Osnovni zahtjevi

Ranjivost – slabost u izvedbi sustava koju je mogu e iskoristiti kako bi se nanjela steta
Prijetnja – skup okolnosti koje mogu izazvati stetu
Napad – postupak kojim se iskoristava ranjivost sustava
Nadzor – mjere predostroznosti

Metode nanosenja stete: **Prekid, presretanje, promjena** (npr. promjena informacije u bazi)**, lažna informacija** (npr. dodavanje informacije u bazu).

Osnovni sigurnosni zahtjevi: **CIA – Confidentiality** (identifikacija i autentifikacija korisnika), **Integrity** (zastita podataka od promjene)**, Availability** (dostupnost usluge u promatranom trenutku ili vremenskom periodu)

Kriptografija

- **Kriptografija –** omogucuje sigurnu komunikaciju preko nesigurnog kanala
- **Postupak komunikacije:** otvoreni tekst + kljuc = sifrat
- **Kriptoanaliza –** znanstvena disciplina koja se bavi proucavanjem postupaka za citanje sifrata bez poznavanja kljuca
- **Kriptologija –** Kriptografija + kriptoanaliza
- **Kriptoalgoritam –** matematicka funkcija za sifriranje i desifriranje
- **Dizajn algoritma –** zbrka – odnos izmedju kljuca i sifrata mora biti slozen, rasprsivanje – svaki ulazni bit mora imati utjecaj na velik broj izlaznih bitova
- **Simetricna kriptografija – isti kljuc za sifriranje i desifriranje**
- **One time pad –** razmjena kljuca dugog kao poruka, neprobojan, dug kljuc, velik broj kljuceva za vise korisnika
- **Stream cipher –** iz kljuca se generira pseudoslucajni niz brojeva i koristi kao kljuc. **Sinkroni** – pseudoslucajni ne ovisi o otvorenom tekstu i sifratu, **Samosinkronizirajuci** – prethodnih N bitova sifrata se koristi za izradu kljuca. **Uporaba:** Bankomati, SSL, bezicna komunikacija. **Algoritmi:** RC4, Helix, Wake, A5/1
- **Block cipher –** otvoreni tekst se podijeli u blokove, preslikava block otvorenog tekst u blok sifrata jednake velicine. **Algoritmi:** DES, AES, RC2, RC5, Blowfish

- **Kada su podaci dulji od bloka:**
  - **ECB** – blokovi se sifriraju nezavisno, ne treba IV
  - **CBC** – sifrat prethodnog XOR blok
  - **PCBC (Propagating CBC)** – prev(poruka xor sifrat) xor blok
  - **CFB (Cipher feedback)** – sifrirani sifrat prev bloka XOR blok
  - **OFB (Output feedback)** – sifrirana sifra prev bloka XOR block
- **Asimetricna kriptografija:** jedan kljuc za sifriranje, drugi za desifriranje, nemogu e izracunavanje privatnog iz javnog u razumnom vremenu. **Primjena:** prijenos podataka, autentifikacija, digitalni potpisi, razmjena tajnih kljuceva.
- **Kriptoanaliza:** brute-force napadi, treba dulji kljuc
- **Dobre strane:**
  - **Simetricni –** brzina, jednostavnost
  - **Asimetricni –** upravljanje kljucevima, tajnost, distribucija
  - **Hibridni –** razmjena simetricnih kljuceva koristenjem asimetricne kriptografija
- **Digitalni potpis:** posiljatelj potpisuje poruku koristeci svoj privatni kljuc, potpis se provjerava javnim kljucem.
- **Hash funkcija:** pretvara proizvoljno dug niz znakova na ulazu u niz fiksne duljine na izlazu. **Primjena:** digitalni potpis, authentifikacija, hash-tablice, za jednoznacu identifikaciju binarnih sadrzaja, checksum. **Algoritmi:**
  - **SHA-1 –** 160 bita, otkrivene kolizije u 2^69 hasheva
  - **MD5 –** 128 bita, razvaljen 2008
  - **DSS (Digital signature standard) –** 80 bita, samo za potpis
- **Postupak digitalnog potpisivanja:**
  - Izracuna se hash poruke
  - Hash se potpise privatnim kljucem i doda na poruku
  - Iz poruke se vadi hash i desifrira javnim kljucem
  - Poruka se hashira i provjerava se s dobivenim hashem

Digitalni certifikat

- **Sadržaj certifikata:**
  - Informacije o korisniku (ime, institucija, drzava)
  - Serijski broj
  - Informacije o vazenju certifikata
  - Informacije o povlacenju certifikata (CRL)
  - Javni kljuc
  - Informacije o instituciji koja je izdala certifikat
  - Digitalni potpis institucije
- **X.509 certifikat**:

    - propisana sintaksa ASN.1
    - kodiranje DER (.cer)
    - kodiranje Base64 (.pem)
    - PKCS#12 (.pfx) – javni i privatni kljuc

- **Vazenje certifikata**
    - Javni kljucevi se mogu dugo koristiti
    - Privatni trebaju trajati sto krace
    - Opoziv kljuca:
        - potpisani dokumenti ne vrijede
        - prije potpisani dokumenti su kompromitirani
    - Provjera certifikata
- **CRL – certificate revocation list –** digitalni objekt koji sadrzi listu opozvanih certifikata i razloga opoziva, potpisuje ju izdavatelj i ima period vazenja.
- **Dijelovi CRL:**
    - informacije o CRL
    - vazenje CRL
    - serijski brojevi povucenih certifikata
    - informacije o instituciji koja je izdala CRL
    - digitalni potpis institucije
- **Vrste CRL:**
    - **Kombinirana -** sadrzi popis svih opozvanihcertifikata ciji period vazenja nije istekao
    - **Segmentirana –** Svaki segment sadrzi sve opozvane certifikate, bez obzira na period vazenja
- **CA – certificate authority –** povjerljiva treca strana, izdaje certifikate i jamci vezu subjekta s javnim kljucem, izdaje i upravlja CRL-ovima, potpisuje svaki certifikat i CRL
- **Odgovornosti CA:** zastita svog priv kljuca, provjera tocnosti podataka prije izdavanja, zastita profila, odrzavanje CRL, distribucija certifikata i CRL, arhiva nakon isteka certifikata
    - Delegacija posla trecim stranama:
        - **RA – registration authority**
        - **Javni imenik –** distribuira CRL i cert, X.500, LDAP
        - **Arhiva**
- **RA –** prikuplja informacije o korisniku i provjerava ih, odobrava izdavanje certifikata prema CA.
- **CP – certificate policy –** odredjuje svrhu koristenja certifikata
    - CP – opcenit dokument, opisuje pravila rada CA i odgovornosti, javno se objavljuje
    - CPS – certifitace practice statements – detaljan dokument, opisuje kako CA implementira CP, ne treba se objaviti

- **Certificate holder –** subjekt koji raspolaze s priv kljucem, dobiva certifikat od CA kroz RA, autentificira se, izradjuje elektronicki potpis, desifrira podatke i sl.
- **Pouzdaju e strane (relaying parties) –**korisnici koji raspolazu s javnim kljucem, koriste repozitorij CA, provjeravaju potpise, sifriraju i sl.

Operacijski sustavi

- **Osnovne metode zastite:**
  - **Razdvajanje**
    - objekti jednog korisnika nisu vidljivi drugom
    - fizicko, vremensko, logicko, kriptografsko
  - **Dijeljenje**
    - **razine zastite –** bez zastite, izolacija, public/private, kontrola pristupa, dinamicko pravo pristupa, kontrola pristupa + onoga sto se radi s objektom
    - **upitna granularnost:** bit, byte, word, polje, zapis, datoteka, disk...
- **Taksonomija pogresaka:**
  - **namjerne –** zlonamjerne i nezlonamjerne (BO, nesanitizacija, TOCTTOU)
  - **nenamjerne –** pogreske pri provjeri valjanosti, pogreske u kontroli pristupa, neadekvatna autentifikacija, narusavanje granicnih uvijeta, logicke pogreske
- **Ranjivosti Unixa -** daemoni (BO), rootkitovi, ENV, /tmp, TOCTTOU
- **Ranjivosti Windowsa –** Registry, Administrator account, enabled by default (IIS, MSSQL)
- **Distionary attack –** rijecnik, precomputed rainbow tables, salting
- **Malware –** skup instrukcija koji se pokrecu kako bi se nacinila steta
- **Mjesaju se podaci i izvorni kod (**interaktivne app**), dodatne funkcionalnosti (**Word, Excel, Postscript)
- **Virus –** racunalni program, dodaje svoj kod aplikacijama, pokrece se iskljucivo djelovanjem korisnika, samostalno se umnaza na racunalu, siri se djelovanjem korisnika (E-mail, USB/DVD, mreza)
  - Prepisuje kod preko, prije ili nakon originalnog ili u MBR/PBS.
  - **Antivirusi –** prepoznavanje koda (fingerprinting), heuristika (prepoznavanje ponasanja)
    - Akcije: popravlja datoteku, stavlja u karantenu, brise datoteku
    - **Nuzan redovit update baze fingerprintova**

        - **Nadzor ponasanja – sumnjive akcije:**
            - pisanje u izvrsne programe
            - pristup MBR-u
            - pristup svim datotekama u direktoriju
            - pristup mrezi
            - pokusaj formatiranja diska ili brisanja sadrzaja istog
            - slusanje na nekom portu
        - **Provjera integriteta –** racuna se hash svake dat i sprema u bazu, upozorava korisnika ako se pocnu razlikovat
        - **Tips:** ne koristiti admin ovlasti, onemoguciti nepotrebne servise, ograniciti pristup kljucnim datotekama, formirati grupe korisnika, koristiti software za zastitu, benchmarkati
        - **Samoodrzavanje:**
            - **Prikrivanje (stealth) –** prikrivanje prisutnosti, presretanje provjere AV-a i dojava ispravnosti
            - **Viseoblicje (polimorfizam) –** neznatno mijenja kod, ali ne i funkcionalnost
            - **Metaoblicje (metamorfizam) –** mijenja i funkcionalnost
            - **Onemogucavanje AV-a**
- **Crvi –** samostalno se umnazaju, samostalno se sire (iskoristavaju nedostatke pri prijenosu podataka, koriste mrezu, blokiraju ostali promet, mass-mailing), originalno koristeni za pronalazak slobodnih procesora u znanstvene svrhe
    - **Dijelovi:**
        - **Bojna glava –** dio koda koji iskoristava ranjivost (BO, file sharing, e-mail, kradja lozinki), backdoor
        - **Pogon –** nakon iskoristavanja ranjivosti mora se infiltrirati u sustav (e-mail, (T)FTP, SMB, HTTP)
        - **Algoritam za odabir mete –** trazi novu metu putem e-mail adresa, /etc/hosts, known_hosts, DNS, generiranjem adresa u istom subnetu
        - **Sustav za odabir mete –** na popis generiran od algoritma radi se scan ranjivosti i otvorenih portova i formira se nova "raketa"
        - **Korisni teret –** otvaranje backdoora, DdoS, koristenje procesorske snage za izracun, izvodjenje drugog napada
    - **Poteskoce:**
        - raznolika okolina zrtvi (nema IE, TFTP..) - mogucnost prilagodjavanja, ali lakse primjeceni zbog velicine
        - ne smiju unistiti racunalo ili zagusiti mrezu
        - ne smije sam sebe pregaziti i ne smije dopustiti da ga drugi crv pregazi

    - **Buducnost –** multiplatformski, iskoristavanje vise ranjivosti, iskoristavanje 0-day exploita, brze sirenje, viseoblicje, metaoblicje
    - **Obrana –** antivirusi, patching, firewall, auditing
- **Trojan – podijela:** zlocudni programi maskirani kao korisni i programski kod ugradjen unutar korisnih programa
    - izgledaju bezopasno
    - ne izvrsavaju se samostalno (potrebno pokrenuti) – SE
    - Isti nazivi kao legitimni procesi
    - Distribuiraju se putem keygena i ilegalnih patcheva
    - Sto mogu: remote access, file sharing, unistavanje podataka, DoS, otvaranje web stranica, sirenje virusa, botnet, keylogging...
- **Rootkit –** trojanski backdoor koji mijenja postavke OS-a
    - zamijenjuje ispravne verzije programa (ls, kill, ps..) i omogucuju udaljen pristup (ssh)
    - user-level rootkit: ima ovlasti korisnika, mijenja aplikacije
    - kernel-level rootkit: mijenja sam OS, admin ovlasti, sakrivaju svoje postojanje
- **Spyware –** skuplja informacije o korisniku (keypress, web stranice, keywords i sl.)
    - **Ciljevi:** kriminal (kradja kartica) i personalizirani marketing
    - **Instalacija:** s drugim legitimnim programima, trojancima, klikanjem na dialog boxeve, koristenjem bugova u preglednicima
    - **Detekcija:** racunalo radi sporije, rusi se i otvaraju se popup
- **Adware –** prikazuje i dohvaca reklamne poruke

Ranjivosti internetskih protokola i aplikacija

- **Metode napada:**
    - **sniffing/eavesdropping –** dohvacanje informacija bez autorizacije
    - **spoofing –** slanje poruke s tudjim identitetom
    - **replaying –** ponavljanje snimljenih poruka
    - **MITM –** emulacija komunikcaije s obje srrane
    - **(R)ARP**
    - **napad na switch**
    - **message tampering –** promjena poruka
    - **fragementation attack**
- **Sniffing –** postavlja NIC u promiskuitetni nacin, vidi sav promet na ethernet segmentu
    - **Detekcija:**

        - **Ping –** saljemo ping na adresu gdje sumnjamo da je sniffer, ali s krivom MAC adresom
        - **ARP –** salje se ARP zahtjev s promjenjenom MAC adresom
        - **DNS –** salje se ping s IP-em koji ne postoji, ako se pojavi DNS upit za navedeni IP
        - **Honeypot –** namjerno pustimo fake U/P kroz mrezu i gledamo hocemo li dobiti pokusaje ulogiravanja.
    - **Sprjecavanje:** Zamjena HUB->Switch, enkripcija (SSL, PGP, ssh, VPN)
- **ARP spoofing –** odgovori na arp upite s MAC adresom naseg racunala = preusmjeravanje prometa kroz nase racunalo.
    - **Detekcija:** pregledom ARP cache-a ili s treceg racunala koje slusa lazne arp odgovore
    - **Prevencija:** koristenje switcheva s port security-em ili arp inspectionom
- **Napadi na switch:**
    - **MAC flooding –** zapuni se forwarding table i switch predje u hub nacin rada
    - **MAC cloning –** napadac promjeni MAC adresu na neku postojecu i switch mu forwarda pakete
- **IP spoofing –** slanje IP datagrama s laznom adresom posiljatelja
    - obrana: filtriranje prometa, zabrana koristenja R suitea (rlogin, rcp, rsh...), TCP seq number
- **Napadi fragmentacijom –** koristi se kada je potrebno IP datagram podijeliti na vise dijelova da stanu u ethernet okvir, radi se na izvoristu i svim routerima izmedju, sastavlja samo na odredistu. Moze zavarati neke firewalle.
    - **Ping of death –** kreira se ICMP echo request paket veci od 65535 okteta i dolazi do BO - DoS
    - **Teardrop –** salju se dva fragmenta koji se djelomicno prekrivaju – crash nakon sastavljanja zadnjeg fragmenta (Linux kernel <2.0.32) - DoS
    - **TCP overwrite –** prepisuje se header proslog fragmenta pomocu offseta i tako se mijenja port
- **ICMP napadi –** u pravilu se radi o DoS napadima s ciljena zagusenja mreze i onemogucavanja pristupa resursima
    - **smurf napad –** salje se ICMP echo request na sveodredisnu adresu posrednicke mreze s laznom informacijom o IP source (postavljenom na adresu zrtve). Svi odgovori idu na adresu zrtve = posrednicka mreza i zrtva zatrpani
- **UDP napadi –** beskonenkciji, nepouzdan, nema kontrole toka, koristi se za prijenos visemedijskih podataka i usluga temeljene na request/reply
    - **UDP spoofing –** mijenjamo izvorisnu adresu UDP paketa
    - **UDP hijacking –** slusamo vezu i odgovaramo na UDP zahtjeve prije servera

- **UDP storm –** lazira se izvorisna adresa i port i povezu se dva automatska udp servisa (npr. chargen i echo)
- **Skeniranje UDP portova –** ako su zatvoreni odgovaraju s ICMP port unreachable, ako ne onda su vjerojatno otvoreni, spora tehnika zbog ogranicenja ICMP poruka od strane OS-a, mogucnost gubitaka UDP paketa putem = krivi rezultati

- **TCP napadi**
  - **port scan –** skeniramo portove da bi prikupili informacije o zrtvi. Trazimo slabosti u servisima
    - TCP connect() - usostavlja se potpuna veza s portom (3-way handshake), laka detekcija
    - TCP SYN – salje se samo SYN paket, ako dobijemo RST nije otvoren, ako dobijemo SYN/ACK je. Zatvaramo odmah s RST
    - TCP FIN – salje se samo FIN faket, ako dobijemo RST zatvoren, ako ne dobijemo nista onda je otvoren
    - Fragmentation scan – fragmentira se TCP zaglavlje – teza detekcija
    - Idlescan – koristi se trece racunalo (zombi). S njega se dobije IP ID (SYN/ACK paket, RST odgovor), onda se s njegovom source adresom posalje SYN paket, zatim se opet od njega zatrazi IP ID. Ako je veci za 2, port na koji smo poslali SYN je otvoren.
  - **TCP obmana** – slanje paketa s source adresom racunala kojem vjeruje napadnuto racunalo, problem pogadjanja ISN-a i ack numbera
  - **TCP hijacking** – preuzima se kontrola nad TCP vezom, slusaju se razmjenjeni paketi, desinkronizira se veza, dodaje ili brise podatke
  - **ACK storm –** paketi koje salju server i klijent imaju neispravne SEQ i ACK brojeve, beskonacna petlja, zagusuju promet
  - **SYN flood –** salju se SYN paketi s ne postojecom source adresom, SYN/ACK ne dolazi nigdje, konekcije ostaju polu otvorene i zapunjuju memoriju racunala - DoS

Firewall

- **Perimiter security:** routeri, firewall, IDS, VPN, softwareska arhitektura, DMZ
- **Firewall –** mrezni uredjaji koji dopusta mreznu komunikaciju u skladu s ACLovima
  - **filtrira pakete –** ovisno o sadrzaju
  - **proxy –** forwarda upite klijenata
- **Ogranicenja –** ne moze se nadzirati sadrzaj, redoviti update filtera, ne stite unutar lokalne mreze, performanse, kompromitiranje firewalla
- **Screened router –** usmjeritelj s mogucnoscu filtriranja paketa
- **Bastion host –** kriticna, ali dobro osigurana tocka u mrezi
- **Dual homed gateway –** koristi se bastion host kao gateway i proxy, onemogucena direktna komunikacije interne i javne mreze
- **Screened host gateway –** screening router + bastion host. Bastion host u internoj mrezi, ali jedini dostupan iz vanjske. Sav ostali promet prema internoj mrezi blokiran. Izlaz preko proxy-a na bastion hostu.
- **Screened subnet –** izoliran subnet izmedju privatne i javne mreze. Dozvoljen pristup u subnet iz obje mreze. Promet izmedju privatne i javne onemogucen. U subnetu bastion hostovi.
- **DMZ – demilitarizirana zona –** Podrucje mreze izmedju 2 filtera. Unutra idu javni servisi, bastion hostovi.

Infrastruktura

- **Napadi na DNS –** pokvareni podaci, neutorizirana osvjezenja, promjene podataka o zoni (glumljenje mastera), zagadjenje cache-a i glumljenje cache-a
- **Ciljevi napada:**
  - **DoS –** slanje negativnih odgovora, preusmjeravanja na posluzitelj za koji smo sigurni da ne zna odgovor
  - **Masquerading –** preusmjeravanje i predstavljanje kao pravi posluzitelj, curenje informacija
  - **Domain hijacking –** preuzimanje domene kompromitiranjem nesigurnih mehanizama osvjezavanja
- **Tipovi napada na DNS:**
  - cache poisoning
  - kompromitiranje posluzitelja
  - spoofing posluzitelja
- **Cache poisonong – Kaminsky attack –** salje se upit za nepostojece adrese i istovremeno se salje velik broj odgovora koji sadrze razlicite query ID-eve, ali i laznu adresu za postojeci server unutar domene (www.paypal.com, a lazni upiti za aaaa.paypal.com)

- **Zastita:**
  - **TSIG – transaction signature –** provjerava identitet pomocu kljuc, obicno kod zone transfera ili dinamickog osvjezavanja podataka, obje strane moraju imati kljuc
  - **DNSSEC – DNS security extensions –** provjerava identitet, "Anchors of trust", problemi s implementacijom
    - osigurava kriptografski dokaz ispravnosti primljenih podataka
    - ne bavi se dinamickim osvjezavanjem ili zone transferom
    - koristi asimetricnu kriptografiju (potpisivanje) izmedju autorativnog NS-a i resolvera
    - Vjerovati ako je root potpisan (15.7.2010)
    - Ne osigurava povjerljivost i ne stiti od DdoS napada
    - Odgovori puno duzi, ponovno potpisivanje kod promjene podataka
- **Napadi na usmjeravanje:**
  - **Utjecaj:**
    - **Podoptimalno usmjeravanje**
    - **Zagusenje**
    - **Particioniranje –** odvajanje mreza, nemogucnost komunikacije s racunalima u drugim mrezama
    - **Preplavljivanje posluzitelja –** oruzje za DoS napade
    - **Kreiranje petlji**
    - **Presretanje prometa**
  - **Tipovi napada:**
    - **Napadi na link**
    - **Napadi na usmjeritelj**