Sažetak 10. poglavlja iz Komunikacijske mreže drugi dio v.2.0 (2013/14)

Sigurnost u informacijskom i komunikacijskom svijetu se može definirati kao sposobnost mreža, usluga i aplikacija da se suprotstave neočekivanim slučajnim događajima i zlonamjernim aktivnostima.

Sigurnosne domene u mrežnom okružju:

- domena korisnika usluga
- domena prijenosa informacija (posebno izloženo prijetnjama)
- domena davatelja usluga

Sigurnosne prijetnje:

- **Presretanje** (*interception*) ili **prisluškivanje** (*evesdropping*): elektronička komunikacija se presreće i preuzima informacija koju razmjenjuju sudionici. Postoji i direktno prisluškivanje na vodu (*wiretapping*) gdje je lakše prisluškivati ako se radi o analognom obliku nego o digitalnom. Prisluškivanje je regulirano zakonski zbog moguće povrede privatnosti.
- **Prekidanje** (*interruption*): u potpunosti onemogućuje komunikaciju, uslugu ili aplikaciju.
    - **Prekid komunikacije**: sudionik A ne može pristupiti B.
    - **Prekid obrade**: sudionik B ne može poslužiti A (tako piše u skripti, možda je krivo).
    - **Uskraćivanje usluge**: napadač izaziva preopterećenje mreže ili šalje stalno zahtjeve.
- **Uplitanje uljeza u komunikaciju** (*tampering*): sudionik A pošalje informaciju, uljez C je promjeni i pošalje sudioniku B ili stvara veliko kašnjenje bez promjene informacije.
- **Ubacivanje zlonamjerne informacije** (*fabrication*)
- **Lažno predstavljanje** ili **maskiranje** (*masquerade*) ili **utjelovljenje** (*impersonation*): uljez C se predstavlja kao sudionik A i šalje informacije sudioniku B (, a on povjeruje da je to A) ili preuzme informacije od A i predstavlja se kao sudionik A.

Sigurnosni zahtjevi:

Ostvaruju se kriptografskim postupcima:

- **Autentičnost** (*authenticity*): potvrda identiteta korisnika. Za to je potrebno provesti autentifikaciju.
- **Cjelovitost**, **integritet** (*integrity*): jamstvo da su podaci i informacije poslane, primljene i pohranjene u izvornom obliku tj. nitko ih nije mijenjao u komunikaciji.
- **Povjerljivost** (*confidentiality*) ili **tajnost** (*secrecy*): podaci se šalju u obliku koji je razumljiv samo pošiljatelju i namjeravanom primatelju.
- **Neporecivost** (*non-repudiation*): zahtijeva se osiguranje mehanizama kojima će se sudionicima onemogućiti poricanje aktivnosti u kojoj su sudjelovali (npr. sudionik A pošalje poruku i naknadno želi to spriječiti).

Ostvaruju se organizacijskim mjerama, izvedbom sustava:

- **Kontrola pristupa** (*access control*): samo autentificiranim sudionicima je dopušten pristup podacima i uslugama (sukladno ulozi sudionika i njegovim pravima pristupa).
- **Raspoloživost** (*availability*): podaci i informacije moraju biti dostupni i u slučaju neočekivanih događaja (npr. nestanak struje). Mreža, usluge i aplikacije moraju biti u operativnom stanju. Raspoloživost se može mjeriti: npr. dopušten je ispad sustava u sve skupa sat vremena godišnje. Zahtijevana raspoloživost u tom slučaju je 1 – 1/(24*365) = 0.9998859.
- **Radna sigurnost** (*operational security*): opisuje mjere kojima se suprotstavlja napadima na mrežu i računala. Analizira se ranjivost i rizik sustava i pokušava se spriječiti ugrožavanje sustava.

Pregled kriptografskih postupaka

- **Tajna**: temelj svake sigurnosti. Koristi se za autentifikaciju, očuvanje cjelovitosti, dokaz neporecivosti, povjerljivost.
- **Kriptologija** (*cryptology*): znanost koja se bavi tajnom tj. postupcima (de)kriptiranja.
  - **Kriptografija** (*cryptography*): stvaranje šifri i pretvorba podataka u uljezu nečitljiv oblik.
  - **Kriptoanaliza** (*cryptoanalysis*): obrnuto od kriptografije.
- Jednostavan primjer kriptiranja: Cezarova šifra (zamijeni slovo na mjestu slova sa slovom koje na mjestu abecede koja je pomaknuta za neki broj).
- **Rezultat šifriranja** je **šifrirani tekst** (*cyphertext*) ili **kriptogram** (*cryptogram*) $\boldsymbol{C}$:
  - $\boldsymbol{E_{K_E}(P) = C}$

    $\boldsymbol{E_{K_E}}$ – postupak kriptiranja $\boldsymbol{K_E}$ – ključ kriptiranja **P** – poruka (otvoreni tekst)
- **Dekriptira se postupkom**
  - $\boldsymbol{D_{K_D}(C) = D_{K_D}\left(E_{K_E}(P)\right) = P}$

    $\boldsymbol{D_{K_D}}$ – postupak dekriptiranja $\boldsymbol{K_D}$ – ključ dekriptiranja
- Algoritmi (de)kriptiranja su javno objavljeni kako bi se provjerila njihova probojnost. Ključevi su tajni.
- **Simetrična kriptografija:** $\boldsymbol{K = K_E = K_D}$
  - Tradicionalna kriptografija. Duljina ključa određuje snagu zaštite. Tipično za kriptiranje pojedine sjednice ili razmjene podataka između procesa ograničene duljine i trajanja.
  - Pretpostavka simetrične kriptografije je da sudionici raspolažu tajnim ključem prije razmjene šifriranih poruka. Uspostava ključa se radi se preko 'nesigurne mreže' i koriste se postupci koji omogućavaju da dva sudionika uspostave ključ bez uporabe kriptografije (*Diffie-Hellman key exchange*, tako piše u skripti, bez objašnjenja).
    Napomena: uz algoritme bi vam bilo pametno pogledati slike 10.9 i 10.10.

- **Algoritmi:**
  - **Standard DES** (*Data Encryption Standard*): za 64-bit blokove, temeljeno na višestrukim abecednim zamjenama (16 puta), ključ duljine 56 bita. Problem: prekratki ključ. A → Kriptiranje →B (dekr):
$$\boldsymbol{P} \;\rightarrow\; \boldsymbol{E_K(P)} \;\rightarrow\; \boldsymbol{D_K\big(E_K(P)\big) = P}$$
  - **Utrostručeni DES**: kaskada s tri transformacije, svaka sa svojim ili dvije od njih s istim tajnim ključem duljine 56 bita. Na kraju duljina ključa: 3*56 = 168 ili 2*56 = 112 bita. A → Kriptiranje → B (dekr):
$$\boldsymbol{P \;\rightarrow\; E_{K1}\Big(D_{K2}\big(E_{K1}(P)\big)\Big) = C \;\rightarrow\; D_{K1}\Big(E_{K2}\big(D_{K1}(C)\big)\Big) = P}$$
  - **Standard AES** (*Advanced Encryption Standard*): zamjena za DES, 128-bit blok, ključevi duljine 128, 192 i 256 bita, programska i sklopovska izvedba, uporaba algoritma javna i licencirana.

- **Asimetrična kriptografija:** $\boldsymbol{K_E \neq K_D}$
  - **Jedan** od ključeva je **tajan** – privatni, a **drugi** može biti **javan** ključ. Svaki sudionik sadrži oba ključa koji se kombiniraju pomoću **kriptografije javnog ključa** (*public key cryptography*).
  - **Načelo rada kriptografije javnog ključa:**
    - Sudionik A ima privatni ključ $\boldsymbol{D_A}$ i javni ključ $\boldsymbol{E_A}$, a sudionik B privatni ključ $\boldsymbol{D_B}$ i javni ključ $\boldsymbol{E_B}$. Prije početka komunikacije sudionici **razmjenjuju javne ključeve** koji se koriste za **kriptiranje**, a **privatni ključevi** za **dekriptiranje**. A → Kriptiranje → B (dekr):
$$\boldsymbol{P \;\rightarrow\; E_B(P) \;\rightarrow\; D_B\big(E_B(P)\big) = P}$$
  - **Algoritmi** koji to ostvaruju (općenito su **100-1000 puta sporiji** od simetričnih):
    - **RSA** (nazvan po autorima): zasniva se na teoriji brojeva, nalaženju prim-brojeva. Nedostatak: potrebni dugi ključevi (>= 1024 bita) = sporo izračunavanje.
    - **Algoritam ruksaka**: ne smatra se više sigurnim.
    - **Izračunavanje diskretnih logaritama**
    - **Eliptičke krivulje**
- **Digitalni potpis:**
  - Osim osiguranja povjerljivosti navedenim kriptografijama potrebno je osigurati autentičnost i neporecivost. Rješenje: digitalni potpis.
  - **Potpis sa simetričnim ključem:**
    - Postoji **središnji autoritet T** koji zna sve tajne ključeve i kojem svi vjeruju. Pošiljatelj **A** šalje T svojim tajnim ključem $\boldsymbol{K_A}$ kriptiranu poruku **P** za primatelja **B** kojoj dodaje vremensku oznaku $\boldsymbol{t}$ i slučajni broj poruke $\boldsymbol{R_A}$. Kriptirana poruka: $\boldsymbol{K_A(B, R_A, t, P)}$.
    - Središnji autoritet T ustanovljuje identitet od A, dekriptira poruku njegovim ključem $\boldsymbol{K_A}$ i zaključuje da treba poslati poruku P s t primatelju B. Dodaje u poruku informaciju o pošiljatelju A te sve kriptira. Potpisuje svojim tajnim ključem $\boldsymbol{K_T}$. Primatelju B prosljeđuje proširenu kriptiranu poruku: $\boldsymbol{K_B(A, R_A, t, P, K_T(A, t, P))}$.
      $\boldsymbol{K_T(A, t, P)}$ – potpis od T.

        - Primatelj dekriptira svojim ključem $\boldsymbol{K_B}$ i siguran je u identitet od A zbog potpisa od T. Time je osigurana i neporecivost. Prijetnja napada ponavljanja se izbjegava vremenskom oznakom t (starost) i slučajnim brojem $\boldsymbol{R_A}$ (već iskorištena poruka).
    - **Potpis javnim ključem:**
        - Izbjegava se središnji autoritet.
        - A kriptira tj. potpisuje poruku svojim privatnim ključem $\boldsymbol{D_A}$ i zatim je kriptira javnim ključem od B: $\boldsymbol{E_B(D_A(P)) = C}$
        - B dekriptira primljenu poruku prvo javnim ključem pošiljatelja $\boldsymbol{E_A}$, a zatim vlastitim privatnim ključem: $\boldsymbol{E_A(D_B(C)) = P}$
        - Algoritam koji to ostvaruje: RSA.
        - Neporecivost je osigurana (samo je A moga potpisati privatnim ključem $\boldsymbol{D_A}$).
    - **Potpis sažetkom poruke (*message digest*, MD):**
        - Ne osigurava tajnost. Tu se stavlja naglasak na integritet, autentičnost i neporecivost. **Brže od kriptiranja**.
        - **Sažetak** poruke je jednosmjerna **hash** funkcija, **MD**:
            - Lako za izračunati.
            - Gotovo nemoguće izračunati P iz MD(P).
            - Nemoguće je odrediti P' čiji je MD(P') = MD(P) (>128 bita).
            - Promjena samo 1 bita daje različit rezultat.
        - **Razlika prema rješenju digitalnog potpisa simetričnim ključem:**
            - T prima poruku od A kriptiranu ključem $\boldsymbol{K_A}$. Dekriptira je i potpisuje s MD(P) te prema B prosljeđuje: $\boldsymbol{K_B(A, R_A, t, P, K_T(A, t, MD(P)))}$
            - Izračun i kriptiranje sažetka traju kraće od kriptiranja cijele poruke i ujedno se smanjuje količina podataka (MD(P) < P).
        - **Razlika prema rješenju digitalnog potpisa javnim ključem:**
            - Kriptiranje poruke se zamjenjuje izračunom i kriptiranjem sažetka. Prenose se poruka i sažetak: $\boldsymbol{P, D_A(MD(P))}$
        - **Algoritmi:**
            - **SHA-1** (*Secure Hash Algorithm*) – vjerojatno najsigurniji (sažetak duljine 160 bita).
            - **MD5** (*Message Digest Algorithm*) – uočeni sigurnosni problemi (128 bita).
            - **DSA** (*Digital Signature Algorithm*) – unutar standarda **DSS** (*Digital Signature Standard*), koristi SHA-1 (duliine 80 bita).

- **Infrastruktura javnog ključa (*Public Key Infrastructure*, PKI):**
    - Kriptografija javnog ključa postavlja dodatan zahtjev: upravljanje javnim ključevima i uspostavljanje **povjerenja** između različitih mreža i organizacija u svrhu sigurnog komuniciranja.
    - Uvodi se rješenje za dokazivanje identiteta korisnika **digitalnim certifikatom** (***digital certificate***) koji je digitalno potpisana izjava kojom se potvrđuje da je korisniku dodijeljen njegov javni ključ.
    - U sastavu infrastrukture djeluju:
        - **Registracijsko tijelo** (*Registration Authority*, RA): provjerava identitet korisnika, ustanovljava sadržaj certifikata te registrira korisnika.
        - **Certifikacijsko tijelo** (*Certification Authority*, CA): izdaje i povlači certifikate, održava i objavljuje informacije o stanju certifikata, omogućuje provjeru certifikata. Svako certifikacijsko tijelo ima svoj certifikat i povezano je s drugim certifikacijskim tijelima. Više certifikacijskih tijela može imati zajedničko registracijsko tijelo. Mogu imati nadležna certifikacijska tijela.
    - Primjer (Slika 10.16): korisnik i se prijavi registracijskom tijelu RA_a koje ima uspostavljeno certifikacijsko tijelo CA_x. RA_a u ime CA_x provjerava identitet od korisnika i podatke certifikata. U certifikat se zapisuje korisnikov javni ključ, a certifikat ovjerava digitalnim potpisom organizacije koja ga je izdala. Privatni ključ korisnik dobiva na povjerljiv i zaštićen način u registracijskom tijelu (ne putem mreže). Neki drugi korisnik može preko zajedničkog CA provjeriti identitet korisnika i, uključujući njegov privatni ključ.
    - **Certifikacijska tijela** trebaju uspostaviti **međusobno povjerenje** i biti povezana kako bi korisnici mogli međusobno provjeravati identitete.
- **Sigurnosna arhitektura Interneta:**
    - Slijedi slojevitu strukturu:
        - **U mrežnom sloju**: sigurnost se postiže protokolom **IPsec** koji proširuje IPv4 sigurnosnim uslugama. Postiže se sigurna razmjena svih datagrama, neovisno o transportnom protokolu, usluzi ili aplikaciji.
        - **U transportnom sloju:** iznad transportnog, a ispod aplikacijsko sloja dodatni sloj **sigurne priključnice** (*Secure Sockets Layer*, **SSL**). SSL se primjenjuje s protokolom **TCP**.
        - **U aplikacijskom sloju:** sigurni pristup webu (HTTP + SSL = **HTTPS**), siguran rad e-pošte (*Pretty Good Privacy*, PGP, i *Secure Multipurpose Internet Mail*, S/MIME), za elektroničke sjednice (*Secure Electronic Transaction*, SET).
    - **Sigurni IP (IPsec):**
        - Obuhvaća protokole koji se primjenjuju za pružanje sigurnosnih usluga mrežnog sloja u Internetu:
            - **Zaglavlje autentičnosti** (*Authentification Header*, **AH**): integritet datagrama i autentičnost izvora se osiguravaju se kodom vjerodostojnost (*Hashed Message Authenitification Code*, HMAC) koji se uključuje u AH, neponavljanje.

        - **Sigurno ovijeni podaci** (*Encapsulating Security Payload*, **ESP)**: osiguranje tajnosti datagrama, autentičnosti, integriteta neponavljanja.
        - **Sigurno udruživanje sudionika** (*Security Association*, SA)
        - **Razmjena ključa u Internetu** (Internet Key Exchange, IKE)
    - Zasniva se na **simetričnoj** kriptografiji (tajnom ključu) zbog **boljih performansi**.
    - Postupak:
        - Definiraju se krajnje točke sigurne komunikacije. Točke mogu biti računala ili mrežni uređaji s funkcijom sigurnog prilaza (*Security Gateway*, SG).
        - Odabire se **transportni** (*transport mode*) ili **tunelski** način rada (*tunnel mode*). Pogledati 61. i 62. str. kako funkcioniraju.
        - Uspostavlja se sigurnosno udruživanje – asocijacija tijekom kojeg se dogovaraju usluge omogućene s AH ili ESP i dostavlja dijeljena tajna pomoću koje sudionici stvaraju tajni ključ.
        - Datagrami se prenose sigurno s AH ili ESP.
- **Sloj sigurne priključnice (SSL):**
    - Dvoslojni protokol. Rješava sigurnosne mehanizme u transportnom sloju. U transportnom sloju nalazi se **SSL-protokol zapisa** (*SSL Record Protocol*) koji fragmentira poruku višeg sloja, uz mogućnost kompresije, dodaje **kod vjerodostojnosti** (*Message Authentification Code*, MAC) i sve zajedno kriptira simetričnim algoritmom. To se prenosi **TCP**-om.
    - **Upravljački podsloj** sadrži **tri** protokola:
        - **SSL-protokol rukovanja** (*SSL Handshake Protocol*) kojim se uspostavlja SSL-sjednica i dogovaraju parametri sigurne veze. Sudionici se međusobno autentificiraju, dogovaraju kripto-algoritam i stvaraju tajni ključ.
        - **SSL-protokol promjene kripto-algoritma** (*SSL Change Cipher Spec Protocol*): šalje se samo **jedna poruka** kojom se dojavljuje započinjanje promjene dogovorenog algoritma i tajnog ključa.
        - **SSL-protokol uzbunjivanja** (*SSL Alert Protocol*) kojim se šalje **poruka upozorenja** o narušenoj sigurnosti što može biti indikacija za prekid SSL-sjednice.
    - Pogledati 64. i 65. stranicu za primjer.