----------1----------
ranjivost - slabost u izvedbi kako bi se
izazvala steta (malware, hoax, mreze)

prijetnja - skup okolnosti za izazivanje stete
(cilj (osoba); metoda(prijevara); vrsta:()

napad - iskoristaqvanje ranjivosti
nadzor - mjere predstoznosti

sigurnost - sposobnost sustava da se odupre
neocekivanim dogadajima

----------2 Podatkovni (Ehternet) ----------
zamijenjen ARP, nema autentifikacije,
staticki se prepisuju dinamickim,
ARP Spoofing --> NDP Spoofing
SEND = NDP + kriptografska zastita
CGA = uredaj RSA kljuceva, zastita od
NDP spoofinga
nedostaci = hrpa kriptografskih operacija,
cuvanje puno stanja, UNIX

R/STP = razapinjuce stablo, BPDU podatkovne
jedinice, cilj --> ostvariti topologiju s najjacim
preklopnicima
faze = root brige, root ports, designated ports,
stanja pristupa (onemogucen, blokirajuci,
osluskuje, ucenje, prosljeduje)
napad = namjerna modifikacija (uskracivanje,
preusmjeravanje), izvrsenje napada (na linuxu
postoji STP)
problem za napadaca = velika kolicina prometa

----------3 Wifi ----------
Radius = mrezni protokol za centralizirani AAA
(authentication, authorization, accounting) ,
model server/client (UDP), backend za autentifikaciju
= korisnik salje NAS serveru zahtijev za pristup
koristenjem svojih vjerodajnica
= NAS i Radius se stiti IPSec tunelom
= koristi sheme PAP, CHAP, EAP
= verificira se identitet korisnika, adresa, broj
telefona, stanje racuna
= NAS salje Radiusu Access Request (
username/password, dodatno podaci o korisniku
(mrezna adresa, broj telefona))
<-- Radius odgovara (access reject, access
challege (pin, token, kartica), access accept

= RADIUSaaS (Radius as Service) - jednostavna
i sigurna autentifikacija, provjera opozvanih certifikata
= Diameter (podrska za TCP, SCTP), zastita na
transportnom sloju TLS/IPsec

----------5----------
Napad na TCP; na putu kojim prolaze TCP
segmenti on path(zasitta IPsec); van puta
kojim prolaze TCP segmenti off path
(pogadanje parametara)

RST napad --> prekine vezu tako da
pogodi src i dst ip i port, fin slicno <--obrana
{ogranicenje max velicine prozora, dodatni
ack segment}
FIN napad --> slican RSTu, zatvara se
pojedini kraj veze
zastite od RST i FIN napada --> TCP MD5/AO
, ogranicenje velicine prozora

SYN flood --> server primi SYN i rezervira
resurse --> ogranicen broj poluotvorenih veza
i tako se moze zagusiti promet

napad : nema potpune zastite,
--> metode zastite : povecanje broja ,
skracanje trajanja, smanjenje kolicine stanja
poluotvorenih veza (syn cache, syn cookie)
--> amplificirani napad -serveru se salje syn
segment s laznom adresom
ICMP napad --> poruke o greskama uzrokuju
prekid veze, port ili protokol nedostizni
<--rjesenje {IPsec, TLS}

----------6 TLS----------
Klijent-Server, clientHello -->, <--(ServerHello,
Certificate, [CertificateRequest], ServerHelloDone)
--> (Certificate, ClientKeyExchange, [CertificateVerify]
ChangeCiipherSpec, Finished); <-- (ChaangeCipherSpec
FInished)

----------6 Cert ----------
Standardi i preporuke --> ASN (serijalizirati na jedinstven
nacin), ITU (BER, CER, DER), BER(format kodiranja
apstraknih informacija, CER, DER), DER (jedan nacin
kodiranja ASN), CER (razlika od DERa po duljini podataka)

PKCS (public key standard) --> #12 format datoteke za
pohranu X.509 uz javni X.509 certifikat
CMS --> sluzi za potpisivanje, sazimanje, autentifikaciju ili
sifriranje bilo kojeg oblika digitalnih podataka