Uvod u bezbjednost računarskih sistema

dr Slavica Tomović
Univerzitet Crne Gore

O čemu se radi?

- Ovaj kurs NIJE:
  - O tome kako postati haker
    - Iako možete naučiti neke korisne alate
- Kurs je o:
  - Fundamentalnim konceptima na kojima se bazira sigurnost računarskih sistema
  - Sigurnosnim mehanizmima ključnih mrežnih protokola
  - Principima razvoja “sigurnih”mrežnih aplikacija

Informacije o predmetu

- Predavač
  - Slavica Tomović
  - Elektrotehnički fakultet, UCG
  - E-mail: slavicat@ucg.ac.me
- Fond časova: 2+1
- Mjesto održavanja predavanja:
  - Sala 109
- Konsultacije:
  - Ponedeljkom, poslije časova (10h)
  - Lab. za telekomunikacije, ETF

Informacije o predmetu

- Način polaganja
  - Kolokvijum (50%)
  - Završni ispit (50%)
- Literatura:
  - Materijali sa predavanja
  - *Network Security Essentials: Applications and Standards, 6th Ed., William Stallings, Pearson, 2017.*
  - *Cryptography and Network Security Principles and Practice, 7th Ed., William Stallings, Pearson, 2017.*
  - *Computer Security: Principles and Practice, 4th Ed., William Stallings and Lawrie Brown, Pearson, 2017.*

Opis kursa

- Uvod u osnovne koncepte bezbjednosti računarskih sistema
- Raspored
  - Osnovni pojmovi i terminologija
  - Klasični kriptografski algoritmi
  - Simtrirčni kriptografski algortimi: DES, 3DES, AES
  - Asimetrični kriptografski algoritmi
  - Razmjena ključeva: Diffie-Hellman
  - Heš funkcije
  - MAC kodovi
  - Infrastruktura javnog ključa: X.509 sertifikati
  - Autentifikacija korisnika: Kerberos
  - Sigurnost transportnog sloja: TLS
  - Sistemska sigurnost: *Password*-i, virusi, detekcija upada, *firewall*

Značaj zaštite informacionog sistema

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

Značaj zaštite informacionog sistema

- Sigurnost podrazumijeva 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, e-uprava, ...) i da većina aplikacija i informacionih sistema koristi internet, to znači da postoji veliki broj sistema koji moraju da vode računa o sigurnosti.

Neki problemi koje treba riješiti

- Presrijetanje poruke i uvid u njen sadržaj
- Neovlašćeni pristup uređajima ili podacima
- Promjena prava pristupa
- Promjena sadržaja podataka
- Poricanje aktivnosti
- Prevare, ucjene, krađe, lažna obavještenja, uticaj na industrijske sisteme
- Sprečavanje dostupnosti usluga

Sigurnost informacija –povezani termini-

- Računarska sigurnost (*Computer Security*)
  - Skup alata dizajniranih da zaštite podatke na računaru (npr. od hakera)
  - Sigurnost operativnog sistema, infrastrukture
  - Sigurnost softvera: maliciozni softver, virusi
  - Kontrola pristupa: *login*, pristup fajlovima
  - *Firewall* zaštita
- Mrežna sigurnost (*Network security*)
  - Zaštita podataka prilikom prenosa
  - Ukoliko se podaci prenose preko više povezanih mreža često se upotrebljava termin **Internet sigurnost**
  - Mrežni protokoli, e-*commerce* aplikacije
  - Autentifikacija korisnika putem mreže
  - Mrežna kontrola pristupa, bezbjednost u *cloud* okruženju
- **Nema jasne granice između gore navedenih klasa sigurnosti!**
  - Npr. virus može biti importovan na sistem preko USB drajva ili optičkog diska, ali takođe i preko Interneta.

Mrežna sigurnost

mjere za sprečavanje, otkrivanje i ispravljanje sigurnosnih propusta prilikom prenosa informacija

Primjeri narušavanja mrežne sigurnosti

Primjer 1

- Korisnik A prenosi fajl korisniku B. Fajl sadrži osjetljive informacije (npr., evidencije o platnim spiskovima) koje treba zaštititi od objavljivanja. Korisnik C, koji nije ovlašćen da pristupa datoteki, može da nadzire prenos i snimi kopiju fajla prilikom prenosa.

Primjer 2

- Administrator mreže, D, prenosi poruku računaru E, koji je u njegovom administrativnom domenu. Poruka sadrži instrukcije za ažuriranje autorizacionog fajla koji sadrži identitite određenog broja korisnika kojima je odobren pristup ovom računaru. Korisnik F presrijeće poruku, mijenja njen sadržaj radi dodavanja ili brisanja unosa, a zatim proslijeđuje poruku računaru E, koji je prihvata kao da dolazi od administratora D i ažurira svoj autorizacioni fajl u skladu s tim.

Primjer 3

- Umjesto da presretne poruku, korisnik F kreira sopstvenu poruku sa željenim unosima i prenosi je računaru E lažno se predstavljajući kao administrator D. Računar E prihvata ovu poruku i mijenja svoj autorizacioni fajl.

Primjeri narušavanja mrežne sigurnosti

Primjer 4

- Zaposleni se otpušta bez najave. Menadžer firme šalje poruku serverskom sistemu kako bi izbrisao korisnički nalog zaposlenog. Nakon šte se korsnički nalog poništi, odgovarajuća potvrda se upisuje u log fajl servera. Međutim, zaposleni može presresti poruku i odložiti akciju dovoljno dugo tako da može preuzeti razne osjetljive informacije. Poruka se zatim prosljeđuje i potvrda uspješno izvršene akcije upisuje se u log fajl. Zlonamjerne aktivnosti zaposlenog mogu proći neopaženo dugo vremena.

Primjer 5

- Klijent šalje poruku brokeru sa uputstvima za razne transakcije koje želi da obavi. Naknadno investicije gube vrijednost i klijent negira slanje poruke.

Računarska sigurnost

- Zaštita koja se pruža automatizovanom informacionom sistemu u cilju postizanja očuvanja integriteta, dostupnosti i poverljivosti resursa informacionog sistema (hardver, softver, firmver, podaci i mrežni resursi)

Ciljevi računarske sigurnosti (CIA triada)

Povjerljivost (*Confidentiality*)

- Povjerljivost podataka
  - Obezbjeđuje da se privatne ili povjerljive informacije ne otkriju neovlašćenim pojedincima ili da im postanu dostupne.
- Privatnost
  - Obezbjeđuje da pojedinci kontrolišu ili utiču na to koje informacije koje se odnose na njih mogu da se prikupljaju i čuvaju, ko to može da radi, kao i kome te informacije mogu da se otkriju.

Integritet (*Integrity*)

- Integritet podataka
  - Obezbjeđuje da informacije i programi mogu da se mijenjaju jedino na određen i ovlašćen način.
- Integritet sistema
  - Obezbjeđuje da sistem izvršava funkciju za koju je namijenjen na neometan način, sprečavajući namjerno ili nenamjerno neovlašćeno manipulisanje sistemom.

Dostupnost (*Availability*)

- Obezbjeđuje efikasan rad sistema i da se ovlašćenim korisnicima ne uskraćuje usluga.

Izazovi zaštite računarskih sistema

- Sigurnost nije jednostavno postići
- Potencijalni nedostaci sigurnosnih mehanizama moraju se uzeti u obzir
- Neophodno je donijeti odluku o tome koji će se mehanizmi zaštite koristiti i gdje
- Bezbjednost zahtjeva redovno, čak neprestano nadgledanje sistema
- Razrađeni bezbjednosni mehanizmi postaju logični tek kad se uzmu u obzir raznovrsni aspekti prijetnje
- Sigurnosni mehanizmi obično uključuju više algoritama i protokola
- Riječ je o stalnoj intelektualnoj borbi kreatora sigurnosnih mehanizama i napadača
- Bezbjednost se još uvek suviše često razmatra naknadno, pa se ugrađuje u sistem pošto je projekat završen, umesto da bude sastavni dio procesa projektovanja
- Mnogi korisnici sigurnosne mehnizme smatraju preprekom za efikasan rad

Metode zaštite

- Na visokom nivou moglo bi da se razmišlja o zaštiti na sledeći način:
  - Polisa/politika
  - Model prijetnje
  - 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 podataka i privatnost
    - Integritet podataka i sistema
    - Dostupnost
    - Autentičnost (*Authenticity*), odgovornost i neporecivost (*Accountability*)

Model prijetnje

- Pretpostavka šta je napadač spreman i šta može da uradi
  - npr. može da pogađa šifre, ne može da ukrade server
  - bolja je pogriješiti tako što će se pretpostaviti da može nešto što ne može

Implementacija polise

- Načini primjene sigurnosnih polisa
  - npr. korisnički nalozi, šifre, enkripcija, pametna kartica za glasanje, digitalni potpis mejla…
  - dvije kategorije:
    - Prevencija - ne dozvoliti da polisa bude narušena
      - npr. *firewall*, 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 obezbijediti da ne postoji način da protivnik u okviru modela prijetnje naruši polisu

Razmatranja

- Ko je protivnik?
  - iznutra, spolja,...
- Šta napadač zna?
- Koje resurse napadač ima?
- Neki principi
  - nema savršenosti, slojevita zaštita, autorizacija svake operacije, podjela uloga, edukacija
- Implementacija može da uključuje:
  - identifikaciju (*username*), *autentikaciju* (*password*), autorizaciju, fizičku zaštitu, kriptografiju, obmanu protivnika (*honeypot*), nepredvidivost i slučajnost (ključevi)
- Primjeri problema: loša polisa, loš model prijetnje, greške u implementaciji

Servisi, Mehanizmi, Napadi

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

OSI Sigurnosna Arhitektura

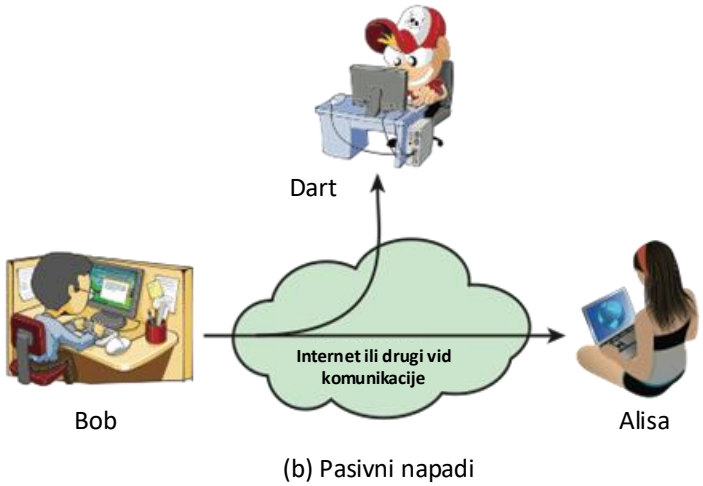
- ITU-T X.800
- Predstavlja sistematski način da se definišu i omoguće sigurnosni zahtjevi
- Pruža koristan i jednostavan pregled koncepata u oblasti zaštite (iz naše perspektive)
- Korisna za menadžere kao način za organizovanje zadataka staranja o bezbjednosti.
- Razvijena kao međunarodni standard
  - Proizvođači računara i komunikacione opreme prave bezbjedonosne funkcije za svoje proizvode i servise u skladu sa ovim standardom

OSI Sigurnosna Arhitektura

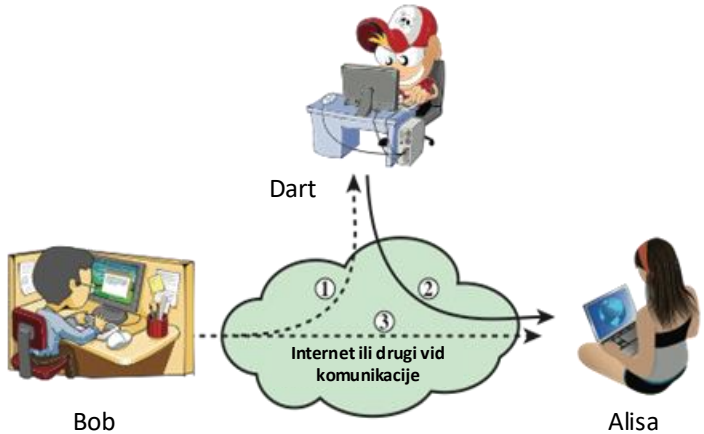
- Sigurnosni napad
  - Bilo koja akcija koja kompromituje bezbjednost informacije neke organizacije
  - Napad i prijetnja se često koriste u istom značenju
- Sigurnosni mehanizam
  - Proces (ili uređaj na kojem se izvršava proces ovog tipa) koji je dizajniran da detektuje i spriječi sigurnosni napad, ili da oporavi sistem nakon napada
- Sigurnosni servis
  - Servis obrade ili komunikacioni servis koji povećava sigurnost sistema za obradu podataka i prenos informacija
  - Namijenjeni su borbi protiv sigurnosnih napada i koriste jedan ili više sigurnosnih mehanizama

Klasifikacija napada

- X.800 i RFC 4949 klasifikuju napade na: *pasivne napade i aktivne napade*
- *Pasivni napad* pokušava da nabavi i iskoristi infromaciju koja se prenosi, ali ne utiče na resurse sistema
- *Aktivni napad* uključuje neku izmjenu toka podataka ili stvaranje lažnog toka



(b) Pasivni napadi



(b) Aktivni napadi

Pasivni napadi

- Prisluškivanje (presnimavanje) ili praćenje prenosa podataka
- Cilj napadača je da pribavi informaciju koja se prenosi
- Teško se otkrivaju

- Dva tipa pasivnih napada:
  - Otkrivanje sadržaja poruke
  - Analiza saobraćaja

Aktivni napadi

- Uključuju modifikacije toka podataka ili kreiranje novog lažnog toka podataka
- Teško ih je spriječiti zbog velike raznovrsnosti potencijalnih fizičkih, softverskih i mrežnih ranjivosti
- Cilj je otkriti napad i izvršiti oporavak od štete izazvane izmjenom podataka ili zakašnjelim podacima.

Maskiranje	• Lažno predstavljanje jednog entiteta drugim entitetom • Obično uključuje jedan od drugih oblika aktivnih napada
Ponavljanje	• Pasivno hvatanje jedinice podataka i njeno naknadno ponavljanje da bi se postigao neovlašćen efekat
Izmjena poruka	• Izmjena legitimne poruke, odlaganje slanja poruke ili izmjena redosleda poruka prilikom prenosa, sa ciljem neovlašćenog pristupa resursima
Uskraćivanje servisa (DoS – Denial of Service)	• Sprečava ili koči normalno korišćenje komunikacionih resursa ili upravljanje istim

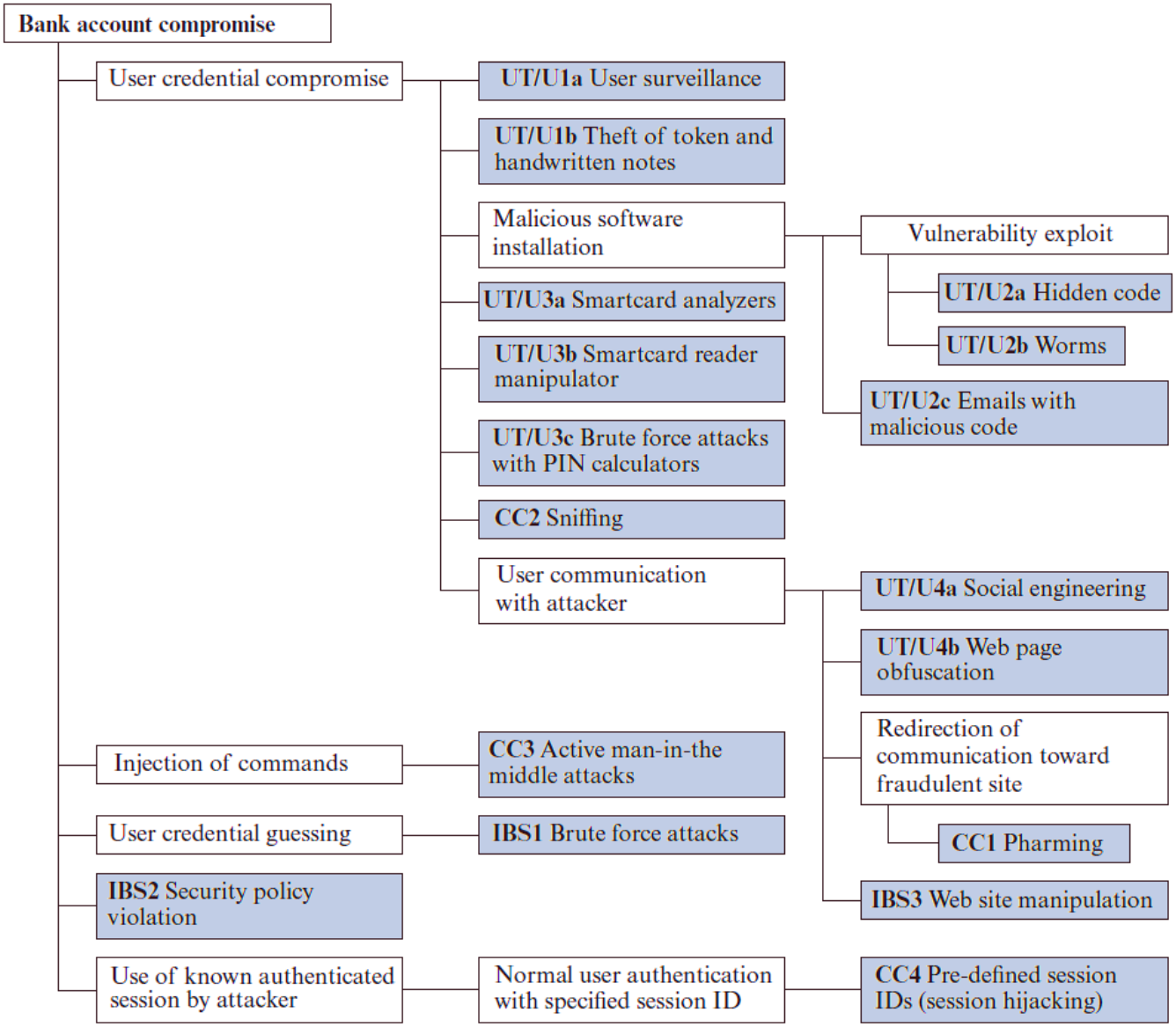
Pravci napada

1. Mrežni pravac – napadi preko mreže
2. Softverski pravac – napadi preko softverskih slabosti
3. Ljudski faktor – korišćenje naivnosti i neznanja

- Potrebno je pokriti analizom sve moguće pravce napada
- Primjeri:
  - Otvoreni porotovi na Web i drugim serverima
  - Servisi dostupni unutar *firewall* zone
  - Kod koji obrađuje dolazne podatke, email, XML, office dokumente i razne druge formate
  - Interfejsi, SQL, Web forme
  - Zaposleni koji imaju pristup osjetljivim podacima

Stablo napada

- Hijerarhijska struktura podataka u vidu stabla koja predstavlja skup potencijalnih tehnika za iskorištavanje sigurnosnih ranjivosti
- Meta napada predstavljena je kao korijen stabla, a načini na koje napadač može doći do svog cilja (mete) predstavljeni su kao grane stabla i pod-čvorovi stabla
- Završni čvorovi na rutama prema korijenu (listovi stabla) predstavljaju različite načine pokretanja napada
- Cilj je efikasno iskoristiti dostupne informacije o obrascima napada



Primjer stabla napada na autentifikaciju prilikom korišćenja Internet bankarstva

Sigurnosni servis

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

Definicije sigurnosnih servisa

- X.800 definicija: servis obezbijeđen kroz sloj protokola sistema u komunikaciji, koji nudi adekvatan nivo zaštite sistema ili prenosa podataka
- RFC 2828 definicija: računarski ili komunikacioni servis koji pruža specifičan oblik zaštite sistemskih resursa
- X.800 ih razvrstava u 5 osnovnih kategorija
  - Autentifikacija (*Authentication*)
  - Kontrola pristupa (*Access Control*)
  - Tajnost podataka (*Data Confidentiality*)
  - Integritet podataka (*Data Integrity*)
  - Neporecivost (*Non-Repudiation*)
  - Dostupnost (*Availability)*

Autentifikacija

- Utvrđivanje autentičnosti veze
  - U slučaju **pojedinačne poruke**, kao što je upozorenje ili signal alarma, funkcija servisa autentifikacije je da uvjeri primaoca da poruka potiče od izvora kako se tvrdi da jeste
  - U slučaju **interakcije u toku**, kao što je veza terminala sa računarom, postoje dva aspekta.
    - prilikom uspostavljanja veze, ovaj servis potvrđuje da su oba entiteta autentična (tj., da je svaki od entiteta taj koji tvrdi da jeste).
    - servis mora da osigura da se konekcija neće ometati od strane treće osobe koja se može maskirati u jednu od dvije legitimne strane da bi neovlašćeno prenosila ili preuzimala poruke.

Dva su specifična servisa autentifikacije definisana X.800 standardom:
• Autentifikacija ravnopravnih entiteta • Autentifikacija izvora podataka

Kontrola pristupa

- Mogućnost da se ograniči i kontroliše pristupanje računarskim sistemima i aplikacijama putem komunikacionih linkova
- Da bi se to postiglo, svaki entitet koji pokuša da dobije pristup mora najprije da se identifikuje, ili autentifikuje, da bi se prava pristupanja prilagodila pojedincu

Povjerljivost podataka

- Zaštita podataka koji se prenose od pasivnih napada
  - Najširi servis štiti sve korisničke podatke koji se prenose između dva korisnika tokom jednog vremenskog perioda
    - Na primer, kada se između dva sistema uspostavi TLS veza, ova "široka" zaštita sprečava otkrivanje bilo kojeg korisničkog podatka koji se prenosi preko TLS veze
  - Uži oblici ovog servisa uključuju zaštitu jedne poruke ili čak konkretnih polja unutar poruke
    - Manje korisno od šireg pristupa, a često i složenije i skuplje za primjenu.
- Zaštita toka saobraćaja od analize
  - Zahtjeva da napadač ne bude u stanju da na komunikacionoj infrastrukturi opazi izvor i odredište, frekvenciju, dužinu, i druge karakteristike saobraćaja

Integritet podataka

Može se odnositi na tok poruka, jednu poruku ili set polja unutar poruke

Servis integriteta orijentisan na vezu (*Connection-oriented*) postupa sa tokom poruka i osigurava da se poruke šalju i primaju bez dupliciranja, dodavanja, mijenjanja, promjena redosleda, ili ponavljanja.

Servis integriteta koji nije orijentisan na vezu (*connectionless*) odnosi se na pojedinačne poruke bez obzira na širi kontekst i uglavnom obezbjeđuje samo zaštitu od mijenjanja poruke.

Neporecivost

- Sprečava i pošiljaoca i primaoca da poreknu prenijetu poruku
- Kada se poruka pošalje, primalac može da dokaže da je navodni pošiljalac zaista poslao poruku
- Kada se poruka primi, pošiljalac može da dokaže da je navodni primalac zaista primio poruku

Dostupnost

- Servis dostupnosti je onaj koji štiti sistem tako da on bude dostupan
- Dostupnost - svojstvo sistema ili sistemskog resursa da bude dostupno i upotrebljivo na zahtjev ovlašćenih sistemskih entiteta, u skladu sa specifikacijom performansi za taj sistem
- Bavi se sigurnosnim problemima koji potiču od napada uskraćivanja usluge
- Zavisi od pravilnog upravljanja i kontrole sistemskim resursima, pa tako zavisi od servisa kontrole pristupa i drugih bezbjednosnih servisa

Sigurnosni mehanizmi

- Mehanizam napravljen da otkrije ili spriječi sigurnosni napad ili da oporavi sistem nakon napada
- Mora da postoji veliki broj mehanizama da bi se podržali zahtjvi sigurnosnih servisa
- Najvažniji element sigurnosnih mehanizama su kriptografske tehnike
- Podjela (X.800):
  - Specifični sigurnosni mehanizmi – mogu da se ugrade u određeni sloj protokola kako bi obezbijedili neki od OSI sigurnosnih servisa
  - Opšti sigurnosti mehanizmi –nijesu svojstveni nijednom OSI servisu niti sloju protokola

Sigurnosni mehanizmi

Specifični sigursnosni mehanizmi

- Enkripcija
- Digitalni potpis
- Kontrole pristupa
- Integritet podataka
- Razmjena autentifikacije
- Dopunjavanje paketa
- Kontrola rutiranja
- Validacija od strane arbitra

Opšti sigurnosni mehanizmi

- Pouzdana funkcionalnost
- Sigurnosne labele
- Detekcija događaja
- Probe ispitivanja sigurnosti
- Sigurnosni oporavak

Veza sigurnosnih servisa i mehanizama

Servis \ Mehanizam	Šifrovanje	Digitalni potpis	Kontrola pristupa	Integritet podataka	Razmjena autentifikacije	Popunjavanje saobraćaja	Kontrola rutiranja	Ovjeravanje
Autentifikacija ravnopravnih entiteta	Da	Da			Da			
Autentifikacija izvora podataka	Da	Da						
Kontrola pristupa			Da					
Povjerljivost	Da						Da	
Povjerljivost toka saobraćaja	Da					Da	Da	
Integritet podataka	Da	Da		Da				
Neporicanje		Da		Da				Da
Dostupnost				Da	Da			

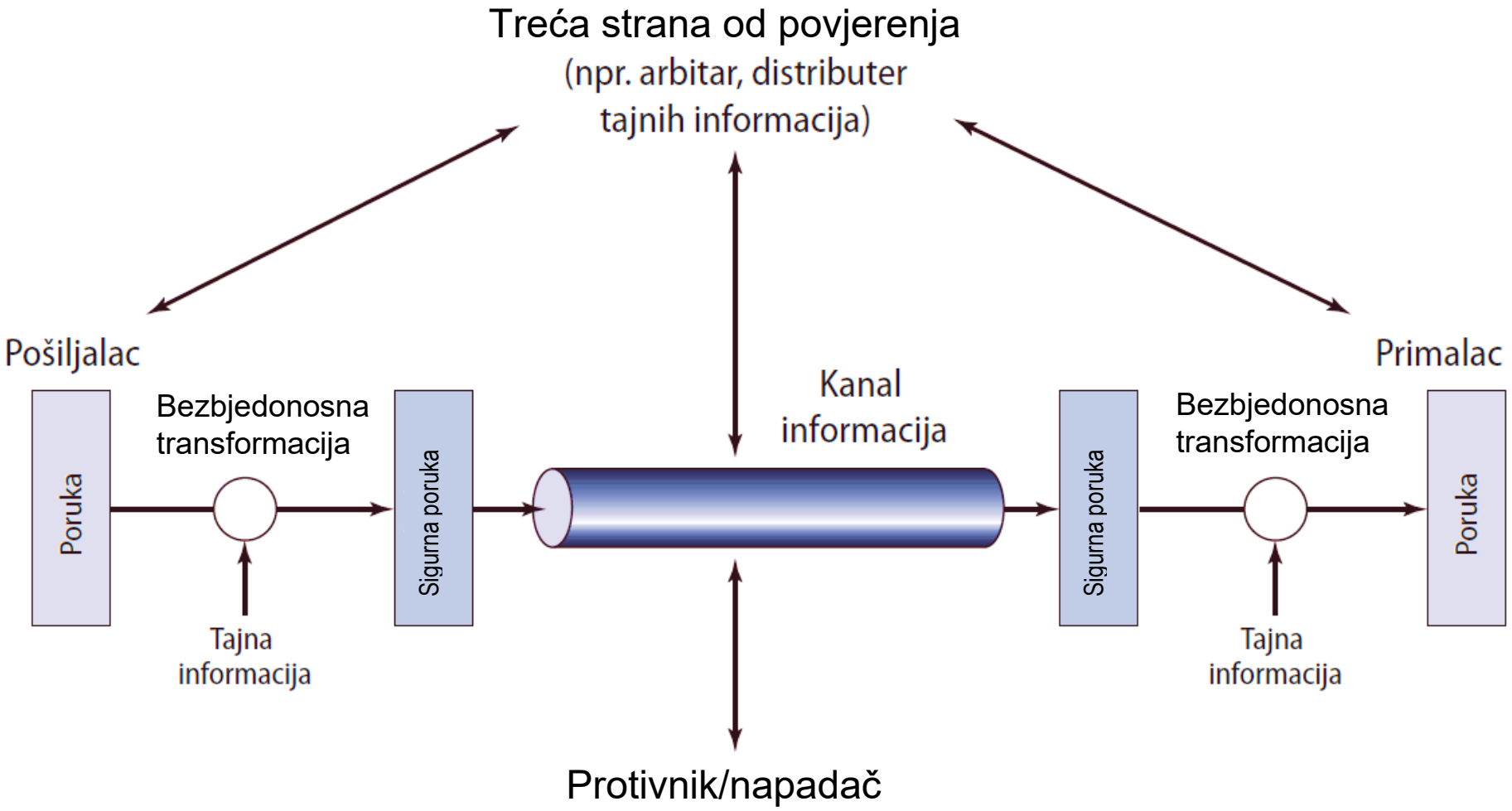
Principi dizajna sigurnih sistema

- Ekonomičnost, jednostavnost
- Podrazumjevano ponašanje – bezbjedno
- Pristup sistemu mora da se uvijek provjeri, ne koristiti zapamćene informacije
- Otvoreni dizajn mehanizama
- Razdvajanje privilegija
- Princip minimalnih privilegija

Principi dizajna sigurnih sistema

- Minimalan broj zajedničkih mehanizama
- Psihološka prihvatljivost
- Izolacija (osjetljivih podataka, procesa i fajlova, sigurnosnih mehanizama)
- Enkapsulacija
- Modularnost
- Zaštita na svim slojevima
- Ne zbunjivati korisnika

Model mrežne sigurnosti



Model mrežne sigurnosti

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

Model sigurnosti mrežnog pristupa

- Da bi se primijenio model, neophodno je:
  - Izabrati odgovarajuće *gejtekiper* funkcije koje definišu procedure prijavljivanja korisnika oslonjene na lozinke i logiku filtriranja projektovanu za otkrivanje i odbijanje crva, virusa i drugih sličnih napada
  - Primijeniti interne sigurnosne kontrole koje nadgledaju aktivnost i analiziraju skladištene informacije pokušavajući da otkriju prisustvo neželjenih uljeza

Neželjeni pristup

- Upad hakera na računarski sistem
- Postavljanje specifične logike u računarski sistem koja iskorišćava ranjivosti u sistemu i može da utiče na rad aplikacionih i pomoćnih programa, kao što su editori i kompajleri
- Programi mogu da predstavljaju dvije vrste prijetnji:
  - Prijetnje pistupanja informacijama
    - Presrijetanje ili mijenjanje podataka za potrebe korisnika koji ne bi trebalo da imaju pristup tim podacima.
  - Servisne prijetnje
    - Iskorišćavanje slabe tačke servisa u računaru da bi se legitimni korisnici ometali u korišćenju servisa

Rezime

- Koncepti računarske i mrežne sigurnosti
  - Definicija
  - Primjeri
  - Izazovi
- OSI sigurnosna arhitektura
- Napadi
  - Pasivni napadi
  - Aktivni napadi
- Pravci napada i stabla napada

- Sigurnosni servisi
  - Autentifikacija
  - Kontrola pristupa
  - Povjerljivost podataka
  - Integritet podataka
  - Neporecivost
  - Dostupnost
- Sigurnosni mehanizmi
- Fundamentalni principi dizajna sigurnih sistema
- Model mrežne sigurnosti
- Model sigurnosti mrežnog pristupa