ZAŠTITA PODATAKA

Uvod

Značaj zaštite

- Tradicionalno su se koristili fizički (kontrola pristupa) i administrativni mehanizmi
- Primena računara zahteva automatizovane alate (komponente) za zaštitu zapamćenog sadržaja
- Korišćenje računarskih i komunikacionih mreža zahteva mere zaštite prilikom prenosa podataka
- Zahtevi u pogledu zaštite podataka su sve značajniji u poslednje vreme (internet, poslovanje preko interneta, usluge koje se pružaju u cloud okruženju)

Značaj zaštite (2)

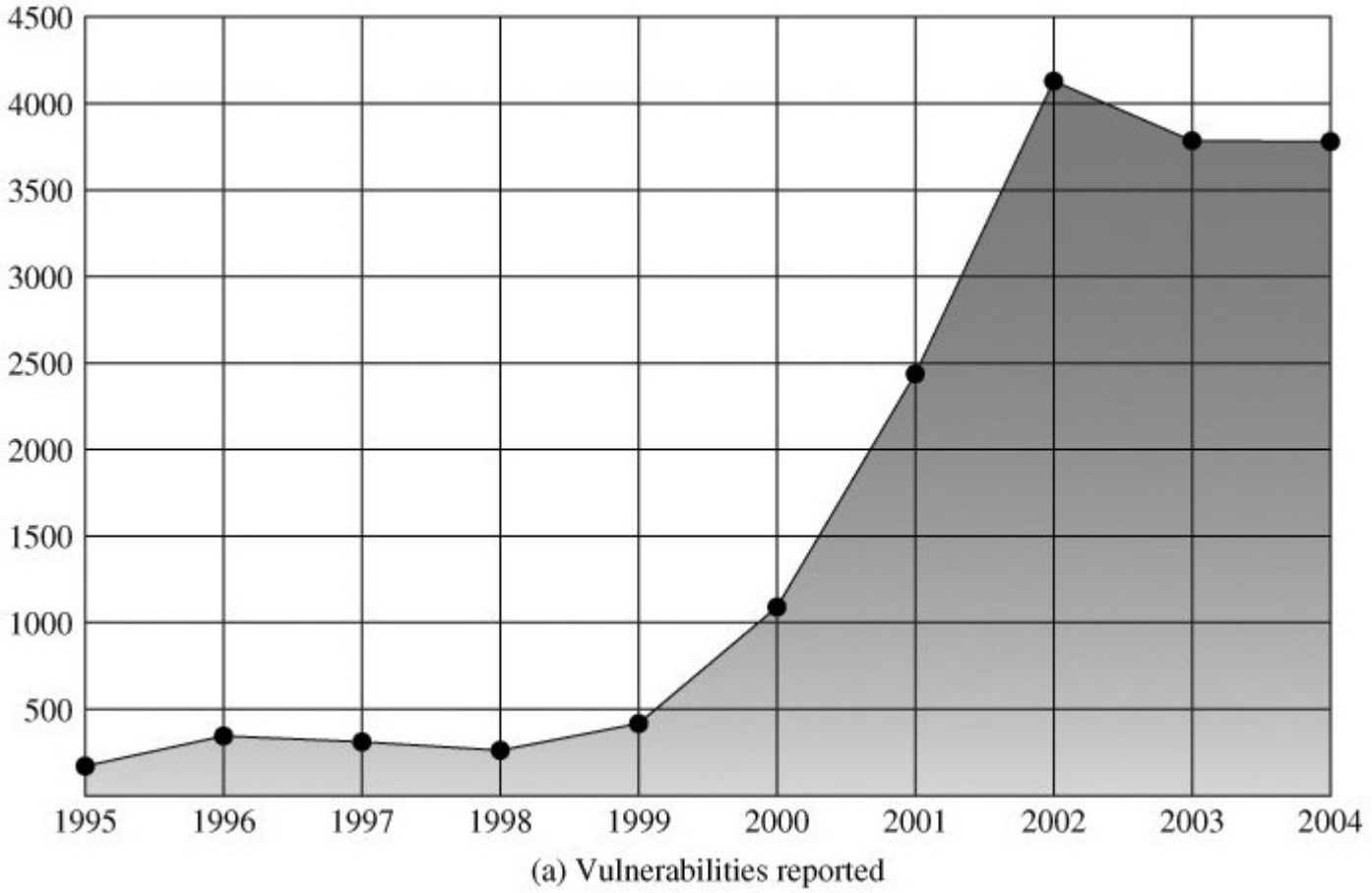
- Zaštita podrazumeva postizanje nekog cilja (izvršavanje programa, komunikaciju, ...) u prisustvu (potencijalnog) protivnika
- S obzirom da je danas sve više toga digitalizovano (administrativni poslovi koji uključuju lične podatke, banke, škole, fakulteti, bolnice, euprava, ...) i da većina aplikacija i informacionih sistema koristi internet, to znači da postoji veliki broj sistema koji moraju da vode računa o zaštiti

Neki problemi koje treba rešiti

- Presretanje poruke i uvid u njen sadržaj
- Neovlašćeni pristup uređajima ili podacima
- Promena prava pristupa
- Promena sadržaja podataka
- Poricanje aktivnosti
- Prevare, ucene, krađe, lažna obaveštenja, uticaj na industrijske sisteme
- Sprečavanje dostupnosti usluga

Broj sigurnosnih propusta

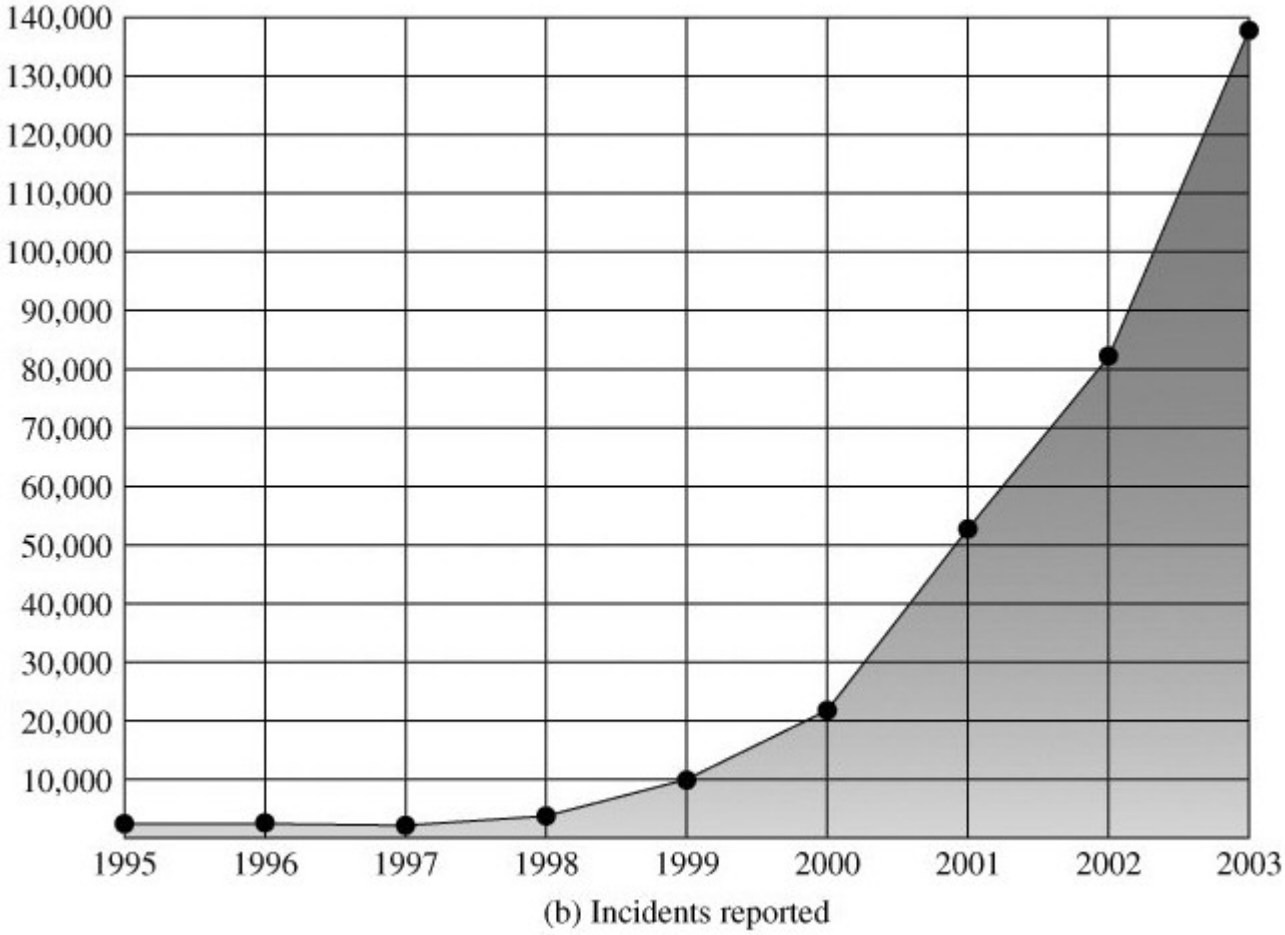
- slabosti na internetu (1995-2004), npr. sigurnosni propusti u operativnim sistemima, kao i slabosti mrežnih uređaja – CERT



(a) Vulnerabilities reported

Broj sigurnosnih incidenata

- broj incidenata prijavljenih CERT-u, npr. DoS napadi, lažna identifikacija korišćenjem IP adrese, prisluškivanje



(b) Incidents reported

Definicije

- ***Računarska sigurnost (Computer Security)*** – generičko ime za skup alata i mera napravljenih da zaštiti podatke u računaru i odvrati hakere
- ***Mrežna sigurnost (Network Security)*** – skup alata i mera za zaštitu podataka prilikom njihovog prenosa
- ***Internet sigurnost (Internet Security)*** – skup alata i mera da se zaštite podaci tokom njihovog prenosa preko više povezanih mreža (interneta)

Cilj kursa

- Fokus su ***internet sigurnost*** i ***računarska sigurnost*** sa aspekta povezanosti računara na internet
- Mere da se odvrati, spreči, otkriju i otklone narušavanja sigurnosti podataka, kako kod prenosa, tako i kod pamćenja i korišćenja u računaru

Metode zaštite

- Na visokom nivou moglo bi da se razmišlja o zaštiti na sledeći način:
  - **Polisa/politika**
  - **model pretnje**
  - **implementacija polise**
  - **krajnji cilj**

Polisa

- cilj koji treba postići
  - npr. samo Ana ima pravo da vidi sadržaj fajla X
- Obično se definiše na sledeći način:
  - koje su uloge,
  - koje su dozvoljene ili nedozvoljene operacije,
  - koji su objekti zaštićeni
    - npr. glasanje, fajl, mejl
  - uobičajeni ciljevi (FIPS PUB 199):
    - poverljivost, (**C**onfidentiality) – podataka i privatnost
    - integritet, (**I**ntegrity) – podataka i sistema
    - dostupnost (**A**vailability)
    - (autentičnost - **A**uthenticity, odgovornost i neporecivost **A**ccountability)

Model pretnje

- pretpostavka šta je napadač spreman i šta može da uradi
  - npr. može da pogađa šifre, ne može da ukrade server
  - bolja greška pretpostaviti da može nešto što ne može

Implementacija polise

- načini na koje se primenjuje polisa
  - npr. korisnički nalozi, šifre, enkripcija, pametna kartica za glasanje, digitalni potpis mejla, katanac za server
  - dve kategorije:
    - prevencija-ne dozvoliti da polisa bude narušena
      - npr. ograda, šifra, enkripcija
    - detekcija-detektovati kada je polisa narušena
      - npr. senzor pokreta, heš kod, detekcija upada, skener virusa
  - često postoji i mehanizam oporavka-ima ulogu zastrašivanja
    - npr. ukloniti uljeza, virus

Krajnji cilj

- Uspostaviti **implementaciju polise** koja će obezbediti da ne postoji način da protivnik u okviru **modela pretnje** naruši **polisu**

Razmatranja

- Zašto je teško?
  - Negativan cilj
- Ko je protivnik?
  - iznutra, spolja,...
- Šta napadač zna?
- Koje resurse napadač ima?

Корисничко име: *празно поље* Лозинка: ' OR 'a'='a

```
SELECT * FROM Users WHERE Username=''AND Password='' OR 'a'='a'
```

Razmatranja (2)

- Neki principi
  - nema savršenosti, slojevita zaštita, autorizacija svake operacije, podela uloga, edukacija
- Implementacija može da uključuje:
  - identifikaciju (username), autentikaciju (password), autorizaciju, fizičku zaštitu, kriptografiju, obmanu protivnika (honeypot), nepredvidivost i slučajnost (ključevi)
- Primeri problema: loša polisa, loš model pretnje, greške u implementaciji

Servisi, Mehanizmi, Napadi

- Potrebno je na sistematizovan način prikazati zahteve
- Postoji niz standarda koji definisu sigurnosne aspekte u računarskim sistemima i načine obezbeđivanja (X.800, RFC2828, ISO27001,...)
- Tri osnovna aspekta sigurnosti informacija (ITU-T X.800):
  - **Napad na sigurnost**
  - **Sigurnosni servis**
  - **Sigurnosni mehanizam**

OSI Sigurnosna Arhitektura

- ITU-T X.800 Sigurnosna arhitektura za OSI
- Predstavlja sistematski način da se definišu i omoguće sigurnosni zahtevi
- Pruža korisan i jednostavan pregled koncepata u oblasti zaštite

Napad na sigurnost

- Bilo koja akcija koja narušava sigurnost informacija u vlasništvu organizacije
- Informaciona sigurnost se odnosi na načine kako da se preduprede napadi, ili ako su se već dogodili, otkriju napadi na informaciono baziranim sistemima
- Izuzetno širok dijapazon napada
- Bitno je fokusirati se na generičke tipove napada
- Često se termini pretnja i napad koriste u istom značenju

Klasifikacija napada na sigurnost

- **Pasivni napadi** – prisluškivanje (presnimavanje) ili praćenje prenosa podataka u cilju:
  - Dobijanja sadržaja poruka ili
  - Praćenja/analize toka saobraćaja
- **Aktivni napadi** – modifikacija toka podataka ili podataka u cilju:
  - Lažnog predstavljanja jednog entiteta drugim entitetom
  - Ponovnog slanja prethodnih poruka
  - Promene poruka u prenosu
  - Odbijanja servisa

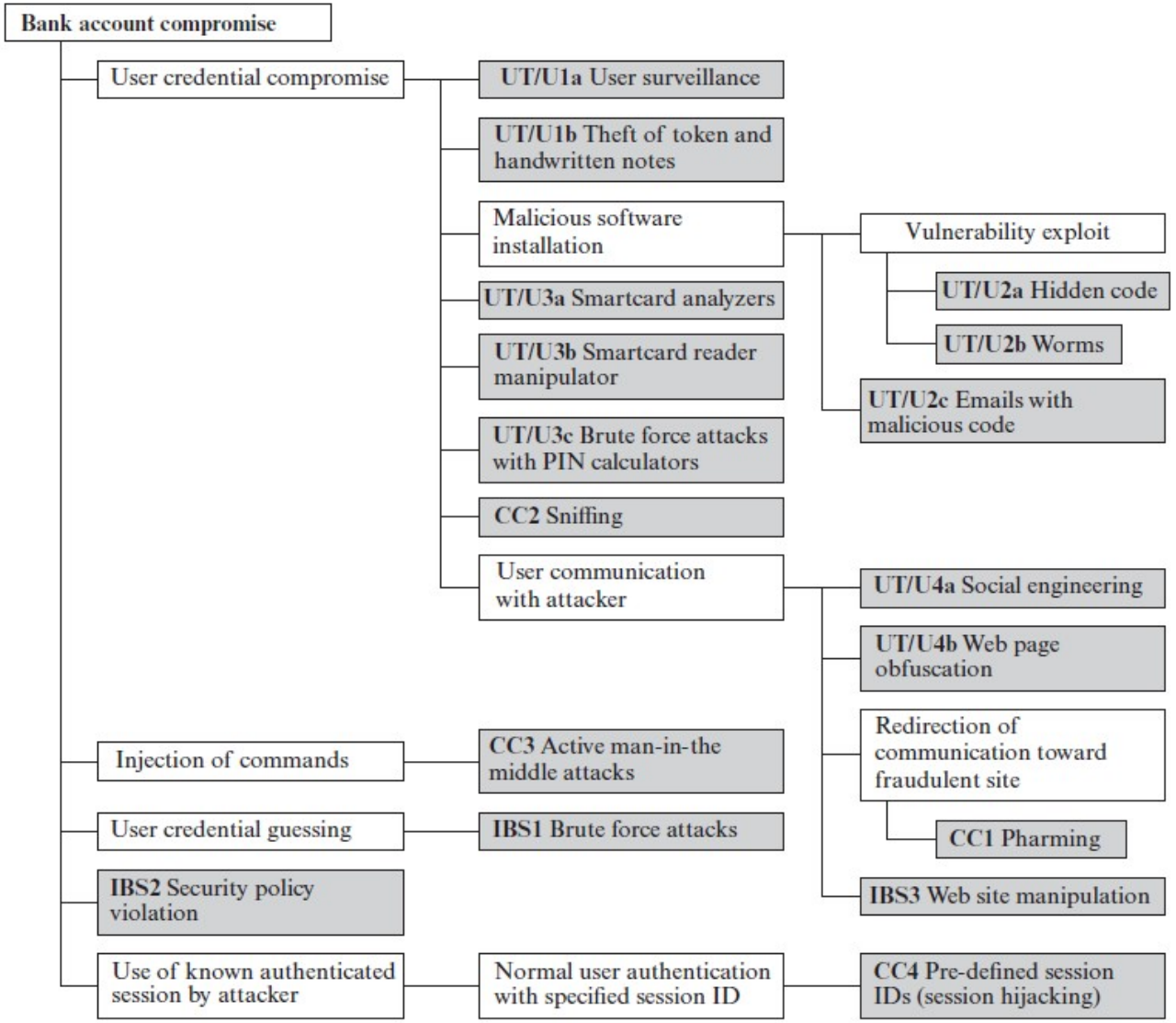
Pravci napada – attack surface

- Mrežni pravac – napadi preko mreže
- Softverski pravac – napadi preko softverskih slabosti
- Ljudski faktor – korišćenje naivnosti i neznanja
- (hardverski pravac) – da li možete da verujete da u hardveru nema skrivenih mana?
- Potrebno je pokriti analizom sve moguće pravce napada

Stabla napada – attack trees

- Metoda analize potencijalnih napada na sistem
- Analiziraju se svi mogući načini kako napadač može da dođe do cilja
- Pogodno za otkrivanje potencijalnih slabosti sistema

Stabla napada - primer



Sigurnosni Servis

- Servis koji poboljšava sigurnost obrade i prenosa podataka unutar neke organizacije (realne ili virtuelne)
- Prave se sa namerom da se suprotstave sigurnosnim napadima
- Koriste jedan ili više sigurnosnih mehanizama da obezbede servis
- Obezbede ekvivalentne funkcije onima koje postoje kod fizičkih dokumenata
  - Potpisi, datumi
  - Zaštita od otkrivanja sadržaja, preinačenja, uništenja
  - Provera (pisarnica), verifikacija ili svedočanstvo
  - Snimanje ili odobravanje

Definicije sigurnosnih servisa

- X.800 definiše kao servis obezbeđen kroz sloj protokola sistema u komunikaciji, koji obezbeđuje adekvatan nivo zaštite sistema ili prenosa podataka
- RFC 2828 definiše kao računarski ili komunikacioni servis pružen od strane sistema da pruži specifičan oblik zaštite sistemskih resursa
- X.800 ih razvrstava u 5 osnovnih kategorija

Kategorije sigurnosnih servisa (X.800)

- ***Autentikacija*** (***Authentication***)– utvrđivanje da je komunikacioni entitet onaj za koji se predstavlja (logička konekcija ili connectionless-email)
- ***Kontrola pristupa (Access Control)*** – sprečavanje neautorizovanog korišćenja resursa
- ***Tajnost podataka (Data Confidentiality)*** – zaštita podataka od neautorizovanog otkrivanja (logička konekcija, connectionless, polje ili tok saobraćaja)
- ***Intergitet podataka (Data Integrity)*** – uveravanje da je primljen podatak isti kao onaj poslat od autorizovanog entiteta (connection ili connectionless, cela ili polje)
- ***Neporecivost (Non-Repudiation)*** – zaštita od poricanja jednog od učesnika u komunikaciji (pošiljalac / primalac)
- **Dostupnost (Availability)**

Sigurnosni mehanizmi

- Mehanizam napravljen da otkrije ili spreči sigurnosni napad ili da oporavi nakon sigurnosnog napada
- Mora da postoji veliki broj mehanizama da bi se podržali zahtevi sigurnosnih servisa
- Najvažniji element koji podržava sigurnosne mehanizme su: kriptografske tehnike

Sigurnosni mehanizmi (X.800)

- Specifični sigurnosni mehanizmi:
  - Šifrovanje, digitalno potpisivanje, kontrola pristupa, integritet podataka, razmena autentikacije, dopunjavanje saobraćaja (paketa), kontrola rutiranja, provera validnosti kod arbitra
- Opšti sigurnosni mehanizmi:
  - Pouzdana funkcionalnost, sigurnosne labele - atribute, detekcija događaja, probe ispitivanja sigurnosti, sigurnosni oporavak

	Mehanizam							
Servis	**Šifrovanje**	**Digitalni potpis**	**Kontrola pristupa**	**Integritet podataka**	**Razmena autentikacije**	**Dodavanje saobraćaja**	**Kontrola rutiranja**	**Beleženje akcija korisnika**
Autentikacija učesnika	Y	Y			Y			
Autentikacija porekla podataka	Y	Y						
Kontrola pristupa			Y					
Tajnost	Y						Y	
Zaštita toka saobraćaja	Y					Y	Y	
Integritet podataka	Y	Y		Y				
Neporecivost		Y		Y				Y
Dostupnost				Y	Y			

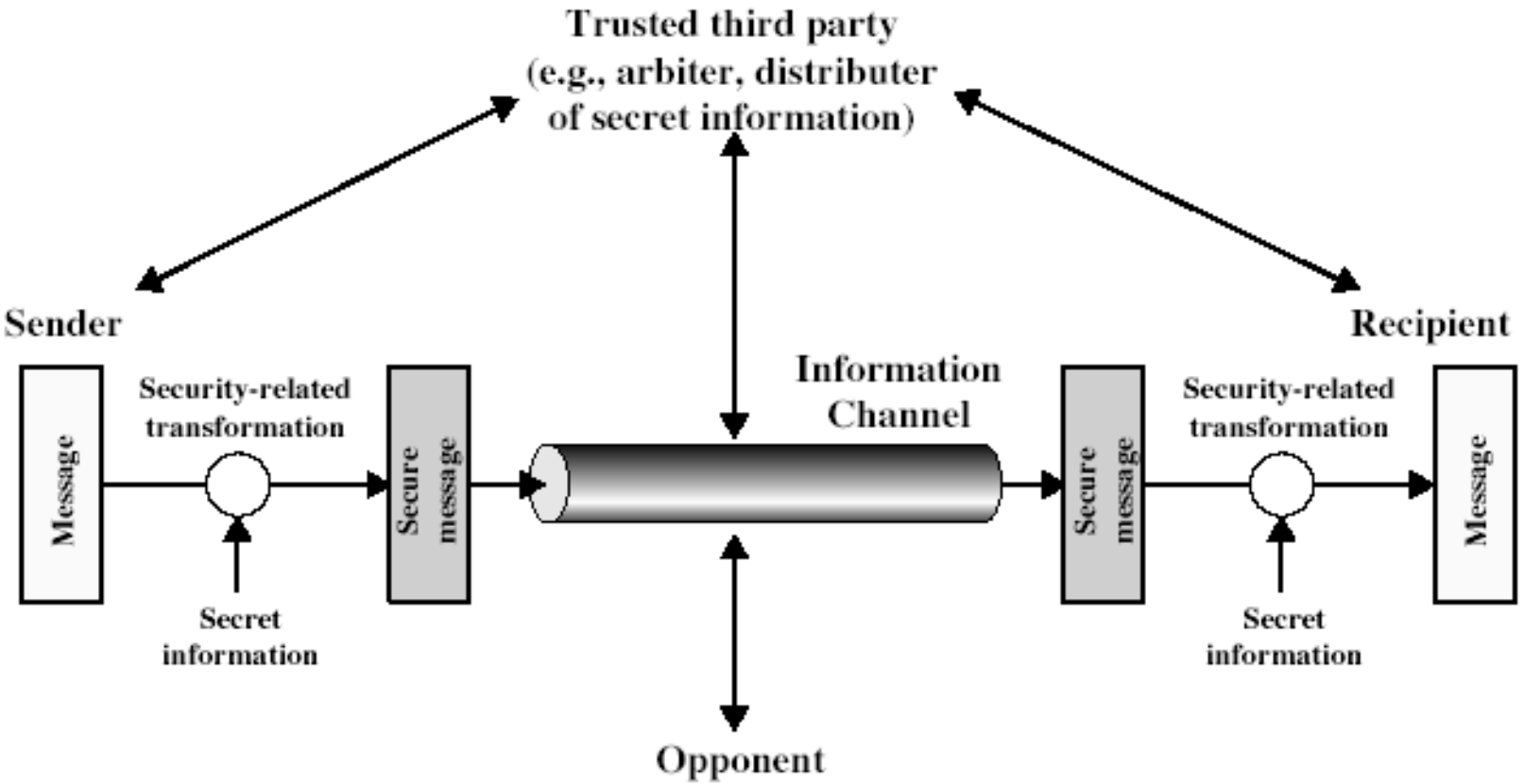
Principi dizajna sigurnih sistema

- Ekonomičnost, jednostavnost
- Podrazumevano ponašanje - bezbedno
- Pristup sistemu mora da se uvek proveri, ne koristiti zapamćene informacije
- Otvoreni dizajn mehanizama
- Razdvajanje privilegija
- Princip minimalnih privilegija

Principi dizajna sigurnih sistema (2)

- Minimalan broj zajedničkih mehanizama
- Psihološka prihvatljivost
- Izolacija (sistem za pristup od osetljivih podataka, procesi i fajlovi, sigurnosni mehanizmi)
- Enkapsulacija
- Modularnost
- Zaštita na svim slojevima (Layering)
- Ne zbunjivati korisnika

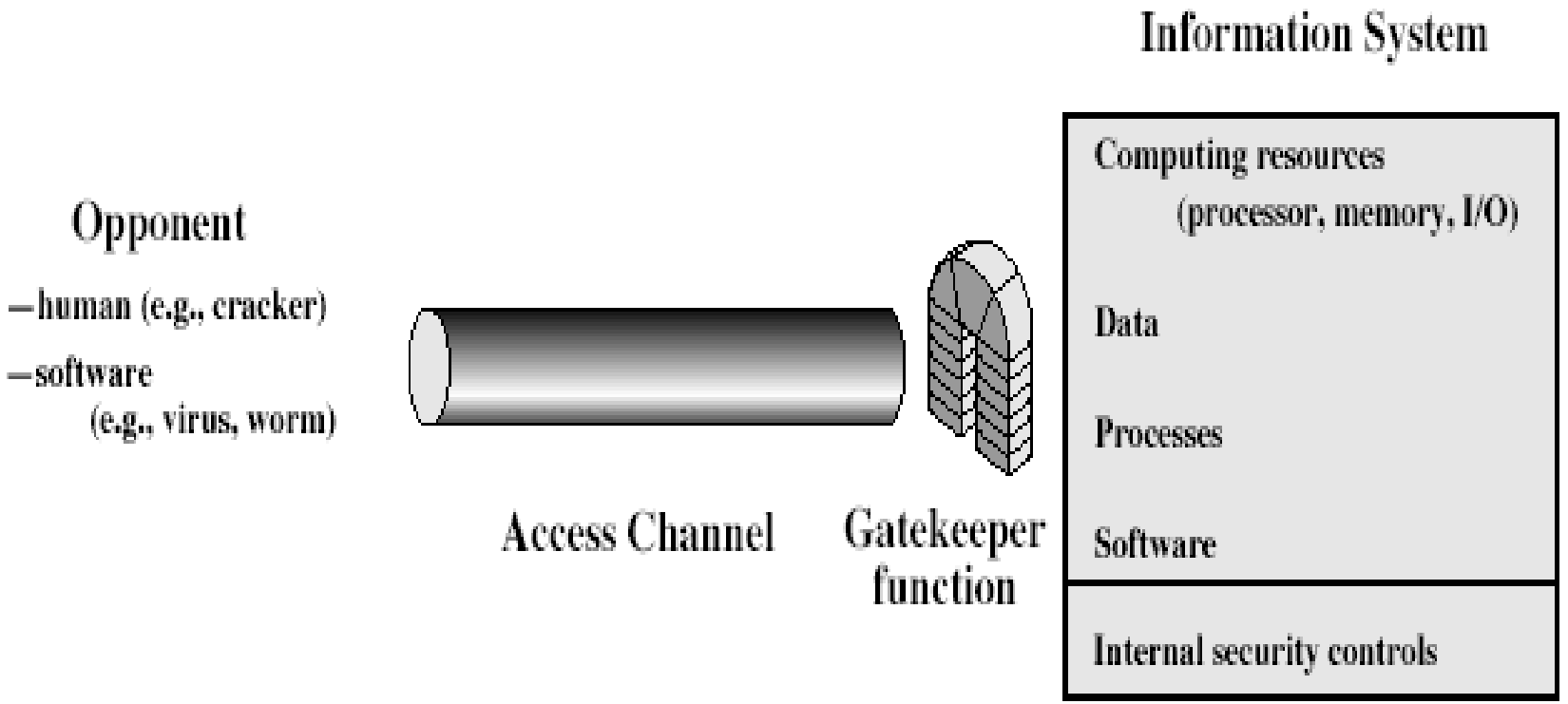
Model mrežne sigurnosti



Model mrežne sigurnosti

- Da bi se primenio model, neophodno je:
  - Projektovati odgovarajući algoritam za sigurnosnu transformaciju
  - Generisati tajnu informaciju (ključ) koji algoritam koristi
  - Razviti metode za distribuciju i deljenje tajne informacije (ključa)
  - Precizno odrediti protokol koji omogućava glavnim učesnicima da koriste transformaciju i tajnu informaciju za ostvarivanje sigurnosnog servisa

Model sigurnosti mrežnog pristupa



Model sigurnosti mrežnog pristupa

- Da bi se primenio model, neophodno je:
  - Izabrati odgovarajuće gatekeeper funkcije da se identifikuju korisnici
  - Primeniti sigurnosne kontrole da samo određeni autorizovani korisnici pristupaju određenoj informaciji ili resursu
- Računarski sistemi u koje imamo poverenje se mogu koristiti za implementaciju modela