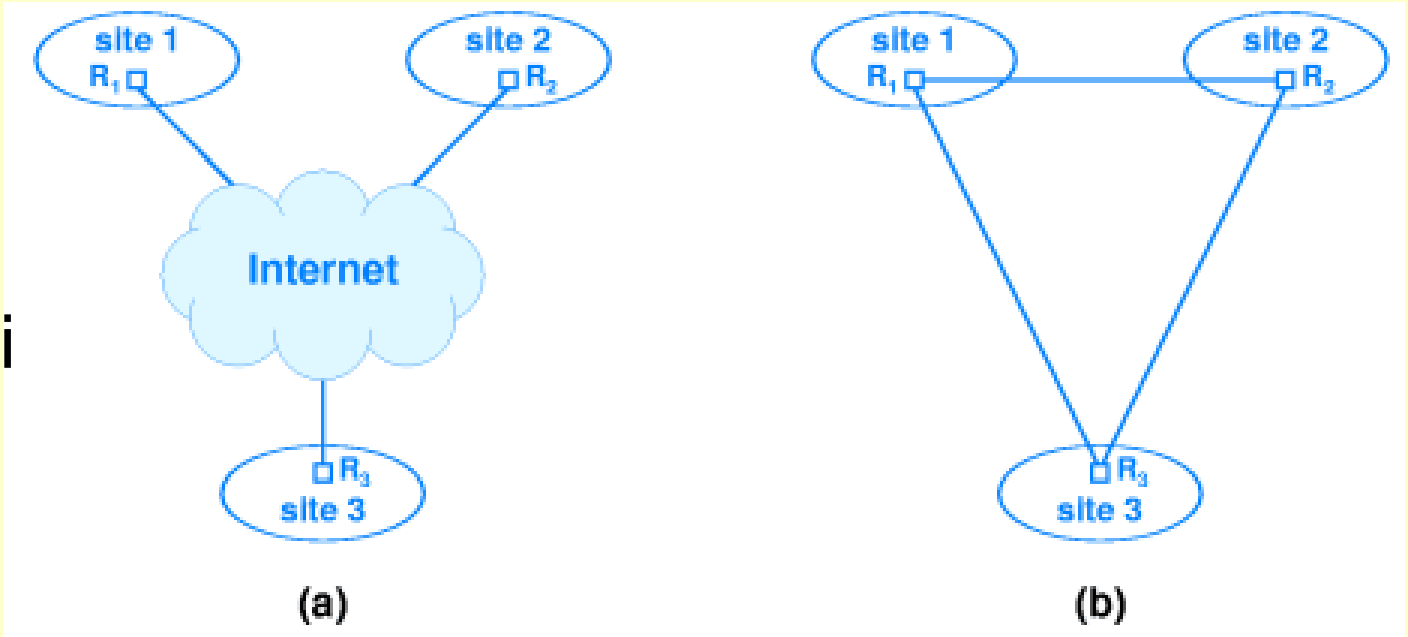
Virtualne privatne mreže (1)

- Zamislimo neku organizaciju koja je raspoređena na više geografskih lokacija. Da bi ta organizacija povezala svoje lokacije u jedan privatni Internet (takozvani *intranet*), ona može koristiti.
  - *Privatne (iznajmljene) veze* koje izravno povezuju usmjernike na dotičnim lokacijama,
  - *Javne Internet veze* kojima se usmjernik na svakoj lokaciji preko lokalnog ISP-a veže na globalni Internet.
- Drugo rješenje je znatno jeftinije no predstavlja sigurnosni rizik jer promet između lokacija prolazi drugim mrežama i podložan je “prisluškivanju”.

Virtualne privatne mreže (2)

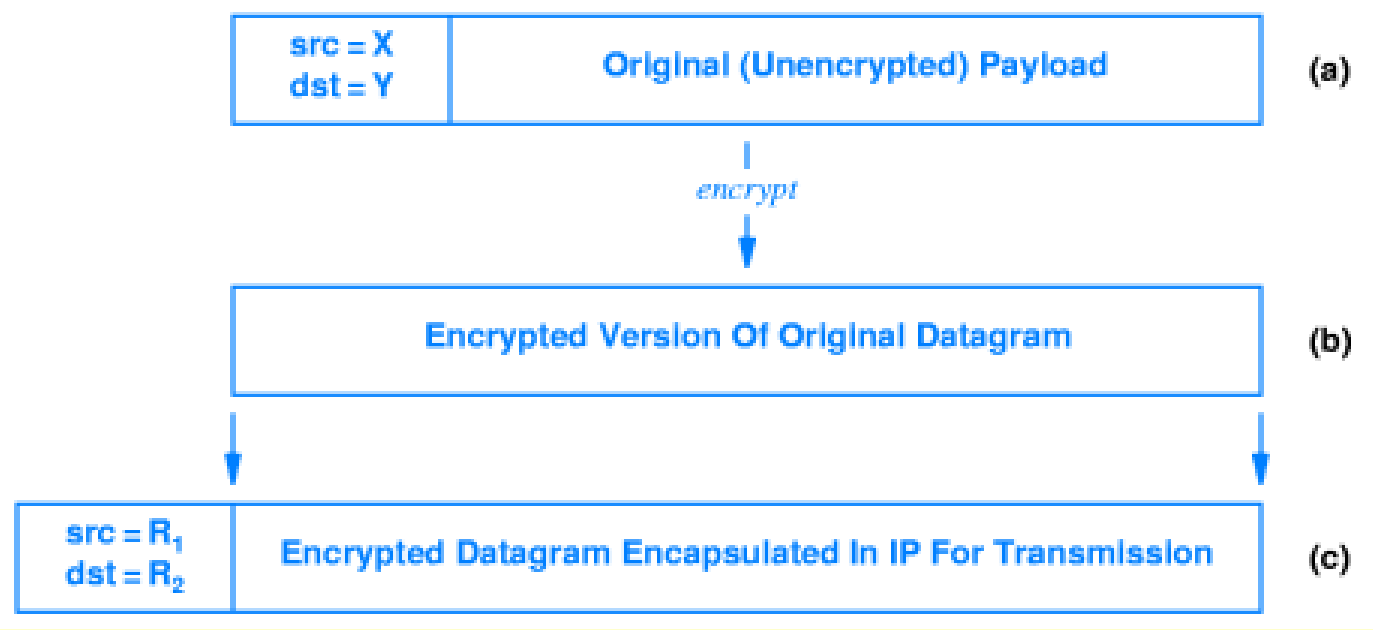
- Kompromisno rješenje naziva se *virtualna privatna mreža* (Virtual Private Network – VPN).
- Podaci između lokacija šalju se javnim Internetom. No VPN softver u usmjernicima na lokacijama osigurava da ti usmjernici komuniciraju isključivo jedan s drugim. Dobiva se iluzija privatne mreže.
- VPN softver također obavlja *kriptiranje* i *tuneliranje*. Datagram između lokacija putuje u kriptiranom obliku.

Sakriveni su sadržaj, adrese pošiljatelja i primatelja.



Virtualne privatne mreže (3)

- Ako se datagram od pošiljatelja X na prvoj lokaciji preko usmjernika R_1 i R_2 šalje primatelju Y na drugoj lokaciji, kriptiranje i tuneliranje izgleda ovako:
  - R_1 kriptira cijeli datagram koji je krenuo od X, te ga umeće kao korisni teret u novi datagram s pošiljateljem R_1 i primateljem R_2.
  - R_2 dekriptira korisni teret iz novog datagrama i tako dobiva polazni datagram kojeg prosljeđuje Y.



Tehnologije za sigurnost (1)

- Navodimo nekoliko standardnih tehnologija za sigurnost koje se intenzivno koriste na Internetu
- *Intrusion Detection System* (IDS). Sustav koji prati sve pakete koji stižu u lokalnu mrežu i upozorava administratora ako se pojavila neka sumnjiva radnja, kao npr TCP port scanning ili SYN flood.
- *Pretty Good Privacy* (PGP). Kriptografski sustav koji se može uključiti u razne aplikacije u svrhu kriptiranja podataka prije slanja na mrežu. Razvijen na MIT, popularan u akademskoj zajednici.
- *Secure Shell* (ssh). Aplikacijski protokol sličan Telnet-u, s time da se svi podaci između klijenta i poslužitelja prenose u kriptiranom obliku. Koristi se unutar programa Putty za sigurno logiranje na udaljeno računalo.

Tehnologije za sigurnost (2)

- *Secure Socket Layer* (SSL). Softver koji se umeće između aplikacije i Socket API i koji kriptira podatke prije slanja kroz Internet. Koristi se na web stranicama koje uključuju financijske transakcije.
- *Remote Authentication Dial-In User Service* (RADIUS). Protokol koji omogućuje centraliziranu autentikaciju, autorizaciju i obračunavanje usluga za grupu korisnika. Popularno rješenje za ISP-ove koji imaju dial-up korisnike, te za VPN-ove koji dozvoljavaju zaposlenicima da se spajaju na zaštićenu mrežu od kuće.
- *Wi-Fi Protected Access* (WPA). Dio standarda za Wi-FI bežični LAN. Služi se kriptiranjem, omogućuje povjerljivost komuniciranja i autentičnost korisnika koji se spajaju na LAN.

Najava kolegija na diplomskom studiju

- Problemi obrađeni u ovom poglavlju detaljnije će se proučavati u kolegiju “Kriptografija i sigurnost mreža” na diplomskom studiju Računarstvo i matematika.
- Kolegij će uključiti sljedeće teme: klasična kriptografija, moderni simetrični blokovski kriptosustavi, kriptosustavi s javnim ključem, testovi prostosti i metode faktorizacije, sigurnost mreža.
- Definirat će se i detaljno analizirati neki od najpoznatijih kriptosustava: DES (tajni ključ), RSA (javni i tajni ključ).
- Objasnit će se matematički razlozi zašto su navedeni kriptosustavi sigurni. Razlozi leže u teoriji brojeva, te imaju veze s računskom složenošću rastavljanja velikih brojeva na proste faktore.