Infrastruktura

- **Ciljevi napada na DNS**
  - Denial of Service – slanje negativnih odgovora, preusmjeravanje na poslužitelj koji ne sadrži traženu uslugu
  - Masquerading – preusmjeravanje komunikacije i predstavljanje kao pravi poslužitelj
  - Domain Hijacking - kompromitiranjem nesigurnih mehanizama osvježavanja preuzima se domena
- **Napadi na DNS – točke ranjivosti**
  1. Pokvareni podaci
  2. Neautorizirana osvježenja
  3. Promijenjeni podaci o zoni (glumljenje mastera)
  4. Zagađenje cachea
  5. Glumljenje cachea
- **Tipovi napada na DNS**
  - Cache poisoning
  - Kompromitiranje poslužitelja
  - Spoofing
- **Early attack (cache poisoning)**
  - Korisnik želi učitati stranicu napadača, šalje upit do DNS servera, napadačev name server vrati odgovor, ali i lažnu IP adresu za neku drugu stranicu (paypal.com)
  - Ciljani name server spremi lažnu IP adresu u cache i ljudi koji mu pristupaju dobiju krivu adresu za paypal.com
- **Kaminsky DNS attack (lažiranje DNS zapisa)**
  - Napadač šalje upit za nepostojeći aaa.paypal.com i istovremeno šalje odgovore s lažnim IP-om, ponavlja to dok ciljani server ne prihvati odgovor i spremi ga u cache, ljudi koji pristupaju tom serveru dobiju krivu IP adresu za paypal.com
- **Tuneliranje kroz DNS**
  - DNS se koristi kao skriveni komunikacijski kanal kako bi se zaobišao vatrozid
- **Napad NXDOMAIN**
  - Napadač preplavljuje poslužitelj upitima za nepostojeće domene, rekurzivni poslužitelj pokušava dohvatiti podatke te mu se cache popunjava rezultatima NXDOMAIN, usporava se vrijeme odziva
- **Zaštita**
  - TSIG (transaction signature) – provjerava identitet pomoću ključa
  - DNSSEC – DNS Security Extensions
    - Provjerava identitet
    - Osigurava kriptografski dokaz ispravnosti primljenih podataka
    - Temelji se na korištenju asimetrične kriptografije, javnih i privatnih ključeva
      - DNS podaci se potpisuju privatnim ključem, javni ključ se objavljuje i koristi se za provjeru potpisa
    - Osigurava autentičnost i integritet
    - Problemi
      - Ne osigurava povjerljivost
      - Ne štiti od DDoS napada
      - Vrijeme života digitalnog potpisa
- **Napadi na usmjeravanje**
  - Utjecaj
    - Podoptimalno usmjeravanje

        - Zagušenje
        - Particioniranje mreže – odvajanje mreža, nemogućnost komuniciranja s računalima u drugim participama
        - Preplavljivanje poslužitelja – oružje za DoS napade
        - Kreiranje petlji
        - Pristup podacima – presretanje prometa
    - Tipovi napada
        - Napadi na link
            - Presretanje
            - Ometanje, modificiranje poruka
            - Ponavljanje starih poruka
        - Napadi na usmjeritelj
            - Usmjeritelj šalje lažne poruke ili ih ne šalje
        - Napadi na BGP
            - Modifikacija, umetanje, brisanje ponavljanje, krivotvorenje

VPN

- Intranet – korisnici unutar kompanije, extranet – korisnici izvan kompanije (dobavljači, proizvođači, partneri)
- **Zahtjevi za udaljen pristup intranetu**
    - Privatnost – integritet podataka
    - Umrežavanje – mogućnost rada iza vatrozida
    - Upravljivost – korištenje različitih načina autentifikacije i direktorija za pohranjivanje informacija o korisnicima
    - Kontrola pristupa – mogućnost administriranja nivoa pristupa, korisnik ne smije imati pristup svim resursima mreže
- **Sigurni udaljeni pristup intranetu**
    - **VPN**
        - Radi na mrežnom sloju, nezavisan o aplikaciji
        - Enkapsulira originalne IP pakete unutar svog vlastitog paketa
        - Komunikacijske veze ostvarene preko jeftinije dijeljene infrastrukture (Interneta)
        - Ista sigurnosna politika i performanse kao i privatne mreže realizirane preko infrastrukture WAN
        - Secure VPN – autentifikacija korisnika, tajnost i integritet podataka
    - **Clientless VPN**
        - Temelji se na korištenju HTTPS, ali može uključivati aplikacije koje koriste SSL/TLS
        - Clientless - računalo ima Web preglednik koji podržava HTTP i HTTPS
- **Prijetnje u VPN-ovima**
    - Neovlašteni pristup prometu
    - Izmjena sadržaja prometa
    - Napadi uskraćivanjem usluge (DoS)
    - Izmjene konfiguracije VPN-a
    - Napadi na protokole VPN-a
- **Obrana u VPN-ovima (na razini korisnika i na razini davatelja usluge)**
    - Šifriranje paketa i kontrolnog prometa
    - Filtri

    - Vatrozid
    - Kontrola pristupa
    - Izolacija
- **Vrste VPN-a**
    - Site-to-site – između dva mrežna entiteta (usmjeritelja), zaštićene mreže iza oba entiteta
    - Remote Access – između uređaja i usmjeritelja, uređaj nema zaštićenu mrežu
- **Tuneliranje u VPN-ovima**
    - Privatni IP paketi omataju se u javne IP pakete
    - Tehnologije tuneliranja – L2TP, PPTP, IPSec
- **IPSec**
    - Rješenje na mrežnom sloju, osigurava sigurnosne usluge sloju IP i višim slojevima
    - Omogućava šifriranje i autentifikaciju
    - Sigurnosni protokoli
        - Authentication Header (AH)
            - Osigurava autentičnost izvora podataka i integritet niza IP datagrama
        - Encapsulating Security Payload (ESP)
            - Osigurava povjerljivost
    - Načini rada
        - Transportni način
            - Redoslijed zaglavlja - IP-IPSec-TCP-podaci
            - Krajnje točke - računala
        - Tunelirani način
            - Redoslijed zaglavlja - NovoIP-IPSec-IzvornoIP-TCP-podaci
            - Krajnje točke – računalo-usmjeritelj ili usmjeritelj-usmjeritelj
    - Sigurnosne usluge IPSec arhitekture
        - Kontrola pristupa
        - Cjelovitost na razini datagrama
        - Vjerodostojnost izvora datagrama
        - Zaštita protiv napada ponovnim slanjem snimljenog prometa
        - Povjerljivost
        - Ograničena povjerljivost prometnog toka – ne vide se izvorišni i odredišni portovi
- **Sigurnosna asocijacija (AS)**
    - Jednosmjerna veza koja prometu koji se odvija preko nje pruža odabranu sigurnosnu uslugu
    - Svaka strana zasebno stvara SA, posebno za AH i ESP (ne oba u istoj SA)
    - Osigurava vjerodostojnost end-to-end ili end-to intermediate
    - Upravljanje ključevima – ručno ili administrirano
- **IPSec SA**
    - Vrste
        - Uni-directional (IPSec SA)
        - Bi-directional (Internet Key Exchange (IKE) SA)
- **Prednosti IPSec**
    - Osigurava se sav promet viših slojeva
    - Korisnici i aplikacije ne moraju brinuti o sigurnosti
    - Stvaraju se tuneli kroz nesigurne mreže
    - Osim samog sadržaja, skriva se i vrsta prometa
    - IPSec je standardni dio IPv6 specifikacije

- **Nedostaci IPSec**
  - Ne autentificira se korisnik, već računalo
  - Nema sigurnosti ako sistem nije siguran ili već kompromitiran

SSL-TLS

- **SSL/TLS – Secure Sockets Layer/Transport Layer Security (SSL v3.0 i TLS 1.2)**
  - Sigurnosni protokol
  - Cilj – uspostavljanje sigurnog i šifriranog komunikacijskog kanala
  - Alternativa standardnom TCP/IP socket sučelju s ugrađenom podrškom za sigurnost
  - Osigurava autentifikaciju poslužitelja (i klijenta), privatnost podataka i cjelovitost podataka (MAC – Message Authentication Code)
  - 2 sloja
    - Protokol „record“ – definira format podataka, šifrira aplikacijske podatke, sadrži MAC
    - Protokol „handshake“ – početna autentifikacija i prijenos ključeva, uspostavljanje šifrirane SSL konekcije
- **SSL/TLS sjednica**
  - korisnik na klijentskoj strani (u pregledniku) zahtijeva dokument s URL koji sadrži https umjesto http
  - preglednik prepoznaje SSL/TLS zahtjev i uspostavlja konekciju s poslužiteljem na TCP portu 443
  - klijent inicira „handshake” korištenjem protokola „record”
- **Ranjivosti i napadi na SSL/TLS**
  - Heartbleed
    - Neispravno rukovanje porukom „keep-alive“
    - Slanjem par HTTP zahtjeva napadač može jednostavno dohvatiti osjetljive podatke iz memorije poslužitelja
  - BEAST
    - Temelji se na predvidljivosti inicijalizacijskog vektora u CBC načinu rada TLS 1.0
    - Uspješno izvođenje otkriva žrtvine HTTP kolačiće i otima sesiju
  - POODLE TLS
    - Iskorištava lošu implementaciju CBC šifriranja u protokolu TLS te napadač može otkriti dijelove podataka (na primjer kolačiće)

Sigurnost Web aplikacija

- **Dvije strane**
  - preglednik (na klijentu)
    - napadi koji iskorištavaju ranjivosti preglednika
    - posljedice
      - instalacija malwarea (keyloggeri, botneti)
      - krađa dokumenata u korporativnim mrežama
      - gubitak privatnih podataka
  - aplikacija (na poslužitelju)
    - pokrenuta na sjedištu: banke, e-trgovina, blogovi
    - jezici: PHP, ASP, JSP, Ruby, Perl...
    - potencijalne rupe: XSS, XSRF, SQL injection
    - posljedice

        - ukradeni brojevi kreditnih kartica
        - defacement web sjedišta
        - krađa podataka
- **Ranjivosti Web aplikacija**
    - **Umetanje (injection)**
        - Aplikacije uzimaju ulazne podatke i interpretiraju ih kao naredbe ili upite
        - Često je ubacivanje SQL naredbi
        - Moguća kompromitacija ili promjena baze podataka
        - Izbjegavanje – izbjeći interpretiranje naredaba, provjeriti što korisnik upiše prije nego se izvede, minimizirati ovlasti nad bazom podataka
    - **Autentifikacija i upravljanje sjednicama**
        - HTTP je stateless, stanje sjednice se prati putem varijable SESSION ID koja se vidi na mreži, u pregledniku, logovima
        - Putem SESSION ID-a se rade kritične stvari – upravljanje lozinkama, login, pošta…
        - Moguća kompromitacija korisničkog računa ili otmica sjednice
        - Izbjegavanje – SSL treba štititi podatke za prijavu i SessionID tijekom cijele sjednice, novi SessionID kod svakog zahtjeva, tokeni
    - **Cross-Site Scripting (XSS)**
        - Podaci od napadača šalju se korisniku u preglednik
        - Podaci mogu biti pohranjeni u bazi, rezultat unosa u obrazac ili poslani izravno JavaScript klijentu
        - Posljedice –krađa korisničkih sjednica, osjetljivih podataka, pisanje po stranici, preusmjeravanje korisnika na phishing ili malware sjedište
        - Izbjegavanje – unos treba „dezinficirati“, izbjeći posebne znakove, napraviti whitelisting onoga što korisnik može unijeti
        - Same origin policy
            - Skripte koje se izvode na jednoj stranici smiju međusobno dijeliti pristup podacima, ali ne smiju sa skriptama koje su na drugim stranicama
            - Najčešći primjer – kolačići (cookies)
                - Preglednik ne šalje pohranjene kolačiće onoj stranici koja na njih nema pravo jer oni sadrže identifikatore sjednica
    - **Nesigurne reference na objekte**
        - Npr. Get parametri u URL-u kojima se određuje broj korisnika ?acct=6054
        - Posljedice – korisnici imaju pristup podacima za koje nisu autorizirani
        - Izbjegavanje – eliminacija referenci, provjera prava pristupa
    - **Loše sigurnosne postavke**
        - Web aplikacije očekuju da je sustav na kojem se nalaze siguran
        - Posljedice – instalacija backdoor aplikacija, neautorizirani pristup
        - Izbjegavanje – provjeriti platformu, patchirati komponente, verificirati konfiguraciju
    - **Nesigurna pohrana šifriranih podataka**
        - Problem ako se ne identificiraju svi osjetljivi podaci i mjesta na kojima se nalaze
        - Posljedice – napadači mijenjaju osjetljive podatke, pronalaze tajne i koriste ih u napadima, sramoćenje tvrtke, nezadovoljstvo korisnika, sudske tužbe
        - Izbjegavanje – verificirati osjetljive podatke i identificirati mjesta na kojima se oni pohranjuju, zaštita podataka šifriranjem, stvaranje, distribucija i zaštita ključeva
    - **Nezaštićeni pristup URL-ovima**

    - Napadač krivotvori pristup stranicama kojima nema pristup (/user/getAccounts promijeni u /admin/getAccounts)
    - Posljedice – napadač pristupa podacima i korisničkim računima drugih korisnika, pokreće funkcionalnosti na koje nema pravo
    - Izbjegavanje – za svaki URL treba provjeriti pravo pristupa, verificirati arhitekturu i implementaciju
- **Lažiranje zahtjeva na drugom sjedištu (Cross Site Request Forgery (CSRF))**
    - Preglednik žrtve se namami da pošalje naredbu ranjivoj web-aplikaciji
    - Ranjivost je uzrokovana činjenicom da preglednici automatski uključuju autentifikacijske podatke (sjednica, IP adresa) u svaki zahtjev (cookie)
    - Iskorištava se činjenice da sjedište vjeruje pregledniku korisnika
    - Posljedice – iniciranje transakcija, pristup osjetljivim podacima, promjena podataka o korisničkom računu
    - Izbjegavanje – dodati neku tajnu (token), ne prihvaćati sve osjetljive podatke automatski, koristiti POST umjesto GET-a, sanitizirati unos korisnika pri spremanju u bazu
- **Ranjive komponente**
    - Veliki sustavi koriste komponentni razvoj, problem ako su komponente ranjive
    - Izbjegavanje – provjeriti korištene komponente, pratiti sigurnosne zakrpe i otkrivene ranjivosti
- **Preusmjeravanje i prosljeđivanje**
    - Redirekcije su česte, ako valjanost nije provjerena, napadač može poslati žrtvu na sjedište po izboru
    - Posljedice – preusmjeravanje na phishing ili malware site, napadačev zahtjev zaobilazi provjeru autentičnosti i izravno pristupa neautoriziranim podacima
    - Izbjegavanje – izbjegavanje prosljeđivanja i preusmjeravanja, ciljani URL ne smije se temeljiti na parametrima koje unese korisnik, a ako se mora, onda provjeriti parametre, i provjeriti prava pristupa
- **Nedovoljna zaštita na transportnom sloju**
    - Nesiguran prijenos osjetljivih podataka, nisu identificirana mjesta na koja se osjetljivi podaci šalju
    - Posljedice – napadač pristupa i mijenja povjerljive i privatne podatke, neugodnost za napadnutu tvrtku, nezadovoljstvo korisnika, gubitak povjerenja
    - Izbjegavanje – zaštita adekvatnim mehanizmima (TLS na konekcijama), šifriranje poruka, digitalni potpis

IDS

- **Uljez**
    - osoba koja pokušava upasti u ili iskoristiti sustav ili njegove resurse
    - 2 kategorije – vanjski (iz vanjske mreže) i unutarnji (iz lokalne mreže)
- **Vrste upada**
    - Fizički – ako ima fizički pristup sustavu
    - Sistemski – želi doći do administratorskih prava
    - Udaljeni upad – s udaljenog računala, najopasniji, teško otkriti identitet uljeza
- **Razlozi upada**
    - Greške u softveru – buffer overflow, neočekivane kombinacije, pogrešno postupanje s unesenim podacima, problem višedretvenosti

- Sistemska konfiguracija – početna konfiguracija lako hakirana, lijeni administratori s praznim lozinkama, stvaranje rupa, iskorištavanje povjerenja prema nekim sustavima
- Probijanje lozinke – slabe lozinke, napad rječnikom, brute force
- Njuškanje nezaštićenog prometa – korištenje zajedničkog medija, njuškanje poslužitelja, udaljeno njuškanje
- Pogreške u dizajnu sustava – rupe u TCP/IP protokolu (smurf attacke, IP spoofing, SYN floods, mijenjanje IP datagrama), rupe u OS-u

- **Tipičan scenarij upada**
  - 1. korak: promatranje izvana – prikupljanje informacija o mreži
  - 2. korak: promatranje iznutra – pinganje računala, UDP/TCP scan
  - 3. korak: iskorištavanje – uljez koristi rupe u sigurnosti
  - 4. korak: upad – korisnik je uspješno upao u mrežu, skrivanje dokaza o upadu
  - 5. korak: unovčavanje – trgovanje podacim, DoS napad
- **IDS (Intrusion Detection System)**
  - Sustavi koji provode postupak otkrivanja uljeza
  - Komplementaran tehnikama prevencije (firewallu)
  - Nadzire aktivnosti korisnika i sustava, identificira neuobičajene aktivnosti i instalira zamke s ciljem otkrivanja napadača
  - **Dva temeljna pristupa za otkrivanje uljeza**
    - Tehnike na prepoznavanju uzoraka nepoželjnog ponašanja
    - Tehnike temeljene na proučavanju nepravilnosti i odstupanja od uobičajenog rada sustava i ponašanja korisnika
  - Položaj u mreži – nadziru mrežu ili računalo
  - Primjer: otkrivanje rootkita – rootkit stvara datoteke (sniffer logs), ručna potvrda – instalirati ps i promatrati procese ili pogledati mrežne konekcije (netstat), automatsko otkrivanje – IDS alati mogu otkriti datoteke koje pripadaju rootkitu
  - **Otkrivanje nepoželjnog ponašanja**
    - Promatrano ponašanje uspoređuje se s opisima poznatih nepoželjnih ponašanja
    - Dobre strane – precizni izvještaji
    - Loše strane – nužno osvježavanje potpisa, velika potrošnja računalnih resursa, ne može otkriti nove, neotkrivene smetnje
  - **Proučavanje nepravilnosti**
    - Ponašanje se uspoređuje s opisom predviđenog, legitimnog ponašanja
    - Alat prvo nauči što je normalna aktivnost u mreži
    - Dobre strane – moguće je otkriti nove, nepoznate napade
    - Loše strane – složena konfiguracija i učenje, velik broj lažnih alarma
  - **Metode detekcije upada**
    - Pregledavanje zapisa o kritičnim sigurnosnim događajima
      - Sve aktivnosti se bilježe i pohranjuju u zapis o nadgledanju
    - Obrada informacija „u letu“
      - Brzo izvlačenje i obrada informacija s ciljanog sustava („žrtve“)
      - Paketi preusmjereni prema IDS-u (sniffer)
    - Profili normalnog ponašanja
      - Kreiranje profila očekivanog ponašanja promatranjem korisnika
    - Potpis devijantnog ponašanja

        - Uključuje dinamični profil sastavljen od prepoznatljivih uzoraka vezanih uz radnje koje bi mogle predstavljati sigurnosni problem
    - Podudaranje parametara uzorka
        - Nadgledanje sistemskih operacija od strane administratora ili operatora
- IDS se smješta iza vatrozida i ispred alarmne mreže
- **Vrste sustava za detekciju upada**
    - **Network Intrusion Detection System (NIDS)**
        - Nadgleda pakete na mreži i pokušava otkriti ima li uljez namjeru upasti u sustav ili uzrokovati DoS
        - Mrežna kartica u promiskuitetnom načinu rada – čita sve pakete
        - Dobre strane – pasivno analizira podatke, nevidljiv napadaču
        - Loše strane – propušta pakete kod velikog zagušenja, ne radi ako je promet šifriran
    - **Host-based IDS**
        - Analizira napade na računalu na kojem je pokrenut
        - Dobre strane – pouzdan svjedok napada
        - Loše strane – ne znaju što se događa na nižim slojevima
    - **System Integrity Verifier**
        - Nadgleda sistemske datoteke kako bi otkrio pokušaj uljeza da ih promijeni
    - **Deception Systems**
        - Sadrži pseudo servise čiji je cilj oponašati dobro poznate rupe u zaštiti kako bi uhvatili uljeza
        - **Honeypot**
            - Uređaj koji predstavlja žrtvu napada
            - Svaka interakcija s njima je sumnjiva
            - Usporavaju ili zaustavljaju napad i zbunjuju napadača
            - Lako se ustanovi što je bio cilj napada
            - Loše strane – prate napad usmjeren samo na njih, napadači ih mogu preuzeti
- **Ograničenja IDS-a**
    - Prospojna mreža – ne postoji jednostavno mjesto gdje bi se priključio sniffer
    - Resursna ograničenja – mora nadgledati, analizirati i pohranjivati informacije generirane od velikog broja računala
    - Problem trenutačnog nadgledanja – zaprimljeni bitovi ne pružaju dovoljno informacija
    - Napadi prikrivanjem stringova – uljez može umetnuti podatak kako bi prikrio string
    - DoS – uljez može zatrpati sustav zahtjevima i onemogućiti reakciju
    - Metode zaobilaženja IDS-a – postoje metode kojima se može prevariti IDS

<u>Mail</u>

- **4 vrste sigurnosnih incidenata**
    - Neprikladno ponašanje koje nije specifično samo za elektroničku poštu (prijetnje, prevare)
    - Zlonamjerne poruke s neželjenim posljedicama po računalo korisnika (virusi, crvi)
    - Zloupotreba usluge (spam, hoax)
    - Gubitak privatnosti i anonimnosti
        - **Web bug**
            - Pošiljatelj može uključiti link na sliku koja kontaktira njegov web poslužitelj pa vidi tko je pročitao mail
        - **Kompromitiranje poruka u mreži**

        - Poruke prolaze kroz niz poslužitelja, vide ih svi na putu
        - Rješenja – šifriranje s kraja na kraj (S/MIME, PGP)
- **Simple Mail Transfer Protocol (SMTP)**
    - Specificira način prijenosa poruka između dva računala
    - Strogo definira sintaksu i redoslijed odvijanja transakcije – polazno računalo šalje naredbe na koje ciljno računalo mora odgovoriti statusnim kodovima
    - Naredbe
        - Obavezne: HELLO, MAIL, RCPT, DANA, RSET, VRFY, NOOP, QUIT
        - Neobavezne: SEND, SOML, SAML, EXPN, HELP, TURN
    - Čvorovi
        - MUA (Mail User Agent)
        - MTA (Mail Transfer Agent)
    - Sigurnosni problemi SMTP-a
        - Uopće nema sigurnosnih mehanizama
        - Otvoren i u tekstualnom obliku
        - Nema autentifikacije
- **Rješenja za osiguranje povjerljivosti**
    - **S/MIME**
        - Sigurnosno proširenje standarda MIME (Multipurpose Internet Mail Extensions)
        - Nije ograničeno samo na elektroničku poštu, koristi se i za druge protokole (HTTP)
        - Usluge kriptozaštite koje nudi S/MIME
            - Digitalni potpis
                - Autentifikacija
                - Cjelovitost poruke
                - Neporecivost
            - Šifriranje
                - Privatnost
                - Sigurnost podataka
        - Standard MIME omogućuje korištenje svih znakova, definiranje strukture i vrste poruke, dodavanje binarnih ili višemedijskih datoteka u poruku
        - Nova zaglavlja
            - MIME-Version – verzija MIME standarda
            - Content-Type – vrsta podataka u pojedinom MIME entitetu (text, image, audio, multipart (više MIME entiteta u tijelu jedne poruke)…)
            - Content-Transfer-Encoding – definira način kodiranja podataka u MIME poruci (7-bit, 8-bit, binary, quoted-printable, base64)
            - Content-ID – jednoznačno definira MIME entitet, slično kao Message-ID poruku
            - Content-Description – opis sadržaja
        - **S/MIME se temelji na Cryptographic Message Syntax**
            - Digitalni potpis, sažetak, autentifikacija, šifriranje bilo kojeg oblika podataka
            - Arhitektura temeljena na upravljanju ključevima i certifikatima
            - Funkcije (pišu se u Content-Type)
                - **enveloped-data**
                    - osigurava privatnost i sigurnost podataka
                    - stvara se jednokratni ključ za šifriranje te se šifrira za svakog primatelja njegovim javnim ključem

        - sve informacije se pohrane u vrijednost RecipientInfo koja se šifrira jednokratnim ključem za šifriranje
        - sve vrijednosti RecipientInfo se postave u vrijednost EnvelopedData
    - **signed-data**
        - osigurava autentičnost, cjelovitost i neporecivost
        - digitalni potpis formira se potpisivanjem sažetka poruke i šifriranjem tog sažetka privatnim ključem pošiljatelja
        - sadržaj i sažetak kodiraju se prema base64 u vrijednost SignedData
        - korisnik mora podržavati S/MIME za čitanje i verificiranje potpisa
    - **clear-signed-data**
        - digitalni potpis formira se potpisivanjem sažetka poruke i šifriranjem tog sažetka privatnim ključem pošiljatelja
        - samo se sažetak kodira prema base64
        - korisnik koji ne podržava S/MIME može čitati, ali ne može verificirati potpis
- Certifikati
    - Korisnici moraju nabaviti certifikate prije upotrebe
- S/MIME u praksi
    - Svi klijenti ne upravljaju dobro poštom
    - Problemi s čitanjem pošte preko weba (webmail)
    - Šifrira s kraja na kraj – ako je u pošti malware, on će proći neprimijećen
    - Traži certificiranje
    - Mogući napadi
        - Prijava pod tuđim imenom
        - Korištenje jednog certifikata, potpisivanje drugog korisnika
        - Krivotvorenje zaglavlja poruke
- **Pretty Good Privacy – PGP**
    - pet osnovnih usluga
        - autentifikacija
        - povjerljivost
        - sažimanje – događa se nakon digitalnog potpisa i prije šifriranja, podržan ZIP
        - kompatibilnost s infrastrukturom elektroničke pošte
        - segmentacija i ponovno slaganje poruke
    - upravljanje ključevima
        - PGP podržava više parova ključeva po svakom pošiljatelju i primatelju
        - Ključevi se pohranjuju lokalno na privjesku – PGP Key Ring
        - Nema središnjeg autoriteta, pojedinci jedni drugima potpisuju ključeve
        - PGP izračunava razinu povjerenja za svaki ključ na privjesku, korisnici sami interpretiraju razine povjerenja

<u>Sigurnost u mobilnoj telefoniji</u>

- Elementi sigurnosti
    - Fizička razina – gubitak uređaja
    - Razina radio signala – ometanje signala, prisluškivanje
    - Signalizacija – identifikacija korisnika i uređaja
    - Web aplikacija – sigurnost transporta paketa, zlonamjerne stranice
    - Aplikacije – sigurnost aplikacija

- **Prijetnje na pokretnim uređajima**
  - **Bluetooth**
    - Ranjivosti – loše implementiran BT složaj, pogrešne IRMC (Integrated Remote Management Controller) dozvole na datoteke, loše implementirane usluge temeljene na BT, otvoreni kanali
    - **Blue jacking**
      - Slanje poruka na uređaj putem BT
      - Bezopasno, ali oblik spama
    - **Blue snarfing**
      - Neovlašteni pristup uređaju s BT putem otvorenih kanala
      - Omogućuje pregledavanje i preuzimanje kontakata, slika, kalendara i poruka
    - **Blue bugging**
      - Slično blue snarfingu, ali omogućuje slanje naredbi uređaju (pozivanje brojeva, slanje SMS-a)
    - **Blue sniping**
      - Proširenje bluetooth napada većim dometom antene
  - **Malware**
    - Virusi, trojanci, crvi
    - Mogu pristupiti lokaciji ili pokretnoj mreži (naplata)
    - Prenose se elektroničkom poštom, linkovi na zlonamjerne stranice, instalacijom naizgled korisnih aplikacija, bluetoothom
    - Posljedice – krađa lozinki i povjerljivih podataka, brisanje podataka s uređaja, slanje SMS poruka na premium brojeme, uništavanje uređaja, šifriranje uređaja
    - Može se spriječiti šifriranjem i testiranjem aplikacija
    - Najugroženiji Android zbog velikog broja korisnika
  - **Wardriving**
    - Geokodiranje pristupnih točaka bežične mreže
    - Napadač se kreće područjem i zapisuje razine signala okolnih bežičnih mreža s GPS koordinatama
    - Može i ne mora biti zlonamjerno
    - Najčešća svrha je utvrđivanje otvorenih ili ranjivih pristupnih točaka
  - **RFID sniffing**
    - RFID (Radio Frequency Identification)
      - Jedinstveno identificira korisnika
      - Antena pobuđuje oznaku koja koristi EM polje antene kako bi odaslala vlastiti identifikator
    - Ako napadač ukrade ID korisnika može se lažno predstavljati
    - Zaštita – šifriranje podataka na oznaci, ograničeni doseg antene
  - **Uskraćivanje usluge (DoS)**
    - Ometanje signala, SMS bombardiranje
    - Automatsko odbijanje dolaznih poziva, periodičko odspajanje s mreže
    - Napadi ove vrste rijetki u mobilnoj telefoniji
  - **Web aplikacije**
    - Slične prijetnje kao i na računalima
    - Phishing, automatsko preuzimanje aplikacija s weba, rizici kod prijenosa podataka, rupe u mobilnim preglednicima

- **Sigurnosni element (SE)**
  - Sigurnosni hardver u koji se smještaju sigurnosno zahtjevne aplikacije
  - Sandboxing aplikacija
  - Provisioning – smještanje aplikacija ili podataka na sigurnosni element
    - OTA (over-the-air)
    - Putem Interneta
    - Putem NFC-a
    - Fiziči putem kartice
- **Obrana od napada**
  - Ažuriranje sustava na najnoviju verziju
  - Ne koristiti aplikacije ili dućane aplikacija treće strane
  - BYOD (Bring your own device) politika
    - Rješenje kontejnerizacija – virtualna particija na pokretnom uređaju na kojoj se nalaze osjetljive aplikacije i podaci
    - Uređaj ima profile – obični i sigurni
    - iOS standardno podržava, potrebno instalirati dodatne platforme na Android