Vatrozid

Perimetar -> routeri, firewall, intrusion detection system, vpn, softverska arhitektura, DMZ

Firewall -> mrežni uređaj koji dopušta, zabranjuje ili prosljeđuje mrežne konekcije u skladu sa sigurnosnom politikom
-> hardverski ili softverski
-> filtriranje paketa ili proxy usluge (komunikacija s poslužiteljima umjesto klijenata)

Screening router -> router ili računalo koje obavlja routing uz mogućnost filtriranja paketa
-> mogućnost blokiranja prometa između mreža ili određenih računala

Bastion host -> kritična, ali dobro osigurana točka u mreži

Dual Homed Gateway -> između privatne mreže i interneta se smješta Bastion host te je direktna komunikacija onemogućena, već sve ide preko korisničkih računa na Bastionu

Screened Host Gateway -> Bastion host je u privatnoj mreži skupa s klijentima te je jedino Bastionu dozvoljen pristup iz javne mreže

Screened Subnet -> Izolirana podmreža između interneta i privatne mreže te je dozvoljen pristup računalima (Bastion host) u podmreži iz javne i iz privatne mreže, ali je promet između privatne i javne mreže onemogućen

DMZ -> demilitarizirana zona, područje mreže između dva filtera paketa, odvaja vanjsku i unutarnju mrežu, sadrži računala koja osiguravaju vanjske usluge i application gateway

Application Gateway / Proxy Gateway -> interpretira protokol određene aplikacije, može obavljati napredno filtriranje

Filtriranje paketa -> selektivno se propuštaju paketi između unutarnje i vanjske mreže na temelju protokola, IP adresa, izvorišnog/odredišnog porta, itd.
-> ranjivo na spoofing, fragmentirani datagrami mogu biti problematični, može se zaobići tuneliranjem

Stateful Inspection -> filtriranje paketa te provjera i održavanje informacije o stanju svake konekcije
-> može se pratiti slijed sesije te provjeravat svaki paket

iptables -> input, output, forward
-> accept, drop, reject (drop ali šalje icmp poruku ili tcp reset)

NAT -> network address translation
-> RFC 3022
-> pretvorba privatnih IP adresa u globalno jedinstvene javne adrese
-> proxy jer jedan host šalje zahtjeve u ime svih internih računala
-> **statička translacija** -> kada postojeći resursi unutar privatne mreže moraju biti javno dostupni onda se preslikava područje javnih IP adresa u blok iste veličine s privatnim adresama
-> **port forwarding** -> statička translacija u kojoj se prosljeđuje promet za samo određeni port, a ne za cijelu IP adresu
-> **dinamička translacija** -> veća grupa internih klijenata dijeli jednu IP adresu ili malu grupu internih adresa u svrhu skrivanja identiteta ili proširivanja prostora raspoloživih adresa, a translacija se kreira tek kad unutarnji klijent uspostavi konekciju kroz NAT

NAT problemi -> neki protokoli ne rade ispravno kad se promijeni broj porta
-> teoretski najviše 65536 konekcija na jednoj IP adresi, ali u pravilu ograničeno na < 50000 konekcija

Moguće hakirati klijente unatoč NATu jer statička translacija ne štiti unutarnja računala. Primjer: upiše se cijeli put do odredišta, NAT uređaj se upiše kao jedna od adresa, a NAT zatim usmjerava datagram do krajnjeg odredišta

Ili korisnik može otvoriti falsificirani email s linkom na web stranicu koja u podlozi skriva trojanskog konja

Honeypot -> računalo ili resurs namjerno stavljen na mrežu kako bi se iskoristio ili manipulirao te se time otkriva nedozvoljena aktivnost

Mobilne mreže

Smartphone prijetnje -> sigurnost aplikacija, bluetooth, malware, wardriving, RFID sniffing, DoS, web aplikacije, gubitak privatnosti (čitanje i preuzimanje poruka/kontakata), financijski gubici (fejk sms poruke), krađa identiteta (RFID)
-> zlonamjerna aplikacija ne predstavlja prijetnju samo vlasniku nego i mreži na koju se spaja
-> tako mreža koja je dobro zaštićena prema internetu može biti kompromitirana

Weak Server Side Controls -> loša kontrola na poslužitelju
-> loše programirano, slaba autentifikacija, upravljanje sjednicama, konfiguracija poslužitelja, napadi umetanjem

Insecure Data Storage -> nesigurna pohrana osjetljivih podataka
-> GDPR regulativa u europi

Insufficient Transport Layer Protection -> nedovoljna zaštita na transportnom sloju
-> česta ranjivost kod svih internetskih aplikacija općenito
-> koristiti HTTPS odnosno SSL/TLS !!!

Unintended Data Leakage -> curenje podataka
-> tijekom razvoja se sve zapisuje u logove a na produkciji ne bi smjelo
-> zbog cachiranja malware može dobiti pristup pohranjenim podacima druge aplikacije

Poor Authorization and Authentication -> loša autorizacija i autentifikacija
-> zbog generalno kraćih lozinki se olakšava napad na lozinke
-> očekuje se da će samo legitimni korisnici pristupati poslužitelju, ali to nije nužno slučaj

Broken Cryptography -> loše upravljanje kriptografijom
-> kriptografija postoji ali su ključevi lako vidljivi napadačima
-> npr korištenje samo ugrađenih mehanizama šifriranja
-> loše upravljanje ključevima
-> izrada vlastitih mehanizama šifriranja
-> korištenje zastarjelih algoritama

Client Side Injection -> umetanje na klijentskoj strani
-> npr korisnik izvede SQL injection ili File inclusion

Security Decisions Via Untrusted Inputs -> sigurnosne odluke na temelju nepovjerljivih izvora
-> **Inter process communication** (IPC) -> mehanizam za dijeljenje podataka između aplikacija
-> jedna aplikacija šalje podatke drugoj poput zahtjeva za lokacijom ili autorizacije
-> s obzirom da malware može pristupiti tim podacima, ne bi trebalo slati osjetljive podatke

Improper Session Handling -> loše upravljanje sjednicom
-> sjednica = pristup pravima korisnika koji je “vlasnik” sjednice
-> cookies, tokeni, …
-> problemi s odjavljivanjem na poslužitelju, vremenska kontrola, upravljanje kolačićima, nesigurni tokeni

Lack of Binary Protections -> nedostatak zaštite binarnog koda aplikacije
-> iz binarnog zapisa je moguće doći do izvornog koda aplikacije
-> u originalnu aplikaciju se nakon otkrivanja izvornog koda ubacuje dodatni kod koji se prikriva kao korisna aplikacija
-> zaštita je detektirati je li uređaj jailbreakan ili rootan te provjeravati

zaštitnu sumu ili detektirati je li aplikacija pokrenuta u debug načinu rada

Code tampering -> mijenjanje podataka i knjižnica koje aplikacija koristi

Reverse Engineering -> otkrivanje izvornog koda
-> promjena funkcionalnosti i ponovna objava aplikacije

Bluetooth ranjivosti -> loše implementiran BT složaj, pogrešne IRMC dozvole na datoteke, loše implementirane usluge temeljene na BT, otvoreni kanali

Blue jacking -> slanje poruka na uređaj putem BT, bezopasno ali spam

Blue snarfing -> neovlašteni pristup uređaju s BT, pronalazi otvorene BT kanale i pristupa uređaju

Blue bugging -> kao blue snarfing, samo što se mogu pozivati brojevi i slati SMS poruke pa se preusmjerava na uređaj napadača, a napadnuti uređaj se predstavlja kao BT slušalica

Blue sniping -> valjda isto kao i blue snarfing samo sa većim dometom zbog antena (do 2km)

Malware -> virusi, trojanci i crvi
-> treba testirati aplikacije kako bi se utvrdilo jesu li štetne za korisnike ili third-party
-> ako su u redu, izdaje se potpis kojim se jamči da je aplikacija prikladna
-> Android -> najugroženiji zbog velikog broja korisnika
-> Blackberry -> najčešće spyware, trojan Zeus
-> Symbian -> najviše postojećeg malwarea i mogućnost da korisnici sami instaliraju aplikacije preuzete s interneta
-> Windows Mobile -> sličan problem kao Symbian
-> iOS -> prilično siguran, jedini potencijalni problem su aplikacije koje pohranjuju korisničke profile na webu i naravno jailbreak

Pegasus -> iskorištavao ranjivosti iOS-a do verzije 9.3.5.
-> klikom na poveznicu telefon se jailbreaka i instalira se malware koji čita poruke, prati pozive, lokacije, …

AdWare -> na Androidu
-> 42 aplikacije na play storeu sa istim AdWareom
-> AdWare se pokreće kao pozadinski servis i komunicira sa C&C poslužiteljem i šalje podatke o uređaju, OSu, itd.
-> nasumično pokreće oglas preko aplikacije

Wardriving -> geokodiranje pristupnih točaka bežične mreže (uređaj sa WiFi i GPS)
-> napadač se kreće područjem i zapisuje razine signala okolnih bežičnih mreža s GPS koordinatama

-> ne mora biti zlonamjerno već se najčešće koristi za utvrđivanje otvorenih ili ranjivih pristupnih točaka

RFID sniffing -> radio frequency identification
-> antena pobuđuje oznaku koja koristi elektromagnetsko polje antene kako bi odaslala vlastiti identifikator
-> RFID jedinstveno identificira korisnika (alternativa kreditnim karticama itd)
-> ako napadač ima pristup uređaju koji jedinstveno identificira korisnika onda se napadač može lažno predstavljati

-> zaštita -> šifriranje podataka na oznaci, ograničeni doseg antene, beskontaktno plaćanje, itd…

Sigurnosni element -> sigurnosni hardware u koji se smještaju sigurnosno zahtjevne aplikacije
-> sa ili bez NFC-a

Komunikacija sa SE -> provisioning -> smještanje aplikacija ili podataka na sigurnosni element
-> OTA, putem interneta, putem NFC-a, fizičkim putem

DoS -> ometanje signala, SMS bombardiranje, automatsko odbijanje dolaznih poziva, periodičko odspajanje s mreže
-> rijetko se viđa u mobilnoj telefoniji

Web aplikacije -> phishing
-> preuzimanje aplikacija s weba
-> rizici kod prijenosa podataka
-> zaštita je upgrade softwarea i ne koristiti third-party aplikacije

Kontejnerizacija -> virtualna particija na pokretnom uređaju na kojoj se nalaze osjetljive aplikacije i podaci
-> uređaj ima profile npr obični i sigurni

IoT

Uzroci loše sigurnosti -> fokus na funkcionalnost sustava/uređaja i sučelja prema korisnicima te se pokušava skratiti vrijeme razvoja zbog konkurencije

Zbog toga što razvijatelji nisu sigurnosni stručnjaci, iskusni napadači mogu pronaći i lako iskoristiti ranjivost

Složaj -> IoT, sučelja u oblaku, mobilna sučelja, web sučelja, mreža, OS, sklopovlje

OWASP -> Open Web Application Security Project
-> smjernice za razvoj sigurnih aplikacija/usluga i testiranje nesigurnih

Application Security Verification Standard -> kuharica za izradu sigurnih (web) aplikacija

Weak Guessable or Hardcoded Passwords -> korištenje jednostavnih lozinki
-> statičke lozinke ili tokeni
-> predvidljivi tokeni / identifikatori sjednica
-> treba uvesti osnovne zahtjeve poput nemogućnosti postavljanja jednostavne lozinke, zaključavanje nakon N pogrešnih lozinki, nemogućnost dolaska do podataka korisnika preko zaboravljene lozinke

Insecure Network Services -> korištenje servisa koji nemaju sigurnu implementaciju/verziju
-> skeniranje portova kako bi se utvrdilo što je pokrenuto, provjera ranjivosti otvorenih servisa, paziti na UPnP portove

Insecure Ecosystem Interfaces -> objedinjene 3 ranjivosti (I1, I7 i I6)
-> nesigurna sučelja weba, mobilne aplikacije za pregled podataka i upravljanje uređajima (mogućnost preuzimanja kontrole putem aplikacije)

Lack of Secure Update Mechanism -> prijenos ažuriranja mora biti šifriran
-> ažurirani software/firmware ne smije sadržavati hardkodirane autentifikacijske podatke
-> treba autentificirati poslužitelja

Use of Insecure or Outdated Components -> korištenje zastarjelih ili nesigurnih komponenti
-> treba pobrojati što se sve koristi, te provjeriti je li ažurirano

Insufficient Privacy Protection -> treba paziti na to što IoT uređaj skuplja od podataka i što se sa njima radi, te jesu li u nekoj mjeri anonimizirani
-> inače napadač može kompromitirati takve podatke

Insecure Data Transfer and Storage -> nepostojanje šifriranja prometa na transportnom sloju
-> potrebno ispravno korištenje PKI

Lack of Device Management -> loše upravljanje i nadzor IoT uređaja

-> treba znati rade li ispravno, u kojem su stanju, itd…
-> rogue node -> lažni uređaj

Insecure Default Settings -> nesigurne pretpostavljene postavke
-> treba omogućiti da korisnik sam forsira jake lozinke, da se logiraju sve akcije u sustavu, da se šalju upozorenja u slučaju incidenta putem maila, smsa, alarma, …

Lack of Physical Hardening -> jednostavan fizički pristup uređaju
-> napadač može onda očitati podatke sa memorijske kartice ili se na uređaj spojiti sa USBom, itd.
-> treba onemogućiti jednostavno otvaranje uređaja te spajanje na ulaze

SSDP DDoS -> amplification napad
-> na uređajima poput PS4, Smart TV, kamere, itd.
-> koriste SSDP za objavu slanjem paketa na multicast adresu
-> nakon objave, računala ih mogu zatražiti karakteristike/usluge
-> napadač lažira IP adresu žrtve i zatraži karakteristike od velikog broja UPnP uređaja

Mail

4 vrste sigurnosnih incidenata -> neprikladno ponašanje (prijetnje, prevare, …)
-> zlonamjerne poruke (virusi, crvi)
-> zlouporaba usluge (spam, hoax)
-> gubitak privatnosti i anonimnosti (kompromitiranje poruka u mreži)

Web bug -> klijent e-pošte prikazuje HTML, pošiljatelj može uključiti link na sliku koja kontaktira njegov web-poslužitelj i saznati tako tko je pročitao mail

Kompromitacija poruke -> poruke prolaze kroz niz mail poslužitelja te ju vide svi na putu
-> rješenje: zahvati u infrastrukturi sustava, šifriranje s kraja na kraj

Simple Mail Transfer Protocol -> specificira način prijenosa poruka između dva računala
-> strogo definira sintaksu i redoslijed odvijanja transakcije
-> čvorovi: Mail User Agent i Mail Transfer Agent
-> obavezne naredbe (HELO, MAIL, RCPT…) i neobavezne (SEND, SOML, SAML, …)

Jednostavan opis SMTP:

1. pošiljatelj se spaja na port 25
2. dobiva odgovor 220
3. pošiljatelj šalje HELO sa ID-em svog računala
4. dobiva odgovor 250 sa ID-em primateljevog računala
5. pošiljatelj šalje svoju e-adresu
6. dobiva odgovor 250 OK
7. pošiljatelj šalje primateljevu web adresu
8. dobiva odgovor 250 OK
9. pošiljatelj šalje podatke
10. Dobiva odgovor 354 End data
11. pošiljatelj šalje poruku
12. dobiva odgovor 250 OK
13. pošiljatelj šalje QUIT
14. Dobiva odgovor 221 Bye

Problemi SMTP-a -> nema sigurnosne mehanizme, nema autentifikacije, podrazumijeva se povjerenje i suradnja

Moguća rješenja -> provjera IP adrese klijenta, ograničena uporaba nekih naredbi, ograničena uporaba naredbi za pristup do korisničkih adresa, provjera valjanosti podataka u zaglavljima, ograničenje veličine poruke, ograničenje broja poruka u zadanom vremenu, …

Autentifikacija korisnika -> npr POP-before-SMTP ili SMTP-after-POP
-> poruke se mogu slati tek nakon dokaza da ih se može i preuzeti

Mail Relay -> prima samo poštu od lokalnih korisnika za vanjske korisnike, od vanjskih korisnika za lokalne korisnike i od lokalnih korisnika za lokalne korisnike

S/MIME -> sigurnosno proširenje standarda MIME
-> nije ograničeno na e-poštu
-> nudi šifriranje i digitalni potpis

MIME -> potreban zbog ograničenja SMTP-a
-> omogućuje korištenje svih znakova, definira strukture poruka i vrste poruka
-> jedini zahtjev je da klijent mora biti kompatibilan sa standardom
-> nova zaglavlja -> MIME-Version, Content-Type, Content-Transfer-Encoding, Content-ID, Content-Description

Multipart -> omogućuje da se u tijelu jedne poruke šalje više MIME entiteta

Content-Transfer-Encoding -> kodiranje sadržaja prilikom prijenosa

Cryptographic Message Syntax -> standard za prijenos šifriranih poruka
-> temeljen na sintaksi standarda RSA Security
-> upravljanje ključeva i certifikata

enveloped-data -> šifrirani sadržaj bilo kojeg tipa i šifrirani ključevi za jednog ili više korisnika

-> stvara se jednokratni ključ za šifriranje, i taj ključ se šifrira za svakog primatelja njegovim javnim ključem

-> sve potrebne informacije se pohrane u RecipientInfo

-> sadržaj se šifrira jednokratnim ključem za šifriranje

-> vrijednosti RecipientInfo za sve primatelje se prikupe i uz šifrirani sadržaj postave u vrijednost EnvelopedData

signed-data -> sadržaj bilo kojeg tipa + jedan ili više digitalnih potpisa

-> digitalni potpis se formira potpisivanjem sažetka poruke i šifriranjem tog sažetka privatnim ključem pošiljatelja

-> sadržaj i sažeci se kodiraju prema base64 u vrijednost SignedData

-> funkcija osigurava autentičnost, cjelovitost i neporecivost

-> korisnik mora podržavati S/MIME

clear-signed-data -> isto digitalni potpis

-> samo sažeci se kodiraju prema base64

-> korisnik koji ne podržava S/MIME može čitati, ali ne može verificirati potpis

Kriptografski algoritmi kod S/MIME -> hash: SHA-1 i obavezno podržavati MD5

-> digitalni potpisi: DSS i RSA

-> šifriranje temp ključeva: ElGamal i RSA

-> šifriranje poruka: 3DES, itd.

Certifikati -> korisnici moraju nabaviti certifikate prije uporabe

-> class 1 certifikat dokazuje da je pošta došla s adrese navedene u polju From, no ne dokazuje identitet korisnika

-> class 2 identificira i verificira korisnika

S/MIME problemi -> šifrira s kraja na kraj pa malware u poruci može proći nezapaženo

-> traži certificiranje što nije svima praktično

-> mogući napad je prijava pod tuđim imenom, korištenje jednog certifikata a potpisivanje drugog korisnika, krivotvorenje zaglavlja poruke

Pretty Good Privacy -> nudi autentifikaciju, povjerljivost, sažimanje, kompatibilnost s infrastrukturom e-pošte te segmentacija i ponovno slaganje poruke

-> sažimanje se događa nakon digitalnog potpisa, a obavlja se prije šifriranja jer otežava kriptoanalizu i korisno je kad se napadi temelje na frekvenciji pojave slova

-> kompatibilnost s infrastrukturom

-> DSS/SHA ili RSA/SHA za digitalni potpis

-> AES, 3DES, itd za simetrično šifriranje

-> Diffie-Hellman ili RSA za asimetrično šifriranje

-> sažimanje = ZIP

-> kompatibilnost = Radix-64

Upravljanje ključevima -> nema središnjeg autoriteta već pojedinci jedni drugima potpisuju ključeve te se takvi certifikati pohranjuju s ključevima na "privjesku"
-> PGP izračunava razinu povjerenja za svaki ključ na "privjesku"

Zbog jednostavnosti, kasnije verzije PGP-a podržavaju certifikate prema standardu X.509

Sender Policy Framework -> u DNS se dodaju IP adrese mail poslužitelja koji smiju slati e-poštu u ime određene domene, te primatelj provjerava DNS SPF zapise i prima poštu samo ako zapis postoji

DomainKeys Identified Mail -> potpisivanje FROM: polja, ostalo opcionalno

Domain-based Message Authentication, Reporting & Conformance
-> pravila koja utvrđuju što raditi s porukom koja ne prolazi SPF/DKIM
-> none (ignoriraj), quarantine (šalji u spam), reject (javi mail poslužitelju da ne prolazi provjeru)

Signalizacija

Odvojeni kanali za signalizaciju i promet u telekomunikacijskim mrežama

Danas najkorišteniji protokol je Common Channel Signaling System no. 7 **(SS7)**

SIGTRAN -> omogućuje korištenje SS7 u mrežama temeljenim na IP-u

Stream Control Transmission Protocol -> protokol transportnog sloja, udp paketi

Arhitektura SS7 -> Signal Switching Pointovi (SSP) i Signal Transfer Pointovi (STP)

Napadi u SS7 -> krađa IMSI (International Mobile Subscriber Identity)
-> Napadač može očitati Temporary IMSI te onda tražiti IMSI koji odgovara TMSI
-> otkrivanje lokacije korisnika
-> praćenje lokacije korisnika
-> SRR -> dolazi poziv/SMS -> gdje je korisnik
-> Paging -> s obzirom da mreža zna uvijek gdje je korisnik, paging poruke ga pozivaju i traže

-> Prisluškivanje dolaznih i odlaznih poziva bez obzira na napadačevu

lokaciju u mreži -> efektivno MITM napad jer napadač na telekomunikacijsku mrežu šalje svoju adresu kao adresu žrtve, te onda pozive prosljeđuje žrtvi, ali ih i prisluškuje

-> presretanje SMS-a -> napadač na MSC ili VLR zatraži promjenu lokacije u ime žrtve
-> šalje MAP poruku Update Location na žrtvin HLR
-> svi SMSovi stižu napadaču

-> lažiranje USSD zahtjeva -> napadač se lažno predstavlja kao žrtva i traži nadoplatu, kod, ili neku transakciju, a nakon pokretanja transakcije presreće SMS namijenjen žrtvi tako da žrtva nije ni svjesna

-> uskraćivanje usluge