Osnovni pojmovi

Pretnje, napadi, ranjivosti, sigurnosni ciljevi i usluge

Sadržaj

- Klasifikacija napada
- Faze napada
- Primer: izviđački napadi
- Ranjivosti, pretnje i jednačina rizika
- Sigurnost kao proces
- Sigurnosni ciljevi i usluge
- Dimenzije napada
- Sigurnosni modeli

O složenosti informacione sigurnosti

- Informaciona sigurnost, kao i sigurnost računarskih sistema i mreža je široka oblast koja sadrži veliki broj gradivnih elemenata (podoblasti).
- Gotovo sve podoblasti su takođe vrlo složene (gledano i sa inženjerskog i naučnog gledišta).
  - Primer: kriptologija (različiti tipovi algoritama), biometrija (različiti modaliteti).
- Ne može se izdvojiti stučnjak (praktičar), a još teže istraživač koji u svim podoblastima (ili velikom broju podoblasti) postiže značajne i upečatljive rezultate!
- Većina praktičara i istraživača se ograničava na nekoliko usko povezanih podoblasti.
  - Praktičar 1: administrator zaštitnih mehanizama računarskih mreža.
  - Praktičar 2: osoba koja se bavi statičkom i dinamičkom analizom koda.
- Dobra praksa:
  - Fokusirajte se na srž i dubinu podoblasti, pratite najnovije trendove i svakodnevno se usavršavajte.
  - Zadržite širinu, tj. ne dozvolite sebi da ostanete neupućeni u ostale podoblasti, naročito one koje su usko povezane sa fokusom interesovanja!
- Policija takođe ima odvojena odeljenja za rešavanje slučajeva ubistava i suzbijanje narkotika!

Napad na sigurnost, sigurnosni mehanizam i usluge

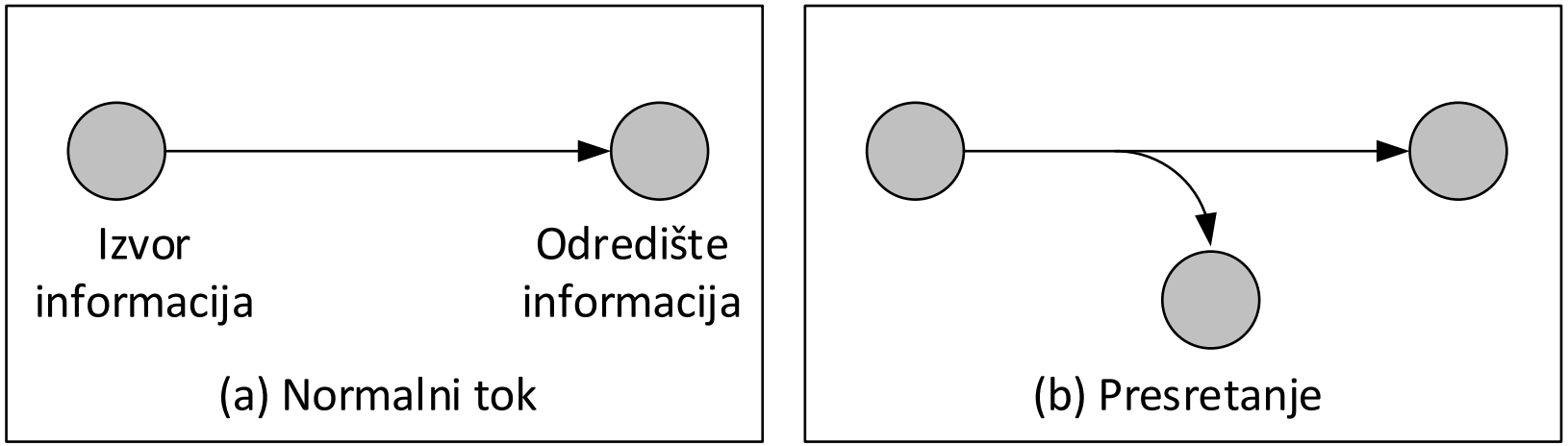
- **Napad na sigurnost** (engl. *security attack*) je bilo koja akcija koja ugrožava sigurnost informacija.
  - Napadi su akcije koje su usmerene na ugrožavanje sigurnosti informacija, računarskih sistema i mreža.
- **Sigurnosni mehanizam** (engl. *security mechanism*) je mehanizam koji treba da detektuje i predupredi napad ili da sistem oporavi od napada.
- **Sigurnosna usluga** (engl. *security service*) je usluga koja povećava sigurnost sistema za obradu i prenos podataka.
  - Sigurnosna usluga podrazumeva upotrebu jednog ili više sigurnosnih mehanizama.
  - Primer: autentifikacija USB tokenom, autentifikacija lozinkom i biometrijskim uzorkom.

Klasifikacija napada

- Postoje različite vrste napada i nekoliko načina klasifikacije.
- Generalno, napadi se mogu podeliti u četiri kategorije:
  - **presretanje** (engl. *interception*),
  - **presecanje**, tj. prekidanje (engl. *interruption*),
  - **izmena** (engl. *modification*),
  - **fabrikovanje** (engl. *fabrication*).

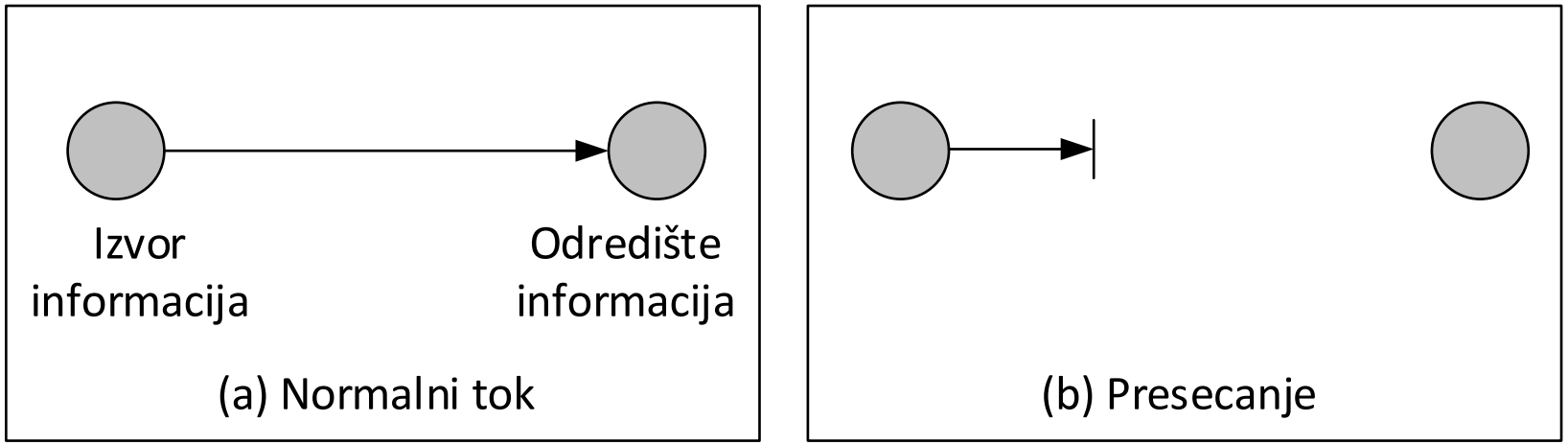
Klasifikacija napada: presretanje

- **Presretanje** je **pasivan** napad na **poverljivost** (engl. *confidentiality*).
- Može biti u praksi sprovedeno kao prisluškivanje saobraćaja, nadziranje njegovog intenziteta, uvid u osetljive informacije ili slično.
- Teško se otkriva jer ne menja podatke, odnosno ne utiče na unutrašnje funkcionisanje sistema.
- Ovakav tip napada ponekad je pripremna faza za neku drugu vrstu napada.



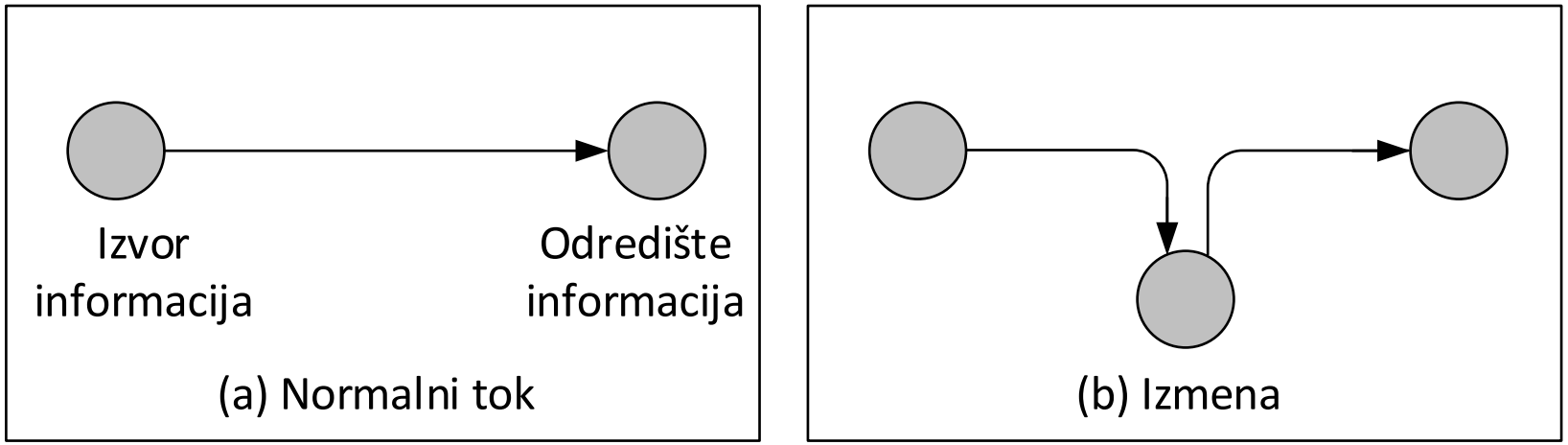
Klasifikacija napada: presecanje

- **Presecanje**, tj. prekidanje je **aktivan** napad na **raspoloživost** (engl. *availability*).
- Presecanjem se prekida tok informacija, tj. onemogućava pružanje neke usluge ili funkcionisanje nekog sistema.
- Primer presecanja bi bio uspešno izvršen DoS / DDoS napad na neku Web stranicu ili uništenje podataka na nekom računarskom sistemu (na primer, infekcija Ransomware-om za koji se zna da se nakon plaćanja otkupa ne dobija ključ za dešifrovanje datoteka).



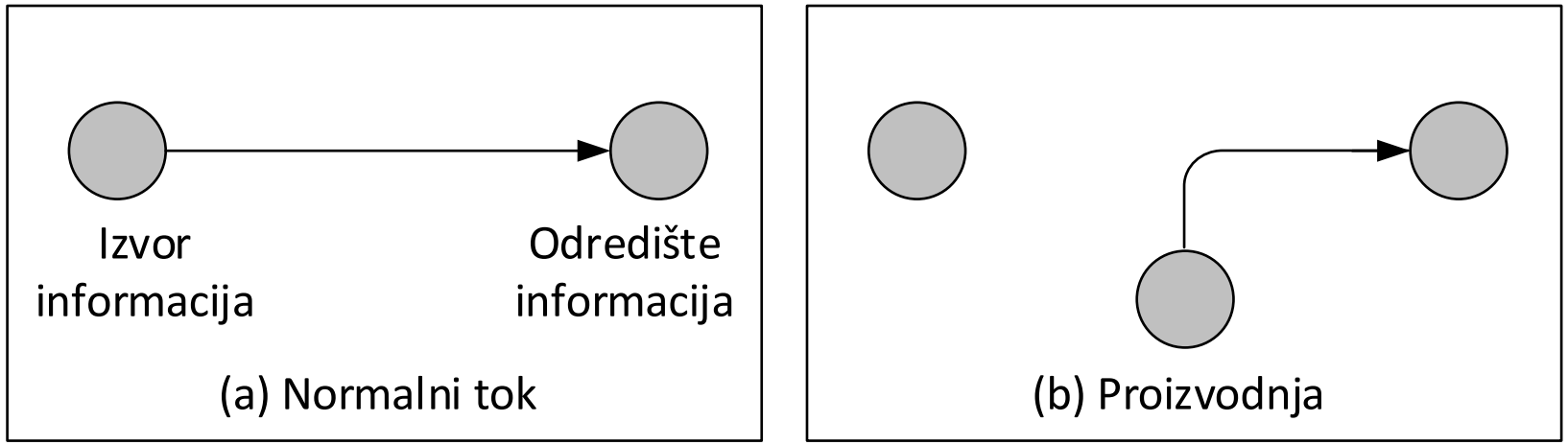
Klasifikacija napada: izmena

- **Izmena** je **aktivan** napad na **integritet** (engl. *integrity*).
- Na prenosnom putu može se ispoljiti kao napad tipa čovek u sredini (engl. *man in the middle*).
- U računarskom sistemu se može ispoljiti kao izmena podataka, pristupnih prava ili načina funkcionisanja programa.
- Iako menja podatke ili sistem, ovaj napad često ostaje neprimećen izvesno vreme, kako zbog nepažnje, tako i zbog složenih tehnika koje se pri ovom napadu koriste.



Klasifikacija napada: fabrikovanje

- **Fabrikovanje** je **aktivan** napad na **autentičnost** (engl. *authenticity*).
- Na primer, napadač generiše lažne podatke, lažni saobraćaj ili izdaje neovlaštene komande.
- U ove napade spada i lažno predstavljanje korisnika, usluge, servera, Web strane ili nekog drugog dela sistema.



Klasifikacija napada prema Kendall-u

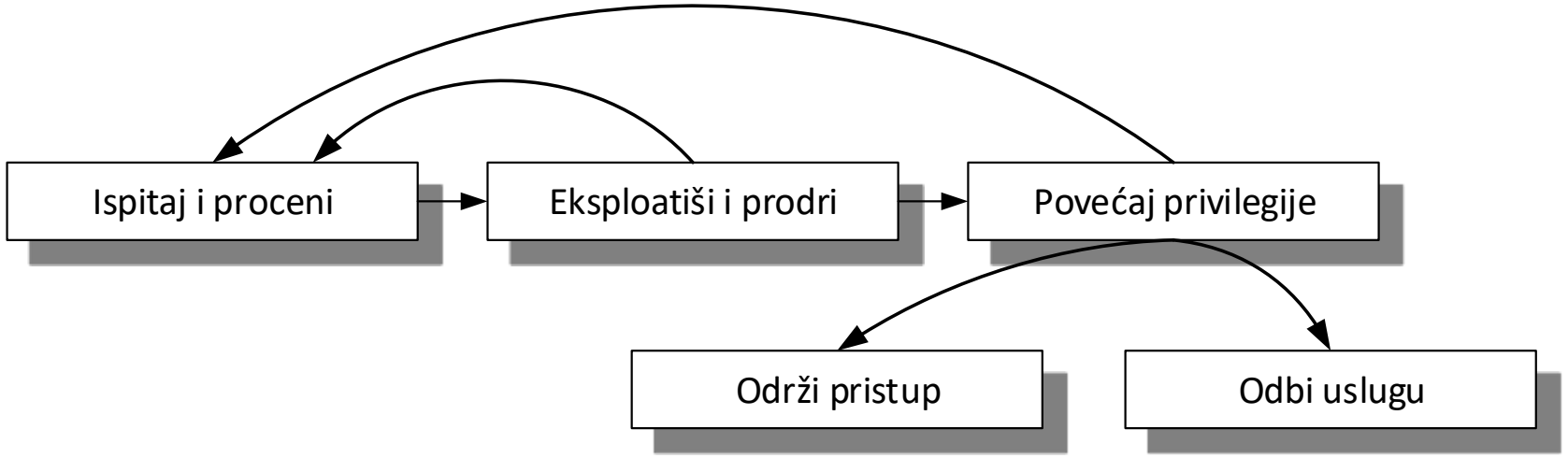
- Alternativno, napadi se shodno Kendall-ovoj taksonomiji mogu klasifikovati i u sledeće četiri kategorije: ispitivački napadi, napadi neovlašćenog sticanja pristupa udaljenom računaru, neovlašćenog povećanja privilegija i odbijanja usluga.
- **Ispitivački napadi** (engl. *probing*).
  - Napadač prikuplja informacije o sistemu ili mreži i traži ranjivosti koje može da iskoristi kao što su neispravno konfigurisani zaštitni mehanizmi.
  - Ovo su pasivni napadi koji se koriste se u fazi pripreme aktivnih napada.
  - Primeri izvođenja: skeniranje portova (nmap), popisivanje (*fingerprinting*), odnosno određivanje tipa i verzije OS kako be se znalo koji sigurnosni propust treba iskoristiti.
- **Napadi neovlašćenog sticanja pristupa udaljenom računaru** (engl. *Remote to Local*, R2L).
  - Napadi kojima se neovlašćeno stiče pristup udaljenom računaru na kome napadač nema legitiman korisnički nalog.
  - Primeri: pogađanje lozinke (rečnika, Rainbow tabele), upotreba rootkit alata.
  - NAPOMENA: rootkit omogućava napadaču da se sakrije i održi privilegovan pristup računaru zaobilaženjem normalne autentifikacije i mehanizama autorizacije.

Klasifikacija napada prema Kendall-u

- **Napadi neovlašćenog povećanja privilegija** (engl. *priviledge escalation*, *User to Root*, U2R).
  - Napadi kojima se eksploatišu ranjivosti operativnih sistema ili softvera.
  - Često su zasnovani na prekoračenju bafera ili dovođenje sistema u stanje trke.
  - Cilj napadača je sticanje većih privilegija na žrtvi, u idealnom slučaju privilegija administratora (odatle potiče naziv *User to Root*).
- **Napadi odbijanja usluga** (engl. *Denial of Service*, DoS).
  - Napadi koji za posledicu imaju nedostupnost resursa.
  - Na primer, napadač neovlašćeno koristi računarske resurse (memorija, CPU), sistem je prezauzet i ne može da odgovori na legitimne zahteve.
  - Primeri izvođenja:
    - Eksploatisanje ranjivosti u sastavljanju fragmenata IP paketa (fragmenti sa preklopnjenim *offest* poljima).
    - Iskorišćavanje ranjivosti uspostavljanja TCP konekcije (veliki broj poluotvorenih konekcija).

Faze napada

- Ove četiri kategorije usklađene su donekle sa osnovnim koracima metodologije napadača:
  - **Ispitaj i proceni** (istraživanje potencijalne mete, identifikovanje i procena ranjivosti, planiranje i eventualna simulacija napada pre samog izvođenja daljih koraka)
  - **Eksploatiši i prodri** (iskorišćavanje identifikovanih ranjivosti i sticanje pristupa sistemu)
  - **Povećaj privilegije** (u idealnom slučaju privilegije administratora)
  - **Održi pristup** (prikrivanje tragova i postavljanje takozvanih sporednih ulaza)
  - **Uradi ono šta si naumio** (odbi uslugu, preuzmi podatke, izmeni ili generiši lažne podatke).



Faze napada (primer)

- Uzmimo za primer napad kod koga napadač pokušava da izmeni stanje na svom bankovnom računu.
  - Prvi korak napadača je izviđanje, odnosno upoznavanje sa organizacijom računarske mreže i informacionog sistema banke.
  - Napadač na osnovu prikupljenih informacija planira napad i prpverava verovatnoću njegovog uspeha na osnovu simulacija.
  - Ukoliko je zadovoljan rezultatima simulacije pristupa izvršavanju napada, odnosno pokušava da neovlašćeno pristupi bazi podataka u kojoj želi da menja podatke.
  - Ukoliko u tome uspe, napadač postiže cilj napada – menja stanje na svom bankovnom računu.
  - Da bi sprečio otkrivanje ove izmene, kao i uspeh eventualne istrage koja bi vodila do njega, napadač zatim uništava sve tragove svog napada (uklanja eventualno instalirane alate, zapise iz dnevničkih datoteka i slično).

Faze napada

- **Napomena 1**.
  - Zavisno od metoda i načina izvođenja, neke vrste napada je podjednako teško ostvariti i na žičnim i na bežičnim mrežama, dok se neki (poput prisluškivanja) mogu mnogo lakše sprovesti na bežičnim mrežama s obzirom na sigurnosne probleme karakteristične za njih.
- **Napomena 2**.
  - Nemaju svi napadi sve faze.
  - Uglavnom je uspešnost u izvršavanju određene faze preduslov za prelazak na sledeću fazu.
  - Na primer, ukoliko napadač pronađe ozbiljan i dobro poznat propust u fazi izviđanja, faza planiranja i simulacije napada može biti izostavljena.
  - Sa druge strane, ukoliko tokom faze izviđanja ne pronađe odgovarajući propust u sistemu koji se napada, napadač neće moći da pristupi narednim fazama.

Primer: izviđački napadi

- Pre samih akcija za postizanje konačnog cilja napada napadač mora da poseduje dovoljno informacija o ciljnom sistemu, kao i o njegovom okruženju.
- U ove informacije spadaju mrežna organizacija okruženja, instalirani softver, verzije i podešavanja, period u kome sistem nije resetovan, aktivni servisi i slično, odnosno sve što može sadržati ranjivosti koje se mogu iskoristiti za potrebe napada.
- Za dobijanje ovih informacija koristi se izviđanje, odnosno tzv. **izviđački napadi**.
- Jedna od osnovnih aktivnosti prilikom napada izviđanja je skeniranje računarskih sistema i mreža.
- Izviđanje se najčešće obavlja na tri nivoa:
  - horizontalno,
  - vertikalno,
  - dubinsko.

Primer: izviđački napadi

- **Horizontalno izviđanje** je proces u kome napadač ispituje koji se mrežni uređaji i računari nalaze u računarskoj mreži i koja je njena topologija.
  - Ovakvo izviđanje se može izvesti na različite načine ali je njegov najjednostavniji oblik korišćenje ICMP protokola, odnosno tzv. „pingovanje“ svih IP adresa iz opsega koje koristi računarska mreža na koju se vrši napad.
  - Primer:

```
$ nmap -sP 192.168.1.*
Starting Nmap 5.51 ( http://nmap.org ) at 2012-08-28 11:11 CEST
Nmap scan report for 192.168.1.7
Host is up (0.00012s latency).
MAC Address: 00:0D:60:32:EA:3E (IBM)
...
```

Primer: izviđački napadi

- **Vertikalno izviđanje** ima za cilj da napadaču pruži informaciju o tome koji su portovi na pojedinačnim mrežnim uređajima (najčešće računarima) otvoreni, odnosno koji se mrežni servisi na njima izvršavaju.
  - Primer:

```
$ nmap 192.168.1.122 -p 1-65535
Nmap scan report for 192.168.1.122
Host is up (0.00024s latency).
Not shown: 65533 closed ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 336.15 seconds
```

Primer: izviđački napadi

- **Dubinsko izviđanje** ima za cilj da napadaču pruži što detaljnije informacije o softveru koji se izvršava na određenom mrežnom uređaju (tip, verzija i podešavanje softvera, a odnose se i na sistemski i na korisnički softver.)
  - Ove informacije imaju najviši značaj jer na osnovu njih napadač otkriva potencijalne bezbednosne rupe koje može iskoristiti za postizanje ciljeva napada.
  - Primer (utvrđivanje verzije operativnog sistema):

```
$ nmap -O 192.168.1.122
Nmap scan report for 192.168.1.122
Host is up (0.00022s latency).
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.19 - 2.6.36
Network Distance: 1 hop
OS detection performed.
Nmap done: 1 IP address (1 host up) scanned in 12.07 seconds
```

Primer: izviđački napadi

- Napadi izviđanja ne moraju biti usmereni na samo jedan ciljni sistem već se mogu koristiti za otkrivanje više sistema koji sadrže odgovarajuće ranjivosti.
  - Na primer, napadači često koriste automatizovane programe tipa agenata koji pronalaze Web sajtove na Internetu zasnovane softverskim rešenjima sa javno dostupnim izvornim kodom (Joomla, WordPress i slično).
  - Napadači u lokalnu bazu podataka smeštaju podatke o njima (najčešće adrese sajtova i informacije o instaliranoj verziji softvera).
  - Onoga trenutka kada se za korišćenu verziju softvera pronađe nova ranjivost napadači pokreću automatizovane skripte koje pristupaju sajtovima zabeleženim u bazi i menjaju sadržaj, preuzimaju podatke i slično.

Primer: izviđački napadi

- Iako napadi izviđanja sami po sebi ne pričinjavaju značajnu štetu (osim manjeg trošenja resursa sistema i mreže koji se napadaju) oni su najava napada kojim će takva šteta biti načinjena!
- Iz tog razloga je poželjno preduzeti dva preventivna koraka:
  - Instalirati alate koji prepoznaju napade izviđanja i o tome izveštavaju administratora
  - Podesiti sopstvene sisteme tako da napadač putem napada izviđanja dobije što oskudniju informaciju.
- Primeri:
  - Korišćenje ICMP protokola je veoma retko potreba regularnih korisnika računarskog sistema i mreže pa se taj protokol može potpuno isključiti ili se o njegovoj upotrebi može obaveštavati administrator.
  - Javno odavanje informacija o verziji i karakteristikama Web servera će biti od koristi najčešće samo zlonamernim korisnicima pa ga je poželjno potpuno isključiti.

Ranjivosti i pretnje

- **Ranjivost** (engl. *vulnerability*) je slabost u nekoj vrednosti, resursu ili imovini koja može biti iskorišćena, tj. eksploatisana.
- Ranjivosti su posledica:
  - **lošeg projektovanja** (greška projektanta),
  - **implementacije** (odgovornost klijenta),
  - **zagađenja** (aplikacija radi više od onog što se očekuje) – na primer, mrežni servis ili aplikacija koja se izvršava sa root privilegijama dozvoljava da se iz nje otvori *shell*.
- **Pretnja** (engl. *threat*) je protivnik, situacija ili splet okolnosti sa mogućnošću i/ili namerama da eksploatiše ranjivost.
  - Finansijski sponzorisani protivnik sa jasno definisanim ciljem i formalnom metodologijom smatra se **strukturiranom pretnjom**.
  - Ova definicija pretnje stara je nekoliko decenija i konsistentna je s načinom opisivanja terorista.
  - Takve pretnje su karakteristične za ekonomsku špijunažu, organizovani kriminal i strane obaveštajne službe.

Razlozi nastanka ranjivosti u softverskim proizvodima

- **Društveni inženjering** je čest uzrok uspešnog izvršavanja napada!
  - Čak i svaki *pen-test* uključuje društveni inženjering (ljudi na ovom delu često „padaju“).
- Alternative uspešnih napada:
  - Loše konfigurisani zaštitni mehanizmi.
  - Iskorišćavanje ranjivosti koje nastaju tokom razvoja softvera.
- Ranjivosti u softveru nastaju kao posledice:
  - **Brzog razvoja softvera** (engl. *agile software development*).
    - Tehnologija mora brzo da evolvira kako bi ostala upotrebljiva.
    - Brza evolucija i iterativna poboljšanja reflektuju se u polje softverskog inženjerstva.
    - Nametnuti su pravci poput brzog razvoja softvera.
    - Nepotpun proces QA softvera ostavlja dovoljno prostora za greške i ranjivosti.
  - Korišćenja metodologije **sigurnost zasnovana na skrivanju** (engl. *security by obscurity*) prilikom razvoja koja ne predpostavlja prisustvo napadača.
    - Ako protivnik otkrije ranjivost, mehanizam koji bi sprečio iskorišćavanje te ranjivosti ne postoji.

Primer ranjivosti: Factoring RSA Export Keys (FREAK)

- **CVE-2015-0204** je SSL/TLS ranjivost koja dozvoljava napadaču da presretne HTTPS konekcije i nametne korišćenje slabe kriptografske zaštite.
- Indirektna je posledica usaglašavanja sa zakonima o izvozu SAD (*USA Export Laws*).
- Zakoni o izvozu kriptografskog softvera za cilj imaju da omogućite NSA da izvršiti kriptoanalitičke napade i onemogućiti druge organizacije sa manjim računarskim resursima da izvrše iste.
- Za RSA izvozne ključeve (engl. *export keys*) moduo može biti najveće dužine 512 bita.
- Ranjivost se iskorišćava na sledeći način:
  - Napad tipa čovek u sredini: manipulisanje dogovora o algoritmima koji će se koristiti u toku sesije, čime se ograničava dužina ključeva koje se koriste.
  - Kriptoanaliza: Number Field Sieve algoritam + *Cloud Computing* servisi koji se mogu iznajmiti za $100.
- U vestima Washington Post objavljenih 3. marta 2015. godine čitamo sledeće: „*Sites affected by the vulnerability included the US federal government websites fbi.gov, whitehouse.gov and nsa.gov*“.

Primer ranjivosti: GHOST

- **CVE-2015-0235** je ranjivost u Linux GNU C biblioteci (glibc).
  - Ova biblioteka je deo gotovo svih distribucija Linux operativnog sistema.
- Ranjivost potiče od mogućeg prekoračenja bafera unutar glibc GetHOST funkcije.
- Funkcija je zadužena za razrešavanje mrežnih adresa.
- Potencijalno ugrožava sigurnost gotovo svog softvera koji se na neki način odnosi na mrežu.
- Ranjivost se smatra kritičnom.
  - Napadač može da je iskoristi i preuzme kontrolu nad ciljnim Linux sistemom bez potrebe za poznavanjem lozinki naloga sa administrativnim privilegijama.
  - Kompanija Qualys navodi sledeće: *„Korišćenjem zlonamernog koda koji iskorišćava ovu ranjivost napadač može izvršiti prozvoljni kod preko Exim servera za elektrosku poštu“*.
- Više informacija o ranjivostima može se naći na Web stranici: *Common Vulnerabilities and Exposures*, https://cve.mitre.org/

O ranjivostima i nekim finansijskim aspektima

- Da li znate u čemu je razlika između nečega što se zove propust i nečega što se zove bag?
  - Defekt u projektovanju i dizajnu se u engleskom jeziku naziva **propust** (engl. *flaw*, sl. levo).
  - Defekt u implementaciji ili kodiranju se u engleskom jeziku naziva bag (usvojen termin, engl. bug).

Slike preuzete iz [3].

O ranjivostima i nekim finansijskim aspektima

- *Security as an Afterhought*

Slika preuzeta iz [3].

Vrednost imovine i jednačina rizika

- **Vrednost imovine** je mera vremena i resursa potrebnih da se neka imovina zameni ili vrati u svoje prethodno stanje.
- Zato se kao ekvivalentan termin može koristiti i **cena zamene**.
  - Server baze podataka na kome se čuvaju informacije o kreditnim karticama klijenata, podrazumevano je vredniji od radne stanice u nekoj laboratoriji za ispitivanje softverskih proizvoda.
- **Rizik** je mera opasnosti, tj. mogućnost da nastane oštećenje ili gubitak neke informacije, hardvera, intelektualne svojine, prestiža ili ugleda.
- Rizik se definiše eksplicitno, na primer:
  - „Rizik narušavanja integriteta baze klijenata“.
  - „Rizik odbijanja usluga od strane on-line portala banke“.
- Rizik se obično izražava u obliku jednačine rizika:
  - Rizik = Pretnja × Ranjivost × Vrednost imovine

Šta je sigurnost?

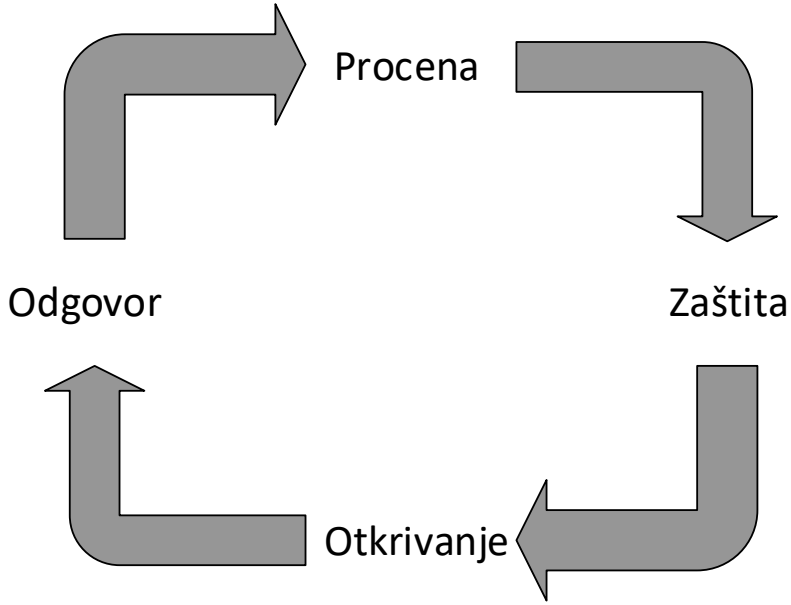
- **Sigurnost je proces održavanja prihvatljivog nivoa rizika**.
- Sigurnost je proces, a ne završno stanje, tj. nije konačni proizvod.
- Organizacija ili institucija ne može se smatrati sigurnom ni u jednom trenutku posle izvršene poslednje provere usklađenosti sa vlastitim sigurnosnim pravilima. Na primer:
  - Danas je urađena procena ranjivosti i ranjivosti nisu otkrivene.
  - Dan kasnije je promenjena konfiguracija postojećeg ili je dodat nov „nezakrpljen“ uređaj.
  - U mreži se pojavljuje ranjivost koju napadač može iskoristiti.
- Kada se govori o sigurnosti i zaštiti informacionih sistema i mreža, nekoliko principa danas važe kao osnovni postulati:
  - Sigurnost je proces. Sigurnost nije proizvod, usluga ili procedura, već skup koji ih sadrži, uz još mnogo elemenata i mera koje se stalno sprovode.
  - Ne postoji **apsolutna sigurnost**.
  - Ne postoji takozvani „**srebrni metak**“ (iako velike svetske kompanije, uključujući tu i tržišne lidere, reklamiraju u raznim medijima svoje proizvode kao svemoćna rešenja).
  - Uz različite metode zaštite, treba imati u vidu i ljudski faktor, sa svim slabostima.

Šta je sigurnost?

- Ukoliko i dalje smatrate da je sigurnost konačni proizvod, odgovorite na sledeće pitanje: da li ulazna vrata imaju bilo kakvu zaštitnu funkciju ukoliko na kratko ošišate živu ogradu?

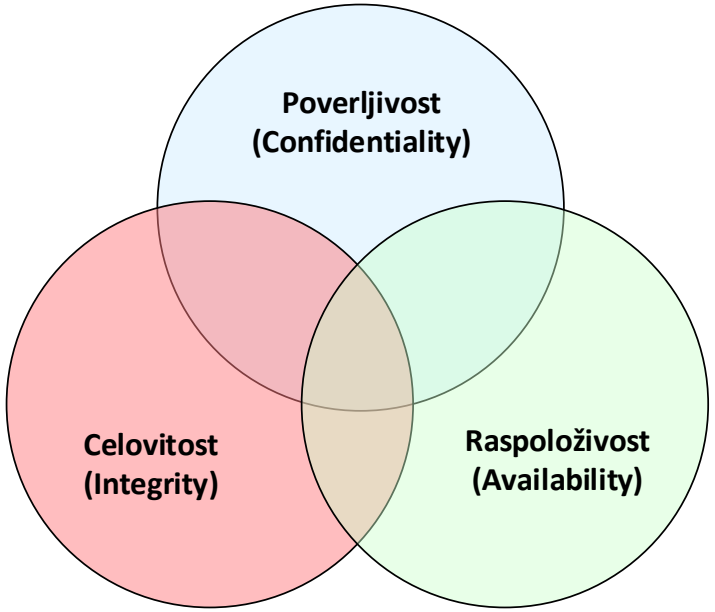
Sigurnost kao proces

- **Procena** (engl. *assessment*), tj. planiranje (engl. *planning*).
- **Zaštita** (engl. *protection*). Smanjivanje mogućnosti ugrožavanja sistema.
- **Otkrivanje** (engl. *detection*). Proces identifikacije upada, tj. povrede sigurnosnih pravila ili incidenata koji se odnose na sigurnost.
- **Odgovor** (engl. *response*). Proces oporavka od posledica upada, primenjuju se šabloni „zakrpi i nastavi“, ili „goni i sudi“.



Sigurnosni ciljevi

- „Veliko trojstvo“ sigurnosti:
  - **CIA** = *Confidentiality* (poverljivost), *Integrity* (integritet), *Availability* (raspoloživost).
- Skraćenice sastavljene od reči suprotnog značenja:
  - **DAD** = *Disclosure* (otkrivanje, obelodanjenje), *Alteration* (izmena), *Destruction* (uništenje).
  - Ova skraćenica se na engleskom jeziku čita „ded“, što znači mrtav.



Sigurnosni ciljevi

- **Poverljivost**. Koncept poverljivosti obuhvata pokušaje da se spreči namerno ili nenamerno neovlašćeno okrivanje sadržaja poruka.
  - Poverljivost se može izgubiti na mnogo načina, kao što su namerno otkrivanje privatnih podataka u vlasništvu kompanije ili pogrešno definisanim pravima pristupa mreži.
- **Integritet** (celovitost). U okviru sigurnosti informacija, koncept integriteta obezbeđuje sledeće:
  - Podatke ne smeju menjati neovlašćena lica ili procesi.
  - Ovlašćena lica ili procesi ne smeju obavljati neovlašćene promene podataka.
  - Podaci su interno i eksterno konsistentni, tj. interni podaci su međusobno konsistentni u svim podcelinama tj. delovima, kao i sa realnim svetom, tj. spoljnim okruženjem.
- **Raspoloživost**. U okviru sigurnosti informacija, koncept raspoloživosti obezbeđuje da odgovarajuće osoblje pouzdano i pravovremeno može da pristupa podacima ili računarskim resursima.
  - Drugim rečima, raspoloživost garantuje da su sistemi podignuti i da rade kao što je predviđeno.

Sigurnosne usluge

- **Sigurnosni mehanizam** je mehanizam koji treba da detektuje i predupredi napad ili da sistem oporavi od napada.
- **Sigurnosna usluga** je usluga koja povećava sigurnost sistema za obradu i prenos podataka i podrazumeva upotrebu jednog ili više sigurnosnih mehanizama.
- U sigurnosne usluge spadaju, na primer:
  - **Autentifikacija** (engl. *authentication*), tj. provera identiteta. Usluga kojom se od svakog korisnika zahteva da se predstavi sistemu pre nego što nešto uradi, i koja obezbeđuje način da svaki objekat (neko ili nešto) koji tvri da ima određen identitet to i dokaže.
  - **Autorizacija** (engl. *authorization*). Najjednostavnije rečeno, određuje koji autentifikovani korisnik ima pravo da pristupi određenim resursima, i na kakav način.
  - **Neporicanje**, priznavanje (engl. *non-repudiation*). Usluga koja obezbeđuje da korisnik koji pošalje poruku ili izmeni neki podatak ne može kasnije tvrditi da on to nije uradio. Na primer, korisnik koji digitalno potpiše dokument svojim privatnim ključem kasnije neće moći da negira da je on taj dokument napravio i potpisao, jer se potpis lako može proveriti.

Sigurnosne usluge

- Sigurnosni mehanizmi (levo) i usluga koja koristi više mehanizama (desno).

Dimenzije napada

- Dve osnovne **dimenzije napada** u računarskim mrežama vezane su za:
  - **njihovu metu** (koji deo računarske mreže se napada),
  - **svrhu** (šta se želi postići napadom).
- Pri tome, većina napada je složena, odnosno da bi se postigao konačan cilj napada potrebno je napasti više različitih delova sistema i ugroziti različite aspekte njihove sigurnosti.
- U osnovne mete napada u računarskim mrežama spadaju:
  - mrežni uređaji (krajnji i posredni),
  - komunikacioni kanali,
  - krajnji korisnici.
- Sledeću dimenziju napada čini njegova svrha, odnosno koja se zaštićena karakteristika napada.
- U osnovne kategorije ovde spadaju:
  - poverljivost,
  - itegritet,
  - raspoloživost.

Dimenzije napada: meta

- Najčešće vršeni napadi u računarskim mrežama su **napadi na mrežne uređaje**.
  - Meta ovavkih napada mogu biti krajnji uređaji (serveri, klijentski računari i slično) ili posredni (komutatori, ruteri, filteri paketa, bežične pristupne tačke i slično).
  - Mogu se napadati svi slojevi OSI referentnog komunikacionog modela.
- U nekim situacijama napadač nema mogućnost ili potrebu da napada mrežne uređaje, već **napada komunikacione kanale**.
  - Napadi mogu biti zasnovani na pasivnoj analizi njihovih signala, ili na aktivnom menjanju, bilo spoljnim uticajem, bilo umetanjem posredujućeg mrežnog uređaja.
  - Dodatno, napadači imaju i mogućnost da kompletno onemoguće komunikaciju presecanjem neobezbeđenih komunikacionih kanala.
- Napadači koji nisu u stanju da izvrše napad na mrežne uređaje i komunikacione kanale pokušavaju da svoj cilj ostvare delovanjem **na krajnje korisnike**.
  - U zavisnosti od toga koji cilj žele da postignu, napadači se lažno predstavljaju, traže od korisnika poverljive podatke, podmeću lažne podatke, pretražuju smeće, zatrpavaju korisnike velikim brojem podataka i tome slično.

Dimenzije napada: svrha

- Svrha **napada na poverljivost** je da se neovlašćeno pristupi određenim podacima, bilo da se oni čuvaju u memoriji nekog računarskog sistema, bilo da se prenose putem računarske mreže.
  - U osnovi, napad je pasivan.
- **Napadi na integritet** imaju za cilj da lažiraju sadržaje komunikacija.
  - Treba imati u vidu da se kod nekih tipova napada (na primer, napad tipa čovek u sredini) putem napada na verodostojnost posredno postiže i napad na poverljivost.
- **Napadi na raspoloživost** imaju za cilj da regularnim korisnicima određenog resursa onemoguće normalan rad sa njim.
  - Na primer, u napadima sa ciljem uskraćivanja usluge često se mrežni serveri zatrpavaju ogromnom količinom besmislenih zahteva sa ciljem da se iscrpu dostupni resursi (procesorsko vreme, memorija, komunikacioni kanal) tako da server postane nedostupan regularnim klijentima.

Dimenzije napada: matrični prikaz

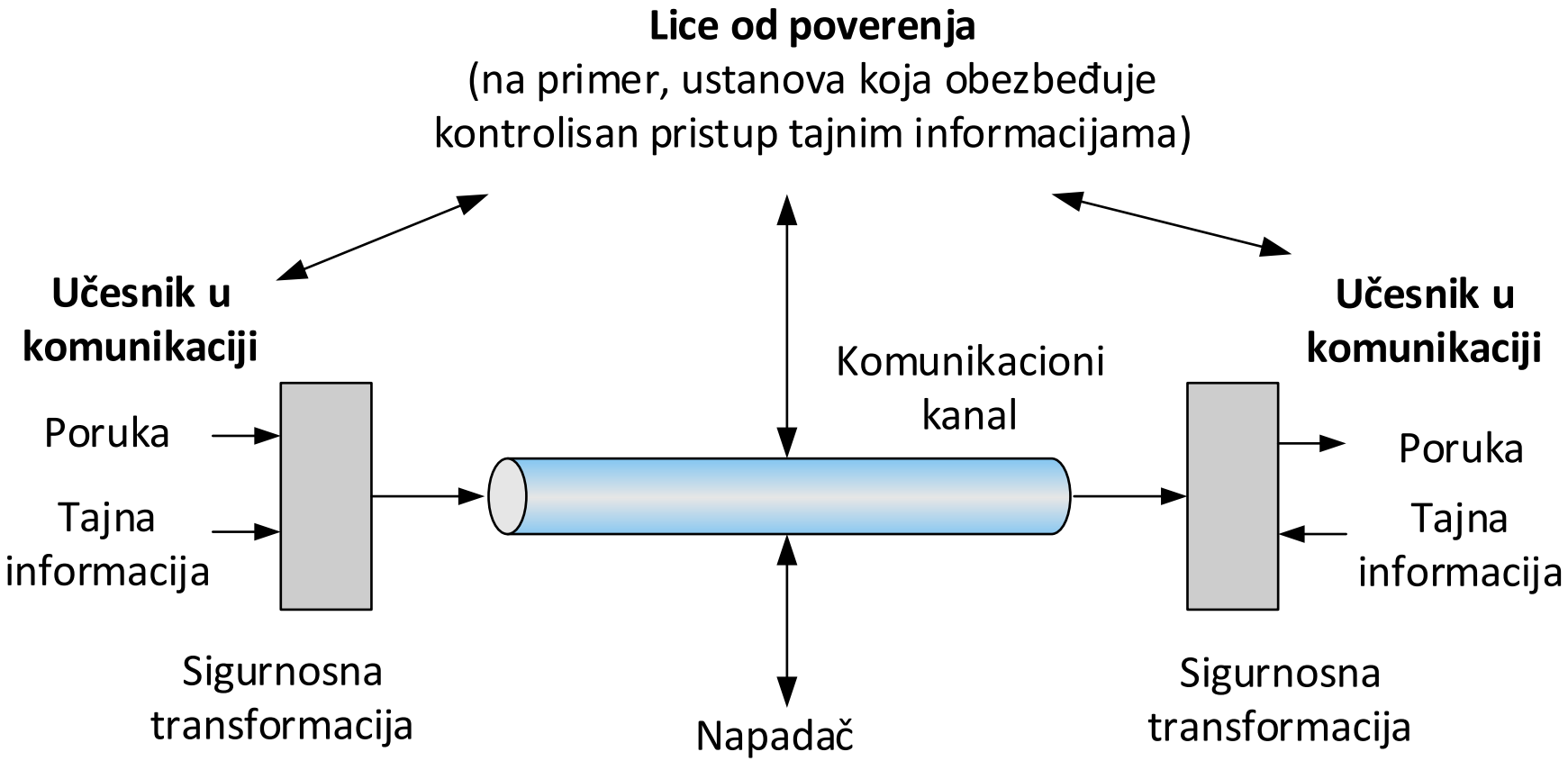
- U skladu sa navedene dve osnovne dimenzije napada može se razviti matrica u koju se mogu svrstati svi do sada poznati napadi u računarskim mrežama.

	Kanali	**Uređaji**	**Korisnici**
Poverljivost	Prisluškivanje	Preuzimanje kontrole i podataka	Obmanjivanje
Integritet	Izmena saobraćaja	Izmena podataka i programa	Lažno predstavljanje, krađa identiteta
Raspoloživost	Presecanje, preopterećivanje	Zauzimanje resursa, slom	Uznemirivanje, dosađivanje, zatrpavanje podacima

Sigurnosni modeli

- Shodno mestu sigurnosne transformacije i funkciji koju ta transformacija obavlja (na primer, šifrovanje ili digitalno potpisivanje) izdvajamo dva sigurnosna modela.
- **Model sa nesigurnim komunikacionim kanalom** pokazuje protok informacija između dva učesnika preko nesigurnog komunikacionog kanala, uz postojanje protivnika, tj. napadača.
  - Oba učesnika primenjuju odgovarajuću sigurnosnu transformaciju sa odgovarajućim tajnim informacijama koje obezbeđuje „lice od poverenja“.
  - Na ovaj način se komunikacioni kanal štiti od napadača koji ne zna i ne može da dobije skrivenu informaciju.
- **Model sigurnog pristupa mrežnim resursima** odnosi se na kontrolisan pristup podacima ili resursima računarskog sistema, u prisustvu potencijalnih napadača. Zasnovan je na:
  - Odgovarajućoj kontroli pristupa unutar samog sistema (na primer, liste za kontrolu pristupa datotekama na disku, prava dodeljena korisnicima nad nekom bazom podataka).
  - Takozvanom „čuvaru“ (engl. *gatekeeper*), tj. zaštitnom mehanizmu koji kontroliše prisup sistemu spolja (na primer, mrežna barijera) kako bi se obezbedila adekvatna sigurnost.

Model sa nesigurnim komunikacionim kanalom

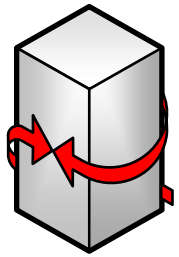


Model sigurnog pristupa mrežnim resursima

Protivnik

- čovek (npr. haker)
- softver (npr. virus, crv)

Pristupni kanal



" Čuvar "
(kontrola pristupa spolja)

Informacioni sistem

Računarski resursi (procesor, memorija, U/I)

Podaci

Procesi

Softver

Interna kontrola prisupa

Ukoliko sigurnost zanemarite ili joj ne pridate dovoljno značaja …

- Na Web sajtu RT (bivši *Russia Today*) čitamo sledeću vest objavljenu 10. septembra 2014. godine:

5 million 'compromised' Google accounts leaked

A database of what appears to be some 5 million login and password pairs for Google accounts has been leaked to a Russian cyber security internet forum. It follows similar leaks of account data for popular Russian web services.

- Autori [2] navode da u pitanju nije kompromitovanje naloga za Gmail, već drugih servisa na kojima su korišćeni Gmail nalozi.

Literatura

1. D. Pleskonjić, N. Maček, B. Đorđević, M. Carić (2007): Sigurnost računarskih sistema i mreža. Mikro knjiga, Beograd.
2. A. Jevremović, M. Veinović, M. Šarac, G. Šimić (2014): Zaštita u računarskim mrežama. Univerzitet Singidunum, Beograd.
3. G. Goluch (2016): Secure Coding & SDLC. RACVIAC SE Europe - Advanced Training Course, 19.10.2016
4. K. Kendall (1999): A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems, Massachusetts Institute of Technology.

Hvala na pažnji

Pitanja su dobrodošla.