Bezbjednost i zaštita informacionih sistema

3. Kontorla pristupa

Prof. dr Nikola Žarić

e-mail: zaric@ucg.ac.me

Servisi za obezbjeđenje sigurnosti

Sigurnosni servisi

Služe za povećanje sigurnosti prenosa i sistema za obradu podataka

Sigurnosni servis koristi jedan ili više sigurnosnih mehanizama, koji treba da detektuju ili spriječe napad, ili da oporave sistem od napada.

Sigurnosni mehanizmi su strukturna i tehnološka rješenja, postupci, pravila i procedure koji se primjenjuju na sistemu radi realizacije sigurnosnih servisa.

Domeni zaštite

Po nekim autorima postoje 4 grupe metoda zaštite:

1. kriptografske,
2. programske,
3. organizacione i
4. fizičke.

Domeni zaštite

Neki autori klasifikuju metode zaštite na sljedeći način:

- Fizičke kontrole
- Audit trails (Revizija ruta)
- Otkrivanje prevare (Fraud detection)
- Steganografija
- Šifrovanje (šifrovanje javnim ključem, generisanje i upravljanje ključevima, sertifikacija)
- Zaštitne barijere (Firewall) i dr.

Domeni zaštite

Organizacija **International Information Systems Security Certification Consortium - definisala je sljedećih 10 domena zaštite:**

1. Sistemi za kontrolu pristupa
2. Sigurnost razvoja aplikacija i sistema
3. Planiranje oporavka od napada i obezbjeđivanje kontinuiranog rada
4. Kriptografija
5. Pravni i etički aspekti sigurnosti.

Domeni zaštite

6. Fizička sigurnost
7. Sigurnost operative
8. Upravljanje sigurnosnim sistemima
9. Sigurnosne arhitekture i modeli
10. Sigurnost komunikacionih i računarskih mreža

Ovih deset oblasti danas se često koriste prilikom klasifikacije zaštitnih metoda.

Područja primjene zaštite

Područja primjene zaštite se mogu podijeliti na osnovu mjesta djelovanja zaštitnih mehanizama:

- **Zaštita na nivou aplikacije** (softverska zaštita aplikacija ....),
- **Zaštita na nivou operativnog sistema** (kontrola pristupa na nivou korisnika, ažuriranje operativnog sistema.....),
- **Zaštita na nivou mrežne infrastrukture** (mrežne barijere....) i
- **Proceduralna i operaciona zaštita** (zaštitne polise, blokada napada, rekonfigurisanje sistema...).

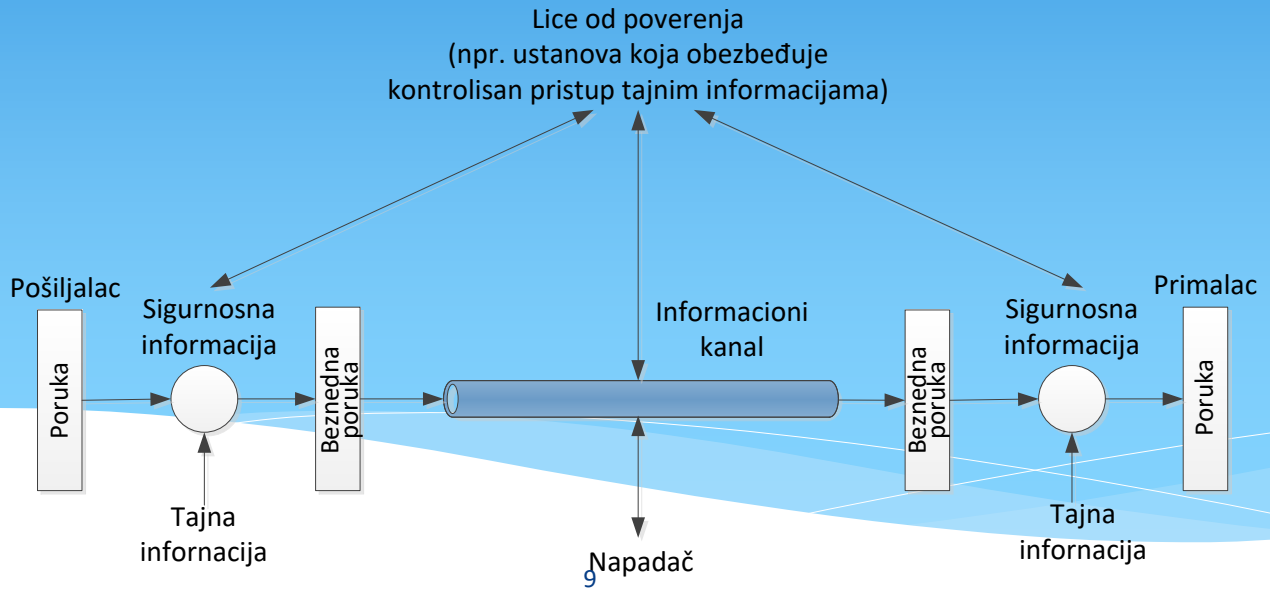
Principi projektovanja sistema zaštite

Pri projektovanju sistema zaštite uzimaju se u obzir sljedeći principi:

- ekonomičnost zaštite,
- pouzdanost zaštite,
- potpuna provjera svih faza (start, radni režim, oporavak, isključivanje i održavanje),
- javnost projekta,
- razdvajanje prava,
- najmanja prava,
- redukcija zajedničkih mehanizama,
- psihološka prihvatljivost (sprega između računara i čovjeka),
- radni faktor,
- evidencija ugrožavanja.

Model, metode i aspekti zaštite

Model na slici prikazuje protok informacija između dva učesnika preko nesigurnog komunikacionog kanala, uz postojanje napadača.



Model, metode i aspekti zaštite

Poruka se prenosi iz jednog dijela u drugi preko Interneta. Bezbjednosni aspekti se razmatraju kada je to neophodno ili poželjno za zaštitu prenosa podataka od napadača koji može predstavljati prijetnju za poverljivost, autentičnost, itd.

Sve tehnike za obezbjeđivanje bezbjednosti imaju dvije komponente:

1. **Transformacije vezane za bezbjednost poslatih informacija**. Primjeri uključuju šifrovanje poruke i dodatog koda zasnovanog na sadržaju poruke, koji se može koristiti za provjeru identiteta pošiljaoca.
2. **Dva subjekta dijele tajne informacije** u nadi da će ostati nepoznate za protivnika. Primjer je ključ za šifrovanje koji se koristi u sprezi sa transformacijom za šifrovanje poruke prije prenosa i dešifrovanje po prijemu.

Model, metode i aspekti zaštite

Lice od povjerenja (treća strana), može biti potrebno za ostvarivanje sigurnog prenosa podataka :

- Na primjer, lice od povjerenja može biti odgovorno za distribuciju tajnih informacija prema dva subjekta i u isto vrijeme i za njihovo čuvanje od protivnika.

- Nekada lice od povjerenja može biti potrebno da presudi sporove između dva subjekta u pogledu vjerodostojnosti prenosa poruka.

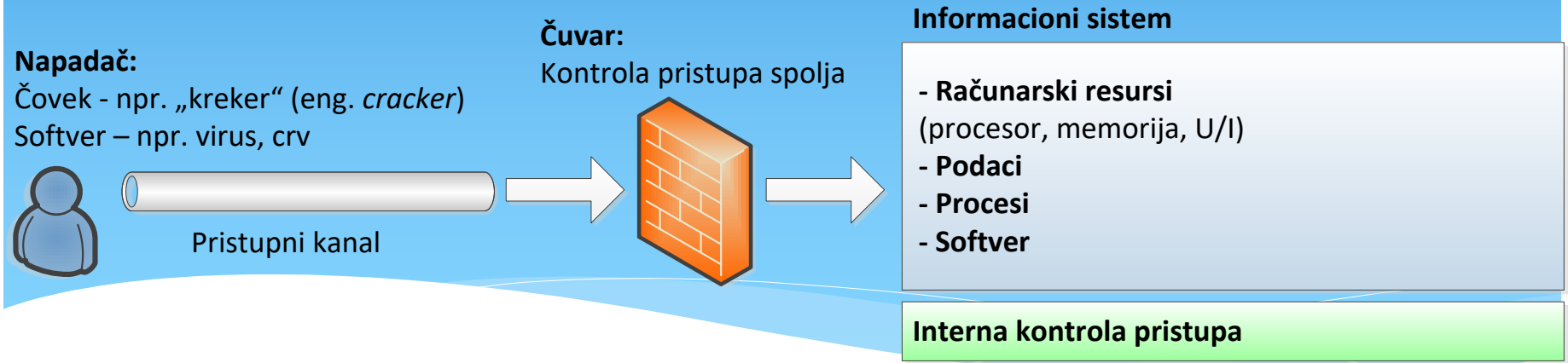
Model, metode i aspekti zaštite

Navedeni opšti model pokazuje da postoje četiri osnovna zadatka u projektovanju određenih bezbjednosnih usluga:

1.Projektovanje algoritma za izvršavanje transformacija vezanih za sigurnost.
2.Generisanje tajnih informacija o tome koji će se algoritam koristiti.
3.Razvoj metode za distribuciju i dijeljenje tajne informacije.
4.Izbor protokola koji će se koristiti kada se upotrebljava sigurnosni algoritam.

Model, metode i aspekti zaštite

Postoje druge bezbjednosne situacije koje se ne uklapaju u prethodni model. Drugi model dat je na slici, koja prikazuje način zaštite informacionog sistem od neželjenog pristupa.



Model, metode i aspekti zaštite

Sigurnosni mehanizmi potrebni za suočavanje sa neželjenim pristupom spadaju u dvije široke kategorije:

1. Prva kategorija se naziva **čuvar (*gatekeeper*) funkcija**.
   Ona uključuje postupke pristupa (user/password) koji su projektovani da omoguće pristup svim ovlašćenim korisnicima, ali i screening logike koja je projektovana da otkrije i odbije crve, viruse i druge slične napade.
2. Ako jednom ili nepoželjni korisnik ili neželjeni softver dobije pristup, **druga linija odbrane** se sastoji od raznih internih kontrola koje nadziru aktivnosti i analiziraju sačuvane podatke u pokušaju da otkriju prisustvo neželjenih programa.

Kontrola pristupa

* **Kontrole pristupa** zasnovane na:

  * nečemu što **osoba zna** (na primjer, PIN broj ili lozinka)
  * nečemu što **osoba ima** (na primjer, sigurnosna identifikaciona kartica)
  * nečemu što **osoba jeste** (biometrija zasnovana na fizičkim karakteristikama)
  * nečemu što **osoba radi** (biometrija zasnovana na karakteristikama ponašanja)

Kontrola pristupa

* Sigurnost zasnovana na **dva faktora**:
  * korišćenje najmanje dva od četiri elementa, da bi se odobrio pristup.
    * Npr: korisniku se dozvoli pristup kada unese lozinku i kad se provjeri otisak prsta.
* Sigurnost zasnovana na **četiri faktora**
  * upotreba sva četiri elementa.

* Danas se za provjeru identiteta najčešće koristi
  * samo jedan faktor
  * (lozinka)

Biometrija

* **Biometrija**
* grčki: **bios – život, metron – mjera**
* skup metoda za identifikovanje pojedinaca
* na osnovu **bioloških karakteristika** i/ili **karakteristika ponašanja**
  * biološke karakteristike:
    * otisak prsta
    * snimak rožnjače oka
    * crte lica
    * geometrija šake
    * DNK
  * karakteristike ponašanja: glas, potpis
* najčešće se koristi za provjeru identiteta

Biometrija

* Najobičniji biometriski sistem se sastoji od **pet komponenti:**
  * **senzor** –
    * sakuplja podatke i pretvara ih u digitalnu formu
  * **algoritam izračunavanja signala** –
    * stvara biometrijsku mapu
  * **skladište podataka** –
    * sadrži početne biometrijske mape sa kojim se nove uspoređuju
  * **algoritam podudaranja** –
    * uspoređuje biometriske mape iz prethodne dvije komponente

Biometrija

* **Karakteristike biometrijskih metoda:**
  * **jedinstvenost** – jednoznačnost identifikacije
  * **trajnost** – dužina zadržavnja karakteristike
  * **prikupljivost** – lakoća dobija uzoraka
  * **izvodljivost** – u kojoj je mjeri moguće u praksi implementirati navedene biometrijske metode i
  * **prihvatljivost** – u kojoj je mjeri implementacija moguća a da se pri tome ne naruše ljudska prava.

Biometrija – otisci prstiju

* Površina kože na prstima je pokrivena sitnim brazdama koje se nazivaju **papilarnim linijama.**
  * **Papilarne linije** jednoznačno identifikuju osobu i nepromjenljive su.
  * **Ne posmatra se pun otisak**, već karakteristične značajne tačke otisaka prstiju.
  * **Razlozi:**
    * u forenzici se često ne nađu potpuni otisci prstiju već djelovi (trag)
    * ušteda vremena

Biometrija – otisci prstiju

* **Otisak** se **opisuje karakterističnim tačkama**:
* **globalne**
  * osnovni uzorci papilarnih linija (lukovi, spirale, petlje)
  * referentni centar, delta (tačka prvog grananja)
  * papilarni broj
* **lokalne (minutacije)**
  * tačke koje se markiraju na krajevima, granama i razdvajanju papilarnih linija.
  * minutacije su glavni nosioci identifikacije
  * dvije osobe ne mogu imati više od 8 zajedničkih minutacija.

Biometrija – otisci prstiju

* Postoji **pet različitih osobina minutacija**:
* **vrsta minutacije**, na primjer:
  * papilarni kraj – nagli prekid papilarne linije
  * grananje (bifurkacija) – grananja linije u više novih
  * papilarne linije koje se dijele na dvije, a zatim se ponovo spajaju u sopstvenu izvornu liniju
* **orijentacija** – smjer u kome "gleda" minutacija
* **zakrivljenost** – brzina promene smera minutacije
* **udaljenost papilarnih linija** u okolini minutacije
* **koordinate** u odnosu na središnju tačku ili deltu.

Biometrija – otisci prstiju

Biometrija – za ili protiv?

* **Fizički**
  * Realna situacija:
    * 2005. u Maleziji su odsjekli prst vlasniku automobila za čije je pokretanje bilo neophodno očitati otisak prsta.
* **Privatnost**
  * LK sa biometrijskim podacima?
  * Zloupotreba prikupljenih podataka za lažiranje pri izvođenju ilegalnih operacija
    * neugodnosti za pojedinca koji je predmet zloupotrebe.

Konvencija o cyber-kriminalu

* **Vijeće Evrope** je u **novembru 2001**. **donijelo konvenciju** kojom je pokušalo **dati smjernice** u borbi protiv računarskog kriminala.
  * **krivična djela protiv tajnosti**, nepovrjedivosti i dostupnosti podataka
  * **krivična djela poput prevare i faslifikovanja** uz pomoć računara
  * **krivična djela koja se odnose na sadržaj podataka**
    * npr distribuciju i širenje uzenmirujućih sadržaja
  * **kršenje autorskih i srodnih prava.**

Konvencija o cyber-kriminalu

* Krivična djela protiv tajnosti, nepovrjedivosti i dostupnosti podataka:
  * **neovlašćen pristup (čl. 2)**
  * **neovlašćeno presretanje podataka (čl. 3)**
  * **mijenjanje sadržaja, brisanje ili oštećenje podataka (čl. 4)**
  * **ometanja normalnog rada računara (čl. 5)**
  * **proizvodnja, prodaja, distribucije ili upotreba uređaja** projektovanih u svrhu počinjenja nekog od prethodno navedenih krivičnih djela (**čl. 6**)

Konvencija o cyber-kriminalu

* **Zakonodavni okvir**
  * neovlašćeno korišćenje računara i računarske mreže
  * računarska sabotaža
  * pravljenje i unošenje računarskih virusa
  * računarska prevara
  * ometanje elektronske obrade i prenosa podataka i funkcionisanja računarske mreže
  * neovlašćen pristup zaštićenom računaru ili računarskoj mreži
  * sprječavanje i ograničavanje pristupa javnoj računarskoj mreži
  * neovlašćeno korišćenje autorskog i drugog srodnog prava

Konvencija o cyber-kriminalu

* **Zakonodavstvo– primjer 1**
* **Neovlašćeni pristup zaštićenom računaru ili računarskoj mreži**
* **[1]** Ko kršeći mjere zaštite neovlašćeno pristupi računaru ili računarskoj mreži, kazniće se novčanom kaznom ili zatvorom **do jedne godine.**
* **[2]** Ko upotrijebi podatak dobijen na način nepredviđen, kazniće se novčanom kaznom ili zatvorom **do tri godine.**
* **[3]** Ako su usljed djela iz prethodnog stava nastupile teške posljedice za drugog, učinilac će se kazniti zatvorom od šest mjeseci do **pet godina.**

Konvencija o cyber-kriminalu

* **Zakonodavstvo – primjer 2**
* **Pravljenje i unošenje računarskih virusa**
  * **[1]** Ko napravi računarski virus u namjeri da ga unese u tuđ računar ili računarsku mrežu, kazniće se novčanom kaznom ili zatvorom **do jedne godine.**
  * **[2]** Ko unese računarski virus u tuđ računar ili računarsku mrežu i time prouzrokuje štetu, kazniće se zatvorom od tri mjeseca do **tri godine.**
* NAPOMENA: Virus nije precizno definisan.
* Zakonom nisu obuhvaćene ostale štetočine :)

Copyright, patenti i licence

* **Autorsko pravo**
  * štiti originalnu implementaciju i način prikaza neke ideje, a ne samu ideju !
* **može se zaštititi izvorni i izvršni kôd**, uputstva i dokumentacija u digitalnom ili pisanom obliku.
* **ne štiti algoritme, metode i matematičke postupke** korišćene u realizaciji softvera
  * štiti od neovlašćenog kopiranja ili oponašanja koda,
  * ali ne štiti od konkurencije koja samostalno i nezavisno (bez uvida u izvorni kôd konkurencije) razvija sličan softver

Copyright, patenti i licence

* **Patent**
* Za razliku od autorskog prava koje štiti prezentaciju ideje i oblik izražavanja, **patent štiti samu ideju**
* **Dakle, patent štiti ideje, algoritme i matematičke postupke** korišćene u programu, a ne **sam kôd**.
  * zabranjuje objavu bilo kakvog sličnog rada pa makar bio i nezavisno razvijen.
  * šta je povoljno za nas koji mrzimo softverske patente?
  * visoka cijena njihovog izdavanja i dugo vrijeme koje mora proći od predaje zahtjeva pa do eventualnog odobrenja za objavljivanje patenta

Društveni aspekti sigurnosti

* **Steganografija**
  * utiskivanje jedne poruke u drugu na neki način
  * pri čemu utisnuta poruka ostaje skrivena
* **primjer – utiskivanje poruke u sliku**
  * npr za utiskivanje vlasničkih prava u sliku (watermarking)
  * **prednost u odnosu na kriptografiju: ne zna se da je poruka skrivena**

Društveni aspekti sigurnosti

* **Sloboda izražavanja i cenzura**
* **Zabranjeni materijal** može da obuhvati lokacije sa sledećim sadržajem (shodno vladajućem režimu):
  * **materijal nepodesan za djecu i omladinu**
  * **govor mržnje** usmjeren na različite etničke, religiozne, seksualne i druge grupe
  * **informacije o demokratiji** i demokratskim vrijednostima
  * **istorijski materijali** koji protivrječe zvaničnoj verziji vlade
  * **priručnici za ilegalne aktivnosti** kao što su obijanje brava, pravljenje oružja, eksploziva i eksplozivnih naprava, razbijanje šifara i slično.

Društveni inženjering

* **Probijanje sigurnosti iskorišćenjem ljudskog faktora**
  * nedostatka svijesti o veličini problema sigurnosti
  * nemara i grešaka
  * neobaviještenosti i neobrazovanosti

*