POGLAVLJE 1

# UVOD

*Kombinacija prostora, vremena i snage koji se moraju uzeti u obzir kao osnovni elementi ove teorije odbrane čini to jednom prilično komplikovanom materijom. Prema tome, nije lako pronaći fiksnu polaznu tačku.*

*– O RATU, KARL FON KLAUZEVIC*

*Umetnost ratovanja uči nas da se ne uzdamo u verovatnoću da neprijatelj neće doći, već u vlastitu spremnost da ga dočekamo; ne u mogućnost da on neće da napadne, već pre u činjenicu da smo svoju poziciju učinili nesavladivom.*

*– UMETNOST RATOVANJA, SUN CU*

## CILJEVI UČENJA

Pošto proučite ovo poglavlje, trebalo bi da budete u stanju da:

- Opišete ključne bezbednosne zahteve poverljivosti, integriteta i raspoloživosti.
- Opišete vrste bezbednosnih pretnji i napada kojima se treba baviti i ponudite primere za vrste pretnji i napada koje se odnose na različite kategorije računarskih i mrežnih vrednosti.
- Rezimirate funkcionalne zahteve za bezbednost računara.
- Opišete bezbednosnu arhitekturu X.800 za OSI.

Zahtevi za **bezbednošću informacija** unutar organizacije doživeli su dve velike promene tokom poslednjih nekoliko desetina godina. Pre rasprostranjene upotrebe opreme za obradu podataka, bezbednost informacija koje su se smatrale dragocenim za organizaciju postizala se pre svega fizičkim i administrativnim sredstvima. Primer za prvo su bili teški ormani za kartoteke koji su imali bravu sa kombinacijom da bi se u njih stavljali osetljivi dokumenti. Primer zaštite administrativnim sredstvima bile su procedure za proveravanje osoblja prilikom zapošljavanja.

Sa uvođenjem računara, postala je očigledna potreba za automatizovanim alatkama za zaštitu fajlova i drugih informacija koje se čuvaju u računaru.To je pogotovo slučaj sa deljenim sistemima, kao što su sistemi sa deljenim vremenom, a potreba je još kritičnija kod sistema kojima može da se pristupa preko javne telefonske mreže, mreže podataka, ili preko Interneta. Generičko ime za kolekciju alatki projektovanih za zaštitu podataka i sprečavanje hakera je **bezbednost računara**.

Druga velika promena koja je imala uticaj na bezbednost je uvođenje distribuiranih sistema i upotreba mreža i sredstava komunikacija za prenošenje podataka od korisnika za terminalom do računara i među računarima. Bezbednosne mere na mreži potrebne su da bi se podaci zaštitili tokom prenošenja. U stvari, izraz **mrežna bezbednost** donekle dovodi u zabludu, jer praktično sve poslovne, upravne i akademske organizacije povezuju svoju opremu za obradu podataka jednom kolekcijom

međusobno povezanih mreža. Takva kolekcija se često naziva internetom[1], pa se koristi izraz **internet bezbednost**.

Ne postoji jasno razgraničenje ta dva oblika bezbednosti. Na primer, jedna vrsta napada na informacione sisteme o kojoj se najviše priča je računarski virus. Virus može da se unese u sistem fizički, ako stigne na optičkom disku pa se zatim učita u računar. Virusi mogu takođe da stignu preko interneta. U svakom slučaju, pošto se virus jednom nađe u sistemu računara, potrebne su interne računarske bezbednosne alatke za otkrivanje i oporavak od virusa.

Ova knjiga se usredsređuje na internet bezbednost, koja se sastoji od mera za odvraćanje, sprečavanje, otkrivanje i oporavak narušavanja bezbednosti koja se odnosi na prenošenje informacija. To je širok pojam koji pokriva mnoštvo mogućnosti. Da biste stekli utisak o područjima obuhvaćenim u ovoj knjizi, razmotrite sledeće primere narušavanja bezbednosti:

1. Korisnik A prenosi jedan fajl korisniku B. Fajl sadrži osetljive informacije (npr., platni spisak) koje moraju da se zaštite od obelodanjivanja. Korisnik C, koji nije ovlašćen za čitanje tog fajla, može da nadgleda prenos i napravi kopiju fajla za vreme prenosa.
2. Upravitelj mreže D, prenosi poruku u računar E, za koji je zadužen. Poruka naređuje računaru E da ažurira fajl ovlašćenja dodavanjem identiteta nekoliko novih korisnika kojima treba odobriti pristup tom računaru. Korisnik F presreće tu poruku, menja njen sadržaj dodavanjem ili brisanjem stavki, a zatim prosleđuje poruku računaru E, koji prihvata poruku kao da je potekla od upravitelja D i ažurira svoj fajl ovlašćenja u skladu sa njom.
3. Umesto da presretne poruku, korisnik F pravi vlastitu poruku od željenih stavki i prenosi tu poruku računaru E kao da je potekla od upravitelja D. Računar E prihvata poruku kao da potiče od upravitelja D i ažurira svoj fajl ovlašćenja u skladu sa njom.
4. Zaposleni dobija otkaz bez upozorenja. Kadrovski rukovodilac šalje poruku serverskom sistemu da se poništi nalog tog zaposlenog. Kada se izvrši poništavanje, server treba da pošalje obaveštenje u fajl zaposlenog kao potvrdu izvršene aktivnosti. Zaposleni uspeva da presretne poruku i zadrži je dovoljno dugo da još jednom pristupi serveru i izvuče osetljive informacije. Poruka se zatim prosleđuje, akcija poništenja se izvršava, i potvrda se evidentira. Postupak zaposlenog se možda još dugo neće primetiti.
5. Klijent šalje brokeru poruku sa instrukcijama za raznovrsne transakcije. Naknadno, investicijama pada vrednost i klijent poriče da je poslao poruku.

Mada ovaj spisak nikako ne iscrpljuje sve moguće vrste narušavanja bezbednosti, on ilustruje opseg briga u mrežnoj bezbednosti.

U ovom poglavlju daje se opšti pregled glavne teme i raspored materijala u preostalom delu knjige. Počinjemo sa opštim opisom servisa i mehanizama mrežne

[1] Izraz internet koristimo sa malim „i" kada se odnosi na bilo koju kolekciju međusobno povezanih mreža. Korporativni intranet je primer interneta. Internet sa velikim „I" može da bude jedna od funkcionalnosti koje neka organizacija koristi za izgradnju svojeg interneta.

bezbednosti i vrsta napada za koje su projektovani. Zatim razvijamo jedan opšti sveukupni model u okviru kojeg se mogu posmatrati servisi i mehanizmi bezbednosti.

## 1.1 POJMOVI BEZBEDNOSTI RAČUNARA

### Definicija bezbednosti računara

U priručniku NIST *Computer Security Handbook* [NIST95] se izraz *bezbednost računara* definiše kao

> **Bezbednost računara:** Zaštita koja se pruža automatizovanom informacionom sistemu sa ciljem da se postignu primenjivi ciljevi očuvanja integriteta, dostupnosti i poverljivosti resursa informacionog sistema (obuhvata hardver, softver, firmver, informacije/podatke i telekomunikacije).

Ovom definicijom predstavljaju se tri ključna cilja koja čine srž bezbednosti računara.

- **Poverljivost (Confidentiality):** Ovaj izraz obuhvata dva povezana pojma:

  **Poverljivost podataka:**[2] Obezbeđuje da se privatne ili poverljive informacije ne otkriju neovlašćenim pojedincima niti da im postanu dostupne.

  **Privatnost:** Obezbeđuje da pojedinci kontrolišu ili utiču na to koje informacije koje se odnose na njih smeju da se prikupljaju i čuvaju, ko to sme da radi, kao i to kome te informacije smeju da se otkriju.
- **Integritet (Integrity):** Ovaj izraz obuhvata dva povezana pojma:

  **Integritet podataka:** Obezbeđuje da informacije i programi mogu da se menjaju jedino na određen i ovlašćen način.

  **Integritet sistema:** Obezbeđuje da sistem izvršava funkciju za koju je namenjen na neometan način, slobodan od namernog ili nenamernog neovlašćenog manipulisanja sistemom.
- **Raspoloživost (Availability):** Obezbeđuje da sistemi rade bez odlaganja i da se ovlašćenim korisnicima ne uskraćuje usluga.

Ova tri pojma čine ono što se često naziva **CIA trijadom** (engl. *CIA triad*). Ta tri pojma obuhvataju osnovne ciljeve bezbednosti kako za podatke i informacije tako i za računarske usluge. Na primer, NIST *Standards for Security Categorization of Federal Information and Information Systems* (FIPS 199) navodi poverljivost, integritet i raspoloživost kao tri cilja bezbednosti za informacije i za informacione sisteme. FIPS 199

[2] RFC 4949 definiše *informaciju* kao „činjenice i ideje, koje mogu da se predstave (kodiraju) kao različiti oblici podataka," a podatke kao „informacije u određenom fizičkom predstavljanju, obično kao niz simbola koji nešto znače; pogotovo predstavljanja informacija koja mogu da se obrade ili proizvedu u računaru". U literaturi o bezbednosti ta razlika se obično ne naglašava, pa je tako i u ovoj knjizi.

daje jednu korisnu karakterizaciju ta tri cilja u smislu zahteva, kao i definiciju gubitka bezbednosti u svakoj od te tri kategorije.

- **Poverljivost:** Čuvanje ovlašćenih ograničenja za pristupanje informacijama i njihovo otkrivanje, uključujući sredstva za zaštitu lične privatnosti i vlasničkih informacija. Gubitak poverljivosti je neovlašćeno otkrivanje informacija.
- **Integritet:** Čuvanje od nepravilnog menjanja ili uništavanja informacija, uključujući obezbeđivanje neporecivosti i autentičnosti informacija. Gubitak integriteta je neovlašćeno menjanje ili uništavanje informacija.
- **Raspoloživost:** Obezbeđivanje pravovremenog i pouzdanog pristupa informacijama i korišćenja informacija. Nivo raspoloživosti se smanjuje usled poremećenog pristupa ili upotrebe informacija ili informacionog sistema.

Mada je za definisanje ciljeva bezbednosti već usvojena CIA triada, u oblasti bezbednosti neki smatraju da su za kompletnu sliku potrebni i dodatni pojmovi. Najčešće se pominju sledeća dva:

- **Autentičnost:** Svojstvo kojim se dokazuje originalnost, mogućnost provere i da se može verovati u validnost poslatih podataka, poruka, kao i u identitet pošiljaoca. To znači proveravanje da li su korisnici zaista oni za koje se predstavljaju i da svaki ulaz koji stiže u sistem potiče od izvora od poverenja.
- **Uračunljivost:** Cilj bezbednosti koji zahteva da se akcija jednog entiteta može ispratiti jedino do tog entiteta. Ovo podržava neporicanje, odvraćanje, izolovanje grešaka, otkrivanje i sprečavanje upada, kao i protivakcije oporavka i pravnog postupka. S obzirom na to da potpuno bezbedni sistemi još uvek nisu dostižan cilj, moramo biti u stanju da pronađemo trag do strane koja je odgovorna za povredu bezbednosti. Sistemi moraju da vode evidenciju svojih aktivnosti da bi se omogućila kasnija pravna analiza traga povrede bezbednosti ili kao pomoć u sporovima oko transakcija.

## Primeri

Sada dajemo nekoliko primera aplikacija koji ilustruju upravo nabrojane zahteve[3]. Za ove primere koristimo tri nivoa uticaja na organizacije ili pojedince u slučaju povrede bezbednosti (npr., gubitka poverljivosti, integriteta, ili raspoloživosti). Ti nivoi su definisani u FIPS 199:

- **Nizak:** Od gubitka se očekuje ograničen negativan uticaj na rad organizacije, na sredstva organizacije, ili na pojedince. Ograničen negativan uticaj znači da, na primer, gubitak poverljivosti, integriteta, ili raspoloživosti može (i) da dovede do degradacije sposobnosti obavljanja zadataka u meri i trajanju u kojem je organizacija u stanju da obavlja svoje osnovne funkcije, ali je efikasnost funkcija primetno umanjena; (ii) da dovede do manjih šteta na sredstvima organizacije;

[3] Ovi primeri uzeti su iz dokumenta bezbednosne polise koji je objavila kancelarija za bezbednost i privatnost informacione tehnologije (Information Technology Security and Privacy Office) univerziteta Purdue.

(iii) da dovede do manjih finansijskih gubitaka; ili (iv) da dovede do manje štete za pojedince.

- **Srednji:** Od gubitka se očekuje ozbiljan negativan uticaj na rad organizacije, na sredstva organizacije, ili na pojedince. Ozbiljan negativan uticaj znači da, na primer, gubitak može (i) da dovede do značajne degradacije sposobnosti obavljanja zadataka u meri i trajanju u kojem je organizacija u stanju da obavlja svoje osnovne funkcije, ali je efikasnost funkcija značajno umanjena; (ii) da dovede do značajnih šteta na sredstvima organizacije; (iii) da dovede do značajnih finansijskih gubitaka; ili (iv) da dovede do značajne štete za pojedince koja ne uključuje gubitak života ili ozbiljne ozlede opasne po život.
- **Visok:** Od gubitka se očekuje opasan ili katastrofalan negativan uticaj na rad organizacije, na sredstva organizacije, ili na pojedince. Opasan ili katastrofalan negativan uticaj znači da, na primer, gubitak može (i) da dovede do opasne degradacije ili do gubitka sposobnosti obavljanja zadataka u meri i trajanju u kojem organizacija nije u stanju da obavlja jednu ili više od svojih osnovnih funkcija; (ii) da dovede do ozbiljne štete na sredstvima organizacije; (iii) da dovede do ozbiljnih finansijskih gubitaka; ili (iv) da dovede do opasne ili katastrofalne štete za pojedince koja uključuje gubitak života ili ozbiljne ozlede opasne po život.

**Poverljivost** Informacije o ocenama studenata predstavljaju vrednost čiju poverljivost studenti smatraju veoma značajnom. U SAD-u, objavljivanje takvih informacija regulisano je zakonom o privatnosti (Family Educational Rights and Privacy Act, FERPA). Informacije o ocenama moraju biti dostupne jedino studentu, njegovim roditeljima i zaposlenima kojima je ta informacija nephodna u njihovom poslu. Informacije o upisu studenata mogu da imaju srednju ocenu poverljivosti. Mada su pokrivene zakonom FERPA, ove informacije svakodnevno vidi više ljudi, manja je verovatnoća da će biti napadnute nego informacije o ocenama, i njihovo otkrivanje dovodi do manje štete. Informacijama imenika (kao što su spiskovi studenata, fakultetski spiskovi, ili spiskovi odeljenja) može se dodeliti niska ocena poverljivosti ili mogu da budu bez ocene. Ove informacije su obično slobodno raspoložive javnosti i objavljuju se na školskom veb sajtu.

**Integritet** Nekoliko aspekata integriteta ilustruje primer informacije o alergijama pacijenta u bolnici, koja se čuva u bazi podataka. Doktor bi morao da bude u stanju da se pouzda u ispravnost i ažurnost ove informacije. Pretpostavimo sada da neki zaposleni (npr., medicinska sestra) koja ima pravo da vidi i ažurira ove informacije namerno falsifikuje podatak da bi naudila bolnici. Baza podataka mora brzo da se vrati na pouzdano stanje, i za grešku mora biti moguće pronaći trag do osobe koja je odgovorna za nju. Informacije o alergijama pacijenta predstavljaju primer vrednosti sa visokim zahtevom za integritetom. Neprecizna informacija može da dovede do ozbiljne opasnosti ili do smrti pacijenta i da izloži bolnicu visokim zahtevima za odštetu.

Primer vrednosti kojoj se može odrediti srednji nivo zahtevanog integriteta je veb sajt koji sadrži forum gde registrovani korisnici diskutuju o nekoj konkretnoj temi. Registrovani korisnik ili haker bi mogao da falsifikuje neke stavke ili da nagrdi veb sajt. Ako taj forum svojim korisnicima služi samo za zabavu, donosi malu ili nikakvu

zaradu od oglašavanja, a ne koristi se za nešto važno kao što je istraživanje, potencijalna šteta nije velika. Administrator bi mogao da pretrpi gubitak nekih podataka, finansijski gubitak i gubitak vremena.

Primer sa niskim zahtevom za integritet je anonimno onlajn glasanje. Mnogi veb sajtovi, kao što su novinske organizacije, nude svojim korisnicima ta glasanja uz veoma malo zaštite. Međutim, netačnost i nenaučnost takvih glasanja se podrazumeva.

**Raspoloživost** Što je komponenta ili servis kritičniji, zahteva se viši nivo raspoloživosti. Razmotrite sistem koji pruža usluge autentifikacije za kritične sisteme, aplikacije i uređaje. Prekid servisa dovodi do nemogućnosti da klijenti pristupe računarskim resursima i da osoblje pristupi resursima koji su potrebni za obavljanje kritičnih poslova. Gubitak usluge dovodi do velikog finansijskog gubitka zbog smanjene produktivnosti zaposlenih i potencijalni gubitak klijenata.

Primer vrednosti koja bi mogla da se oceni srednjom zahtevanom raspoloživošću je javni veb sajt univerziteta; ovaj veb sajt pruža informacije za trenutne i moguće studente i donatore. Takav sajt ne predstavlja kritičnu komponentu informacionog sistema univerziteta, ali može biti neugodno ako nije raspoloživ.

Aplikacija za onlajn pretraživanje telefonskog imenika može da se klasifikuje niskom zahtevanom raspoloživošću. Mada privremeni gubitak ove aplikacije može da bude dosadna stvar, postoje i drugi načini da se dođe do tih informacija, kao što je štampani imenik ili služba u centrali.

## Izazovi bezbednosti računara

Bezbednost računara i mreža je i očaravajuća i složena. Neki od razloga su:

1. Bezbednost nije tako jednostavna kao što bi početniku mogla da izgleda. Zahtevi izgledaju jasni; zaista, većina glavnih zahteva za uslugu bezbednosti može da se opiše samorazumljivim pojmovima od jedne reči: poverljivost, autentifikacija, neporicanje i integritet. Ali mehanizmi kojima se ti zahtevi ispunjavaju mogu da budu prilično složeni, a za njihovo razumevanje može da bude potrebno prilično suptilno rezonovanje.
2. Kod projektovanja konkretnog bezbednosnog mehanizma ili algoritma, moraju uvek da se razmotre potencijalni napadi na to odbrambeno sredstvo. U mnogim slučajevima, uspešni napadi se projektuju tako što se problem razmatra na sasvim drugačiji način, pa se tako iskoristi neka neočekivana slabost mehanizma.
3. Zbog tačke 2, procedure koje se koriste za pružanje određenih usluga često izgledaju nelogične. Uobičajeno je da bezbednosni mehanizam bude složen, a iz navođenja konkretnog zahteva nije očigledno da su potrebne tako razrađene mere. Razrađeni bezbednosni mehanizmi postaju logični tek kad se uzmu u obzir raznovrsni aspekti pretnje.
4. Pošto se izgrade razni bezbednosni mehanizmi, neophodno je doneti odluku gde da se oni primene. To se odnosi kako na fizičku lokaciju (npr., na kojim tačkama u mreži je određeni bezbednosni mehanizam potreban) tako i u logičkom smislu [npr., u kojem sloju ili u kojim slojevima arhitekture kao što je TCP/IP (Transmission Control Protocol/Internet Protocol) treba mehanizme postaviti].

5. Bezbednosni mehanizmi obično ne uključuju samo jedan algoritam ili protokol. Oni takođe zahtevaju da učesnici poseduju neku tajnu informaciju (npr., ključ za šifrovanje), pa se postavlja pitanje pravljenja, distribucije i zaštite te tajne informacije. Takođe može da postoji i oslanjanje na komunikacione protokole čije ponašanje može da komplikuje zadatak razvijanja bezbednosnog mehanizma. Na primer, ako se za ispravno funkcionisanje bezbednosnog mehanizma zahteva postavljanje vremenskih ograničenja za prenos poruke od pošiljaoca do primaoca, onda svaki protokol ili mreža koja uvodi promenljiva, nepredvidiva odlaganja može da obesmisli takvo vremensko ograničenje.
6. Bezbednost računara i mreže je u suštini intelektualna borba između napadača koji pokušava da otkrije rupe i projektanta ili administratora koji pokušava da ih zatvori. Velika prednost na strani napadača je to što je njemu dovoljno da pronađe samo jednu slabu tačku, dok projektant mora da pronađe i eliminiše sve slabe tačke da bi postigao savršenu bezbednost.
7. Korisnici i menadžeri sistema prirodno su skloni da ne uviđaju korist od investiranja u bezbednost sve dok se ne desi otkaz bezbednosti.
8. Bezbednost zahteva redovno, čak neprestano nadgledanje, a to je teško u današnjim kratkoročnim preopterećenim okruženjima.
9. Bezbednost se još uvek suviše često razmatra naknadno, pa se ugrađuje u sistem pošto je projekat završen, umesto da bude sastavni deo procesa projektovanja.
10. Mnogi korisnici (pa čak i administratori bezbednosti) posmatraju jaku bezbednost informacionog sistema ili korišćenja informacija kao smetnju efikasnom radu koji je blizak korisniku.

Upravo nabrojane teškoće nalazićemo na različite načine dok u ovoj knjizi budemo ispitivali različite bezbednosne pretnje i mehanizme.

## 1.2 OSI ARHITEKTURA BEZBEDNOSTI

Da bi se pravilno ocenile bezbednosne potrebe jedne organizacije i da bi se procenili i odabrali različiti bezbednosni proizvodi i polise, menadžeru zaduženom za bezbednost računara i mreže potreban je neki sistematski način za definisanje zahteva za bezbednošću i za pojedinačno opisivanje pristupa za zadovoljenje tih zahteva.

To je teško već u centralizovanom okruženju za obradu podataka; sa uvođenjem lokalne i regionalne mreže, problemi se uvećavaju.

Preporuka ITU-T[4] X.800, *Security Architecture for OSI*, definiše jedan takav sistematski pristup[5]. OSI arhitektura bezbednosti je korisna za menadžere kao način

[4] Sektor za standardizaciju telekomunikacija (ITU-T, Telecommunication Standardization Sector) međunarodne unije za telekomunikacije (ITU, International Telecommunication Union) je agencija koju sponzorišu Ujedinjene nacije i koja razvija standarde, koji se zovu preporuke (Recommendations), i koji se odnose na telekomunikacije i na međusobno povezivanje otvorenih sistema (OSI, open systems interconnection).

[5] OSI arhitektura bezbednosti razvijena je u kontekstu arhitekture OSI protokola, opisanog u Dodatku D. Međutim, za potrebe u ovom poglavlju nije potrebno poznavanje arhitekture OSI protokola.

**Tabela 1.1** Pretnje i napadi (RFC 4949)

| |
|---|
| **Pretnja** |
| Potencijal za narušavanje bezbednosti, koji postoji kada postoji prilika, sposobnost, akcija, ili događaj koji bi mogao da probije bezbednost i prouzrokuje štetu. To jest, pretnja je moguća opasnost koja može da iskoristi neku ranjivost. |
| **Napad** |
| Napad na bezbednost sistema koji potiče od razumne pretnje. To jest, razumna radnja kao nameran pokušaj (pogotovo u smislu metoda ili tehnike) da se izbegnu bezbednosni servisi i povredi polisa bezbednosti nekog sistema. |

za organizovanje zadatka staranja o bezbednosti. Štaviše, pošto je ova arhitektura razvijena kao međunarodni standard, dobavljači računara i komunikacija prave bezbednosne funkcije svojih proizvoda i servisa koji se povezuju sa ovom strukturisanom definicijom servisa i mehanizama.

Za naše potrebe, OSI arhitektura bezbednosti predstavlja koristan, mada apstraktan, pregled mnogih pojmova kojima se ova knjiga bavi. OSI arhitektura bezbednosti usredsređena je na bezbednosne napade, mehanizme i servise. Oni se mogu ukratko definisati kao:

- **Bezbednosni napad:** Svaka aktivnost koja ugrožava bezbednost informacija u vlasništvu organizacije.
- **Bezbednosni mehanizam:** Proces (ili uređaj u kojem se nalazi takav proces) projektovan za otkrivanje, sprečavanje, ili oporavak od bezbednosnog napada.
- **Bezbednosni servis:** Servis za obradu ili komunikaciju koji unapređuje bezbednost sistema za obradu podataka i prenosa informacija jedne organizacije. Servisi su namenjeni za suprotstavljanje bezbednosnim napadima, a za pružanje te usluge koriste jedan bezbednosni mehanizam ili više njih.

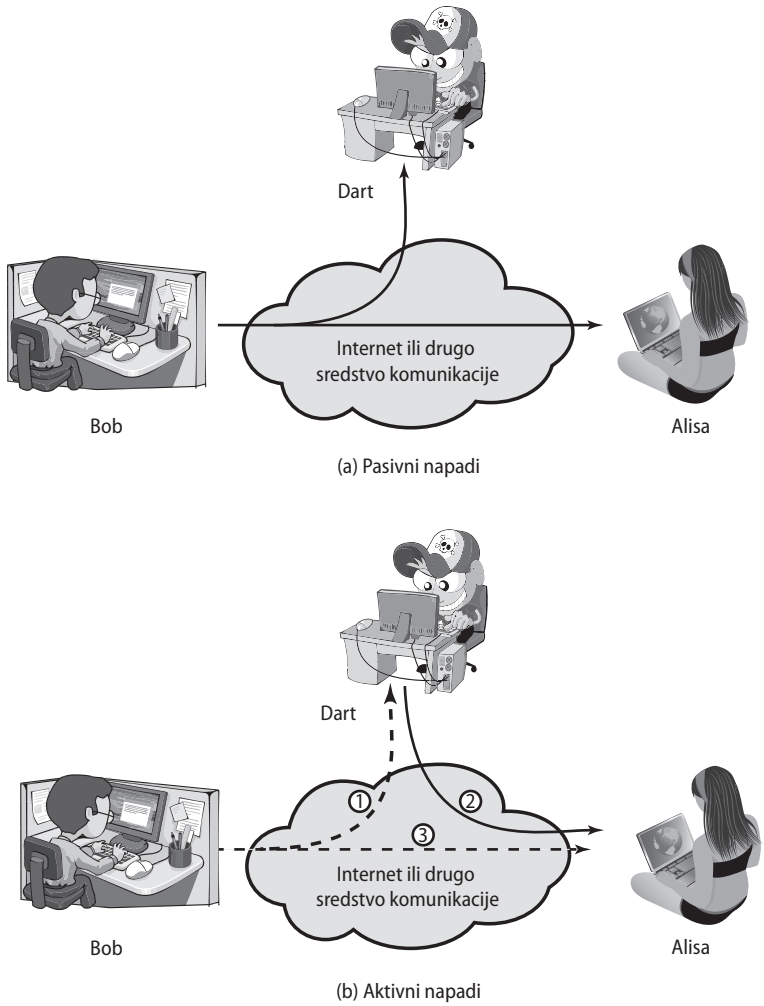
U literaturi, izrazi *pretnja* i *napad* obično se koriste u manje više istom smislu. Tabela 1.1 sadrži definicije uzete iz dokumenta RFC 4949, glosara bezbednosti na internetu (*Internet Security Glossary*).

## 1.3 BEZBEDNOSNI NAPADI

Jedan koristan način za klasifikaciju bezbednosnih napada, koji se koristi i u X.800 i u RFC 4949, je podela na *pasivne napade* i na *aktivne napade*. Pasivan napad pokušava da sazna ili da iskoristi informaciju iz sistema ali ne utiče na sistemske resurse. Aktivni napad pokušava da izmeni sistemske resurse ili da utiče na njihov rad.

### Pasivni napadi

Pasivni napadi (slika 1.1a) su kao prisluškivanje, ili nadgledanje prenosa. Cilj protivnika je da pribavi informaciju koja se prenosi. Dve vrste pasivnih napada su otkrivanje sadržaja poruke i analiza saobraćaja.




**Slika 1.1** Bezbednosni napadi

**Otkrivanje sadržaja poruke** je lako razumljivo. Telefonski razgovor, poruka elektronske pošte, i fajl koji se prenosi mogu da sadrže osetljive ili poverljive informacije. Mi bismo hteli da sprečimo da protivnik sazna sadržaj ovih prenosa.

Druga vrsta pasivnog napada, **analiza saobraćaja**, je suptilnija. Pretpostavimo da imamo način da maskiramo sadržaj poruka ili drugog saobraćaja informacija tako da protivnici, sve i da uhvate poruku, ne mogu da izvuku informaciju iz nje. Uobičajena tehnika za maskiranje sadržaja je šifrovanje. Ako smo uspostavili zaštitu šifrovanjem, protivnik ipak može da uoči šablon tih poruka. Protivnik bi mogao da odredi lokaciju i identitet računara u komunikaciji i mogao bi da uoči učestalost i dužinu razmenjenih poruka. Te informacije bi mogle da mu budu korisne da nasluti prirodu komunikacije koja se odvija.

Pasivni napadi se veoma teško otkrivaju, zato što ne dolazi ni do kakve izmene podataka. Obično se saobraćaj poruka šalje i prima na naizgled normalan način, pa ni pošiljalac ni primalac nisu svesni da je još neko pročitao poruku ili uočio šablon komunikacije. Međutim, izvodljivo je da se spreči uspeh takvih napada, obično pomoću šifrovanja. Prema tome, u borbi sa pasivnim napadima, naglasak je na sprečavanju a ne na otkrivanju.

### Aktivni napadi

Aktivni napadi (slika 1.1b) uključuju neku izmenu toka podataka ili stvaranje lažnog toka i mogu da se podele na četiri kategorije: maskiranje, ponavljanje, izmena poruka i uskraćivanje usluga.

**Maskiranje (Masquerade)** se dešava kada se jedan entitet pretvara da je neki drugi entitet (putanja 2 na slici 1.1b je aktivan napad). Napad maskiranjem obično uključuje i jedan od ostalih oblika aktivnog napada. Na primer, moguće je uhvatiti sekvencu autentifikacije i ponoviti je nakon izvršenja važeće autentifikacije, pa ovlašćeni entitet sa manje privilegija može da pribavi dodatne privilegije tako što se predstavi kao entitet koji ima te veće privilegije.

**Ponavljanje (Replay)** uključuje pasivno hvatanje jedinice podataka i njeno naknadno ponavljanje da bi se postigao neovlašćen efekat (putanje 1, 2, i 3 aktivnog napada).

**Izmena poruka (Modification of messages)** jednostavno znači da se promeni neki deo legitimne poruke, ili da se poruke odlože ili im se izmeni redosled, da bi se proizveo neovlašćen efekat (putanje 1 i 2 aktivnog napada). Na primer, poruka koja glasi „Dozvoliti da John Smith čita poverljivi fajl `nalozi`" izmeni se u „Dozvoliti da Fred Brown čita poverljivi fajl `nalozi`."

**Uskraćivanje usluga (DoS, Denial of Service)** sprečava ili koči normalno korišćenje komunikacionih sredstava ili njihovo upravljanje (putanja 3 aktivnog napada). Ovaj napad može da ima konkretan cilj; na primer, jedan entitet može da obustavi sve poruke usmerene na određeno odredište (npr., servis praćenja bezbednosnih događaja). Drugi oblik uskraćivanja usluge je poremećaj cele mreže—bilo da se mreža onemogući, bilo da se preoptereti porukama tako da se degradiraju performanse.

Aktivni napadi imaju karakteristike suprotne pasivnim napadima. Dok se pasivni napadi teško otkrivaju, postoje mere koje sprečavaju njihov uspeh. Na drugoj strani, aktivne napade je teško potpuno sprečiti zbog velike raznovrsnosti potencijalnih fizičkih, softverskih i mrežnih ranjivosti. Umesto toga, cilj je da se aktivni napadi otkriju i da se izvrši oporavak od štete izazvane promenjenim ili odloženim podacima. Ukoliko otkrivanje ima zastrašujući efekat, može takođe da doprinese prevenciji.

## 1.4 BEZBEDNOSNI SERVISI

X.800 definiše bezbednosni servis kao servis koji pruža jedan sloj protokola otvorenog komunikacionog sistema i koji obezbeđuje adekvatnu bezbednost sistema ili transfera podataka. Možda je jasnije definisanje u dokumentu RFC 4949, u kojem se nalazi sledeća definicija: Servis obrade ili komunikacije koji pruža sistem da bi sistemskim

**Tabela 1.2** Bezbednosni servisi (X.800)

| AUTENTIFIKACIJA | INTEGRITET PODATAKA |
|---|---|
| Pouzdanost da je entitet u komunikaciji onaj koji tvrdi da jeste.<br><br>**Autentifikacija ravnopravnih entiteta**<br>Koristi se kod logičke veze radi uverenja u identitet povezanih entiteta.<br><br>**Autentifikacija izvora podataka**<br>U transferu bez direktnog uspostavljanja veze, pruža pouzdanost da je izvor primljenih podataka taj koji tvrdi da jeste. | Pouzdanost da su primljeni podaci tačno isti onakvi kakve je poslao ovlašćeni entitet (tj, da ne sadrže nikakve izmene, dodavanja, brisanja niti ponavljanja).<br><br>**Integritet veze sa oporavljanjem**<br>Omogućava integritet svih korisničkih podataka u vezi i otkriva svaku izmenu, dodavanje, brisanje, ili ponavljanje bilo kojih podataka u celom nizu podataka, sa pokušajem oporavka.<br><br>**Integritet veze bez oporavljanja**<br>Kao prethodno, ali omogućava samo otkrivanje bez oporavljanja.<br><br>**Integritet veze selektivna polja**<br>Omogućava integritet izabranih polja u korisničkim podacima bloka podataka koji se prenosi u vezi i utvrđuje da li su izabrana polja menjana, dodavana, brisana ili ponovljena.<br><br>**Integritet bez direktnog povezivanja**<br>Omogućava integritet pojedinačnog bloka podataka bez direktnog uspostavljanja veze i može da utvrdi da li je bilo izmene podataka. Dodatno je moguće obezbediti ograničeno otkrivanje ponavljanja.<br><br>**Integritet bez direktnog povezivanja – selektivna polja**<br>Omogućava integritet izabranih polja u okviru pojedinačnog bloka podataka bez direktnog uspostavljanja veze; može da utvrdi da li je bilo izmene odabranih polja. |
| **KONTROLA PRISTUPA**<br>Sprečavanje neovlašćenog korišćenja resursa (tj, ovaj servis kontroliše ko sme da pristupa resursu, pod kojim uslovima može doći do pristupanja, i šta smeju da rade oni koji pristupaju resursu). | **NEPORICANJE**<br>Pruža zaštitu od poricanja jednog od entiteta uključenih u komunikaciju da su učestvovali u jednom delu ili u celoj komunikaciji.<br><br>**Neporicanje, Izvor**<br>Dokaz da je poruku poslala navedena strana.<br><br>**Neporicanje, Odredište**<br>Dokaz da je poruku primila navedena strana. |
| **POVERLJIVOST PODATAKA**<br>Zaštita podataka od neovlašćenog obelodanjivanja.<br><br>**Poverljivost sa direktnom vezom**<br>Zaštita svih korisničkih podataka u vezi.<br><br>**Poverljivost bez direktnog povezivanja**<br>Zaštita svih korisničkih podataka u pojedinačnom bloku podataka.<br><br>**Poverljivost – selektivna polja**<br>Poverljivost izabranih polja u korisničkim podacima u vezi ili u pojedinačnom bloku podataka.<br><br>**Poverljivost toka saobraćaja**<br>Zaštita informacija koje se mogu izvući iz posmatranja tokova saobraćaja. | |

resursima pružio konkretnu vrstu zaštite; bezbednosni servisi primenjuju bezbednosne polise i primenjuju se pomoću bezbednosnih mehanizama.

X.800 deli ove servise na pet kategorija i četrnaest konkretnih servisa (tabela 1.2). Razmotrićemo sve pojedinačne kategorije[6].

[6] Ne postoji opšta saglasnost o mnogim izrazima koji se koriste u literaturi o bezbednosti. Na primer, izraz integritet ponekad se koristi tako da se odnosi na sve aspekte bezbednosti informacija. Izraz autentifikacija ponekad se koristi tako da se odnosi kako na proveru identiteta tako i na različite funkcije navedene u ovom poglavlju kao integritet. Ovde se koristi u skladu sa X.800 i RFC 4949.

## Autentifikacija

Servis **autentifikacije** bavi se obezbeđivanjem da veza bude autentična. U slučaju pojedinačne poruke, kao što je upozorenje ili signal alarma, funkcija servisa autentifikacije je da uveri 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. Najpre, prilikom uspostavljanja veze, ovaj servis potvrđuje da su oba entiteta autentična (tj., da je svaki od entiteta taj koji tvrdi da jeste). Drugo, servis mora da obezbedi da se veza ne ometa tako da se neko treći maskira u jednu od dve legitimne strane da bi neovlašćeno prenosio ili preuzimao poruke.

U X.800 definišu se dva konkretna servisa autentifikacije:

- **Autentifikacija ravnopravnih entiteta:** Obezbeđuje potvrdu identiteta ravnopravnog entiteta u pridruživanju. Dva entiteta se smatraju ravnopravnim ako primenjuju isti protokol u različitim sistemima (npr., dva TCP modula u dva sistema koji su u vezi). Autentifikacija ravnopravnih entiteta se obezbeđuje za korišćenje prilikom uspostavljanja veze ili u fazi transfera podataka. Ona pokušava da obezbedi poverenje da entitet nije maskiran niti da neovlašćeno ponavlja neku raniju vezu.
- **Autentifikacija izvora podataka:** Obezbeđuje potvrdu izvora jedinice podataka. Ne pruža zaštitu od dupliciranja ili menjanja jedinica podataka. Ova vrsta servisa podržava aplikacije kao što je elektronska pošta, gde nema prethodnih interakcija među entitetima koji komuniciraju.

## Kontrola pristupa

U kontekstu mrežne bezbednosti, **kontrola pristupa** je mogućnost da se pristupanje računarskim sistemima i aplikacijama putem komunikacionih linkova ograniči i kontroliše. Da bi se to postiglo, svaki entitet koji pokuša da dobije pristup mora najpre da se identifikuje, ili autentifikuje, da bi se prava pristupanja prilagodila pojedincu.

## Poverljivost podataka

**Poverljivost** je zaštita podataka koji se prenose od pasivnih napada. S obzirom na sadržaj prenosa podataka, može se prepoznati nekoliko nivoa zaštite. Najširi servis štiti sve korisničke podatke koji se prenose između dva korisnika tokom jednog vremenskog perioda. Na primer, kada se između dva sistema uspostavi SSL veza, ova široka zaštita sprečava otkrivanje bilo kojeg korisničkog podatka koji se prenosi preko SSL veze. Moguće je takođe definisati uže oblike ovog servisa, uključujući zaštitu jedne same poruke ili čak konkretnih polja unutar poruke. Takvo rafiniranje je manje korisno od šireg pristupa i može da bude složenije i skuplje za primenu.

Drugi aspekt poverljivosti je zaštita toka saobraćaja od analize. To zahteva da napadač ne bude u stanju da na sredstvu za komunikaciju opazi izvor i odredište, frekvenciju, dužinu, i druge karakteristike saobraćaja.

## Integritet podataka

Isto kao poverljivost, **integritet** može da se primeni na tok poruka, na pojedinačnu poruku, ili na izabrana polja unutar poruke. I ovde, najkorisniji i najjednostavniji pristup je potpuna zaštita toka.

Servis integriteta orijentisan na vezu postupa sa tokom poruka i osigurava da se poruke šalju i primaju bez dupliciranja, dodavanja, menjanja, promena redosleda, ili ponavljanja. Ovaj servis obuhvata i uništavanje podataka. Prema tome, servis integriteta orijentisan na vezu odnosi se kako na menjanje toka poruka tako i na DoS (uskraćivanje usluge). Na drugoj strani, servis integriteta bez direktnog uspostavljanja veze odnosi se na pojedinačne poruke bez obzira na širi kontekst i uglavnom obezbeđuje samo zaštitu od menjanja poruke.

Može se povući razlika između servisa sa obnavljanjem i bez njega. Pošto se servis integriteta odnosi na aktivne napade, bavimo se otkrivanjem a ne sprečavanjem. Ako se otkrije kršenje integriteta, servis može jednostavno da prijavi to kršenje, a za obnavljanje je potreban neki drugi deo softvera ili ručna intervencija. Alternativno, postoje mehanizmi za oporavak od gubitka integriteta podataka, kao što ćemo kasnije videti. Ugrađivanje mehanizama za automatizovano obnavljanje obično je privlačnija alternativa.

## Neporecivost

**Neporicanje** sprečava i pošiljaoca i primaoca da poreknu prenetu poruku. Tako, kada se poruka pošalje, primalac može da dokaže da je navodni pošiljalac zaista poslao poruku. Slično tome, kada se poruka primi, pošiljalac može da dokaže da je navodni primalac zaista primio poruku.

## Servis raspoloživosti

I X.800 i RFC 4949 definišu **raspoloživost** kao svojstvo sistema ili sistemskog resursa da bude dostupno i upotrebljivo na zahtev ovlašćenih sistemskih entiteta, u skladu sa specifikacijom performansi za taj sistem (tj., sistem je raspoloživ ako obezbeđuje usluge prema dizajnu sistema kad god to korisnici zatraže). Različiti napadi mogu da dovedu do gubitka ili do smanjenja raspoloživosti. Neki od ovih napada rešavaju se automatskim protivmerama, kao što su autentifikacija i šifrovanje, dok drugi zahtevaju neku vrstu fizičke akcije za sprečavanje ili za oporavak od gubitka raspoloživosti elemenata jednog distribuiranog sistema.

X.800 tretira raspoloživost kao svojstvo koje se vezuje za različite bezbednosne servise. Međutim, logično je pozvati jedan konkretan servis raspoloživosti. Servis raspoloživosti je onaj koji štiti sistem tako da ovaj bude raspoloživ. Taj servis se bavi bezbednosnim problemima koji potiču od napada uskraćivanja usluge. On zavisi od pravilnog upravljanja i kontrole sistemskih resursa pa tako zavisi od servisa kontrole pristupa i drugih bezbednosnih servisa.

## 1.5 BEZBEDNOSNI MEHANIZMI

Tabela 1.3 navodi bezbednosne mehanizme definisane u X.800. Mehanizmi su podeljeni na one koji se primenjuju u nekom konkretnom sloju protokola, kao što je TCP ili protokol sloja aplikacija, i one koji nisu svojstveni nekom konkretnom sloju protokola ili bezbednosnom servisu. Ti mehanizmi će biti obrađeni na odgovarajućim mestima u knjizi, pa ih sada nećemo razrađivati osim komentarom definicije šifrovanja. X.800

**Tabela 1.3** Bezbednosni mehanizmi (X.800)

| KONKRETNI BEZBEDNOSNI MEHANIZMI<br>Mogu da se ugrade u odgovarajući sloj protokola radi obezbeđivanja nekog od servisa OSI bezbednosti. | PRODORNI BEZBEDNOSNI MEHANIZMI<br>Mehanizmi koji nisu svojstveni nijednom određenom servisu OSI bezbednosti niti sloju protokola. |
|---|---|
| **Šifrovanje**<br>Primena matematičkih algoritama za pretvaranje podataka u neki oblik koji nije lako razumljiv. Transformacija i posle toga obnavljanje podataka zavise od jednog algoritma i ni od jedog ili od nekoliko ključeva za šifrovanje. | **Pouzdana funkcionalnost**<br>Ono što se smatra ispravnim što se tiče nekog kriterijuma (npr., uspostavljeno bezbednosnom polisom). |
| **Digitalni potpis**<br>Podaci koji se dodaju na kraj, ili kriptografska transformacija podataka, jedinica podataka koja omogućava primaocu jednice podataka da proveri izvor i integritet jedinice podataka i zaštita od falsifikovanja (npr., primaoca). | **Bezbednosna oznaka**<br>Oznaka vezana za neki resurs (koji može da bude i jedinica podataka) koja imenuje ili označava bezbednosne atribute tog resursa. |
| **Kontrola pristupa**<br>Raznovrsni mehanizmi koji nameću pravila pristupanja resursima. | **Otkrivanje događaja**<br>Otkrivanje događaja relevantnih za bezbednost. |
| **Integritet podataka**<br>Raznovrsni mehanizmi koji se koriste za obezbeđivanje integriteta jedinice podataka ili toka jedinica podataka. | **Praćenje bezbednosnih događaja**<br>Podaci prikupljeni i potencijalno upotrebljeni da bi se olakšalo bezbednosno praćenje, a to je nezavisan pregled i ispitivanje sistemskih evidencija i aktivnosti. |
| **Razmena autentifikacije**<br>Mehanizam namenjen za proveru identiteta nekog entiteta pomoću razmene informacija. | **Bezbednosno obnavljanje**<br>Rešava zahteve mehanizama, kao što su obrada događaja i funkcije upravljanja, i preduzima akcije obnavljanja. |
| **Popunjavanje saobraćaja**<br>Ubacivanje bitova u praznine toka podataka radi ometanja pokušaja da se analizira saobraćaj. | |
| **Kontrola rutiranja**<br>Omogućava biranje konkretne fizički bezbedne rute za određene podatke i dozvoljava izmenu rutiranja, pogotovo ako se sumnja na narušavanje bezbednosti. | |
| **Overavanje**<br>Korišćenje treće strane od poverenja za obezbeđivanje određenih svojstava razmene podataka. | |

**Tabela 1.4** Odnos između bezbednosnih servisa i mehanizama

| Servis \ Mehanizam | Šifrovanje | Digitalni potpis | Kontrola pristupa | Integritet podataka | Razmena autentifikacije | Popunjavanje saobraćaja | Kontrola rutiranja | Overavanje |
|---|---|---|---|---|---|---|---|---|
| Autentifikacija ravnopravnih entiteta | Da | Da | | | Da | | | |
| Autentifikacija izvora podataka | Da | Da | | | | | | |
| Kontrola pristupa | | | Da | | | | | |
| Poverljivost | Da | | | | | | Da | |
| Poverljivost toka saobraćaja | Da | | | | | Da | Da | |
| Integritet podataka | Da | Da | | Da | | | | |
| Neporicanje | | Da | | Da | | | | Da |
| Raspoloživost | | | | Da | Da | | | |

razlikuje reverzibilne i ireverzibilne mehanizme šifrovanja. Reverzibilan mehanizam šifrovanja je jednostavan algoritam šifrovanja koji omogućava da se podaci šifruju i nakon toga dešifruju. U ireverzibilne mehanizme šifrovanja spadaju heš algoritmi i šifre za autentifikaciju poruka, koji se koriste u aplikacijama za digitalne potpise i autentifikaciju poruka.

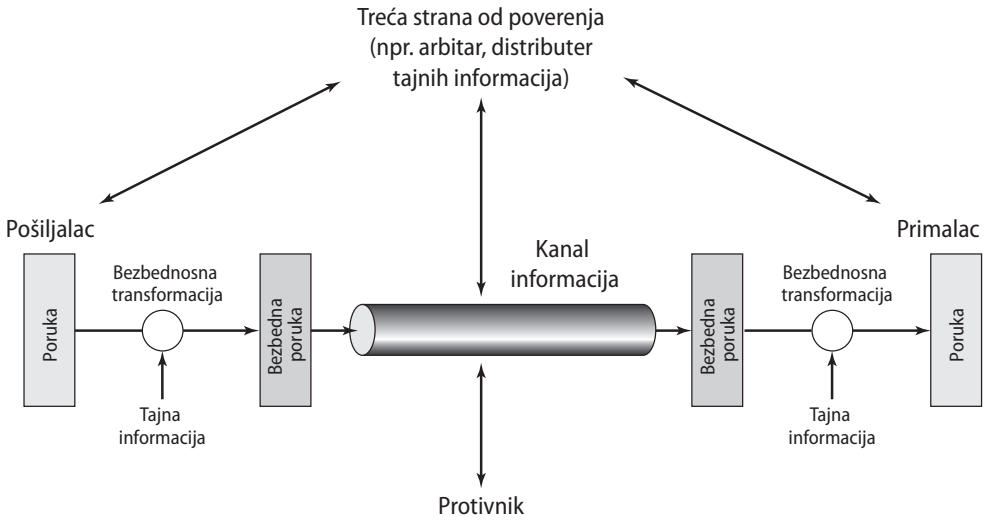
Tabela 1.4, zasnovana na jednoj tabeli iz X.800, pokazuje odnos između bezbednosnih servisa i bezbednosnih mehanizama.

## 1.6 MODEL ZA MREŽNU BEZBEDNOST

Model za veliki deo onoga o čemu ćemo raspravljati obuhvaćen je, na veoma uopšten način, na slici 1.2. Poruka treba da se prenese od jedne strane na drugu preko neke vrste Internet servisa. Dve strane, to su *glavni učesnici* (*principali*) u ovoj transakciji, moraju da sarađuju da bi se razmena izvršila. Logički kanal informacija uspostavlja se definisanjem rute kroz Internet od izvora do odredišta i tako što ova dva principala kooperativno koriste komunikacione protokole (npr., TCP/IP).

Bezbednosni aspekti ulaze u igru kada je neophodno ili poželjno da se prenos informacija zaštiti od protivnika koji može da predstavlja pretnju po poverljivost, autentičnost i tako dalje. Sve tehnike za pribavljanje bezbednosti imaju dve komponente:

1. Bezbednosnu transformaciju informacije koja treba da se pošalje. Primeri su šifrovanje poruke, koje tako izokrene poruku da ona bude nečitka za protivnika,




**Slika 1.2** Model za mrežnu bezbednost

i dodavanje šifre zasnovane na sadržaju poruke, koja može da se upotrebi za potvrdu identiteta pošiljaoca.

2. Neku tajnu informaciju zajedničku za oba principala a, nadamo se, nepoznatu protivniku. Primer je ključ za šifrovanje koji se koristi u spoju sa transformacijom za izokretanje poruke pre prenosa i za ispravljanje posle prijema[7].

Za bezbedan prenos može da bude potrebna treća strana od poverenja. Na primer, treća strana može da bude zadužena da distribuira tajne informacije ovim principalima i krije ih od svakog protivnika. Treća strana može i da bude zadužena za arbitražu ako dođe do osporavanja među principalima u pogledu autentičnosti prenosa poruke.

U ovom opštem modelu vide se četiri osnovna zadatka za projektovanje određenog bezbednosnog servisa:

1. Projektovanje algoritma za vršenje bezbednosne transformacije. Algoritam treba da bude takav da protivnik ne može da ga porazi.
2. Generisanje tajne informacije koju će koristiti algoritam.
3. Razvijanje metoda za distribuciju i deljenje tajne informacije.
4. Određivanje protokola koji će dva principala koji koriste bezbednosni algoritam i tajnu informaciju koristiti za postizanje određenog bezbednosnog servisa.

Prvi i drugi deo ove knjige usredsređeni su na vrste bezbednosnih mehanizama i servisa koji se uklapaju u model sa slike 1.2. Međutim, postoje i druge zanimljive situacije vezane za bezbednost koje se ne uklapaju u taj model ali se razmatraju u ovoj knjizi. Uopšteni model tih drugih situacija ilustrovan je na slici 1.3, gde se reflektuje

[7] U poglavlju 3 opisan je jedan vid šifrovanja, poznat kao asimetrično šifrovanje, u kojem samo jedan od dva principala mora da poseduje tajnu informaciju.

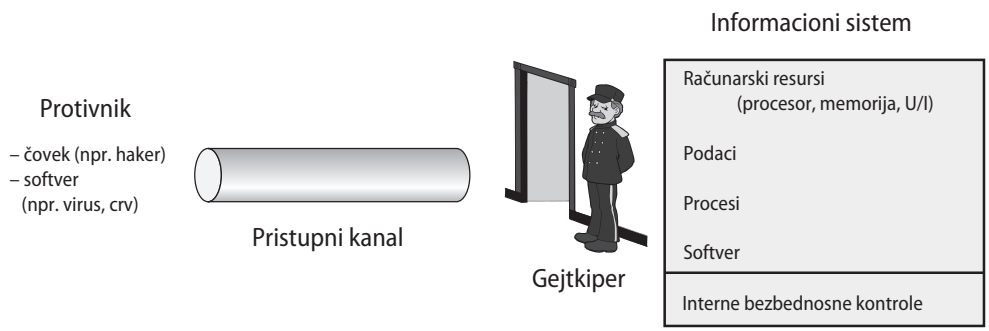
briga za zaštitu informacionog sistema od neželjenog pristupanja. Većina čitalaca upoznata je sa brigama koje izaziva postojanje hakera koji pokušavaju da prodru u sisteme dostupne preko mreže. Haker može da bude neko ko, bez ikakve zle namere, jednostavno uživa da provaljuje u računarske sisteme. Uljez može da bude nezadovoljan zaposleni koji želi da nanese štetu, ili kriminalac koji hoće da iskoristi računarske resurse radi finansijske dobiti (npr., pribavi brojeve kreditnih kartica ili da vrši nezakonite transfere novca).

Još jedna vrsta neželjenog pristupa je kada se u računarski sistem postavi logika 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 dve vrste pretnji:

1. **Pretnje pristupanja informacijama:** Presretanje ili menjanje podataka za račun korisnika koji ne bi trebalo da imaju pristup tim podacima.
2. **Pretnje usluga:** Iskorišćavanje slabe tačke servisa u računaru da bi se legitimni korisnici ometali u korišćenju.

Virusi i crvi su dva primera softverskih napada. Takvi napadi mogu da se unesu u sistem putem diska koji sadrži neželjenu logiku sakrivenu u softveru koji je inače koristan. Takođe mogu da se ubace u sistem preko mreže; ovaj drugi mehanizam je zanimljiviji za mrežnu bezbednost.

**Bezbednosni mehanizmi** potrebni da bi se izašlo na kraj sa neželjenim pristupanjem spadaju u jednu od dve šire kategorije (slika 1.3). Prva kategorija bi mogla da se nazove vratarska funkcija ili funkcija gejtkipera. Ona uključuje procedure prijavljivanja oslonjene na lozinke koje su projektovane da odbiju pristup svima osim ovlašćenim korisnicima i logiku filtriranja projektovanu za otkrivanje i odbijanje crva, virusa i drugih sličnih napada. Ako neželjeni korisnik ili neželjeni softver uspe da pristupi, druga linija odbrane se sastoji od raznovrsnih unutrašnjih kontrola koje nadgledaju aktivnost i analiziraju uskladištene informacije pokušavajući da otkriju prisustvo neželjenih uljeza. Ta pitanja se istražuju u trećem delu.




**Slika 1.3** Model bezbednosti mrežnog pristupa

## 1.7 STANDARDI

Mnoge bezbednosne tehnike i aplikacije opisane u ovoj knjizi navedene su kao standardi. Osim toga, razvijeni su i standardi za upravljačku praksu i sveukupnu arhitekturu bezbednosnih mehanizama i servisa. U celoj ovoj knjizi, opisujemo najvažnije standarde koji se koriste ili se razvijaju za različite aspekte kriptografije i mrežne bezbednosti. U razvijanje i promovisanje ovih standarda uključene su različite organizacije. Najvažnije od tih organizacija (u tekućem kontekstu) su sledeće.

- **Nacionalni institut za standarde i tehnologiju (National Institute of Standards and Technology):** NIST je savezna agencija SAD koja se bavi naukom, standardima i tehnologijom merenja vezanih za korišćenje u vladi SAD i za promovisanje inovacija u privatnom sektoru SAD. Uprkos njegovim nacionalnim okvirima, NIST-ovi Savezni standardi za obradu informacija (**FIPS, Federal Information Processing Standards**) i publikacije (**SP, Special Publications**) imaju uticaj u celom svetu.
- **Društvo Interneta (Internet Society):** ISOC je međunarodna profesionalna organizacija čiji su članovi organizacije i pojedinci iz celog sveta. Ona ima rukovodeću ulogu u rešavanju pitanja koja stoje pred budućnošću Interneta i predstavlja organizaciono središte za grupe odgovorne za standarde za infrastrukturu Interneta, uključujući IETF (Internet Engineering Task Force) i komitet za arhitekturu Interneta (IAB, Internet Architecture Board). Te organizacije razvijaju Internet standarde i povezane specifikacije, koje se sve objavljuju kao **RFC dokumenti** (**Requests for Comments**).

  Detaljniji opis ovih organizacija nalazi se u Dodatku C.

## 1.8 KRATAK PREGLED OVE KNJIGE

Ovo poglavlje služi kao uvod u celu knjigu. Ostatak knjige podeljen je na tri dela.

**Prvi deo:** Sadrži koncizan pregled kriptografskih algoritama i protokola na kojima se zasnivaju aplikacije za bezbednost mreže, uključujući šifrovanje, heš funkcije i digitalne potpise.

**Drugi deo:** Ispituje upotrebu kriptografskih algoritama i bezbednosnih protokola radi ostvarivanja bezbednosti na mrežama i na Internetu. Teme uključuju upravljanje ključevima, autentifikaciju korisnika, kontrolu pristupa mreži, bezbednost oblaka, bezbednost transportnog sloja, bezbednost bežičnih mreža, bezbednost e-pošte i IP bezbednost.

**Treći deo:** Bavi se bezbednosnim sredstvima projektovanim za zaštitu računarskih sistema od bezbednosnih pretnji, uključujući uljeze, viruse i crve. Ovaj deo sadrži i razmatranje tehnologije mrežnih barijera.

Pored toga, dva onlajn poglavlja pokrivaju bezbednost upravljanja mrežama i zakonska i etička pitanja.

## 1.9 PREPORUKE ZA ČITANJE

[STAL12] pruža jedan širi uvod u bezbednost računara. [SCHN00] bi vredelo da pročita svako ko se praktično bavi bezbednošću računara ili mreža: opisuju se ograničenja tehnologije (a posebno kriptografije) u pružanju bezbednosti, kao i potreba da se uzmu u obzir hardver, softverska implementacija, mreže i ljudi uključeni u pružanje i napadanje bezbednosti.

Korisno je pročitati neke klasične udžbenike o bezbednosti računara; oni daju istorijsku perspektivu iz koje se procenjuju trenutan rad i razmišljanje. Radovi koje treba pročitati su [WARE79], [BROW72], [SALT75], [SHAN77], i [SUMM84]. Dva novija, kratka rada o bezbednosti računara su [ANDR04] i [LAMP04]. [NIST95] je iscrpna (290 stranica) obrada ove teme. Još jedna dobra obrada je [NRC91]. Takođe je korisna [FRAS97].

**ANDR04** Andrews, M., and Whittaker, J. „Computer Security." *IEEE Security and Privacy*, September/October 2004.

**BROW72** Browne, P. „Computer Security—A Survey." *ACM SIGMIS Database*, Fall 1972.

**FRAS97** Fraser, B. *Site Security Handbook.* RFC 2196, September 1997.

**LAMP04** Lampson, B. „Computer Security in the Real World." *Computer*, June 2004.

**NIST95** National Institute of Standards and Technology. *An Introduction to Computer Security: The NIST Handbook.* Special Publication 800–12. October 1995.

**NRC91** National Research Council. *Computers at Risk: Safe Computing in the Information Age.* Washington, D.C.: National Academy Press, 1991.

**SALT75** Saltzer, J., and Schroeder, M. „The Protection of Information in Computer Systems." *Proceedings of the IEEE*, September 1975.

**SCHN00** Schneier, B. *Secrets and Lies: Digital Security in a Networked World.* New York: Wiley 2000.

**SHAN77** Shanker, K. „The Total Computer Security Problem: An Overview." *Computer*, June 1977.

**STAL12** Stallings, W., and Brown, L. *Computer Security, Second Edition*. Upper Saddle River, NJ: Prentice Hall, 2012.

**SUMM84** Summers, R. „An Overview of Computer Security." *IBM Systems Journal*, Vol. 23, No. 4, 1984.

**WARE79** Ware, W., ed. *Security Controls for Computer Systems.* RAND Report 609–1. October 1979

## 1.10 INTERNET I VEB RESURSI

Na Internetu i Vebu postoji nekoliko resursa za podršku ove knjige i za pomoć u držanju koraka sa razvojem ovog polja.

### Veb sajt za ovu knjigu

Tu je **Companion Website** za ovu knjigu na adresi WilliamStallings.com/NetworkSecurity.

Za studente, ovaj veb sajt sadrži spisak relevantnih linkova, sređenih po poglavljima i list sa greškama otkrivenim u knjizi nakon štampanja. Za instruktore, ovaj veb sajt daje linkove ka stranicama kurseva koje postavljaju profesori koji predaju pomoću ove knjige.

U ovom izdanju, velika količina originalnog materijala na engleskom za pomoć studentima i nastavnicima dostupna je i na pratećem CD-u. Tu su tri dodatna poglavlja, devet dodataka, praktične vežbe i mnoštvo korisnih dokumenata na koja upućuju reference iz teksta.

### Sajt „Computer Science Student Resource Site"

Ja takođe održavam sajt **Computer Science Student Resource Site**, na ComputerScienceStudent.com.

Svrha tog sajta je da ponudi dokumente, informacije, i linkove za studente i profesionalce računarske struke. Linkovi i dokumenti su organizovani u šest kategorija:

- **Matematika (Math):** Obnavljanje osnovne matematike, početnica za analizu redova, početnica za numeričke sisteme, i linkovi ka mnogim matematičkim sajtovima.
- **Uputstva (How-to):** Saveti i uputstva za rešavanje problema za domaće zadatke, za pisanje tehničkih izveštaja, i pripremanje tehničkih prezentacija.
- **Resursi za istraživanja (Research resources):** Linkovi ka važnim zbirkama referata, tehničkih izveštaja i bibliografija.
- **Karijera u računarskoj nauci (Computer science careers):** Korisni linkovi i dokumenti za one koji razmatraju karijeru u računarskoj nauci.
- **Razno (Miscellaneous):** Raznovrsni drugi zanimljivi dokumenti i linkovi.
- **Zabava (Humor and other diversions):** Morate povremeno da skrenete misli sa posla.

### Drugi veb sajtovi

Brojni veb sajtovi sadrže informacije vezane za teme iz ove knjige. Pridruženi veb sajt Companion nudi linkove ka tim sajtovima, sređene po poglavljima. Osim toga, na Internetu postoje i brojni forumi koji se bave kriptografijom. Linkovi ka tim forumima mogu se naći na pridruženom veb sajtu Companion.

## 1.11 KLJUČNI IZRAZI, PITANJA ZA OBNAVLJANJE I PROBLEMI

### Ključni izrazi

| | | |
|---|---|---|
| aktivan napad | integritet | ponavljanje |
| analiza saobraćaja | integritet podataka | poverljivost podataka |
| autentičnost | kontrola pristupa | raspoloživost |
| autentifikacija | maskiranje | šifrovanje |
| bezbednosni mehanizmi | neporicanje | uljez |
| bezbednosni napadi | OSI arhitektura bezbednosti | uskraćivanje usluge |
| bezbednosni servisi | pasivan napad | |

## Pitanja za obnavljanje

**1.1** Šta je to OSI arhitektura bezbednosti?

**1.2** Koja je razlika između pasivnih i aktivnih pretnji bezbednosti?

**1.3** Nabrojte i ukratko definišite kategorije pasivnih i aktivnih bezbednosnih napada.

**1.4** Nabrojte i ukratko definišite kategorije bezbednosnih servisa.

**1.5** Nabrojte i ukratko definišite kategorije bezbednosnih mehanizama.

## Problemi

**1.1** Razmotrite bankomat (ATM, automated teller machine) u koji korisnici upisuju lični identifikacioni broj (PIN, personal identification number) i ubacuju karticu da bi pristupili svom računu. Navedite primere za zahteve poverljivosti, integriteta i raspoloživosti u tom sistemu. U svakom primeru, navedite stepen važnosti tih zahteva.

**1.2** Ponovite problem 1.1 za telefonski komutirani sistem koji usmerava pozive kroz komutiranu mrežu na osnovu telefonskog broja koji traži pozivalac.

**1.3** Razmotrite sistem za stono izdavaštvo koji proizvodi dokumente za različite organizacije.

- **a.** Navedite primer za vrstu publikacije za koju je najvažniji zahtev poverljivost sačuvanih podataka.
- **b.** Navedite primer za vrstu publikacije za koju je najvažniji zahtev integritet podataka.
- **c.** Navedite primer gde je najvažniji zahtev raspoloživost sistema.

**1.4** Za svaku od sledećih vrednosti, odredite stepen uticaja (nizak, srednji, ili visok) za gubitak poverljivosti, raspoloživosti, odnosno integriteta. Obrazložite odgovore.

- **a.** Organizacija koja upravlja javnim informacijama na svom veb serveru.
- **b.** Policijska organizacija koja upravlja krajnje osetljivim informacijama istrage.
- **c.** Finansijska organizacija koja upravlja rutinskim administrativnim informacijama (informacijama koje se ne odnose na privatnost).
- **d.** Informacioni sistem koji se koristi za velike nabavke u organizaciji za ugovaranje koji sadrži kako osetljive informacije iz faze pre zaključivanja ugovora, tako i rutinske administrativne informacije. Procenite uticaj za ta dva skupa podataka zasebno i za informacioni sistem kao celinu.
- **e.** Elektrana sadrži SCADA (supervisory control and data acquisition) sistem nadzora i prikupljanja informacija koji kontroliše distribuciju električne energije za jedno veliko vojno postrojenje. SCADA sistem sadrži i senzorske podatke u realnom vremenu i rutinske administrativne informacije. Procenite uticaj za ta dva skupa podataka zasebno i za informacioni sistem kao celinu.

**1.5** Napravite matricu sličnu tabeli 1.4 koja prikazuje odnos bezbednosnih servisa i napada.

**1.6** Napravite matricu sličnu tabeli 1.4 koja prikazuje odnos bezbednosnih mehanizama i napada.

**1.7** Pročitajte sve klasične radove navedene u odeljku 1.9. Sastavite izveštaj od 500-1000 reči (ili PowerPoint prezentaciju od 8 do 12 slajdova) sa rezimeom ključnih pojmova koji proističu iz tih radova, naglašavajući pojmove zajedničke za većinu radova ili za sve njih.