SIGURNOST INFORMACIJSKIH SISTEMA

1. Uvod u informacijsku sigurnost

Ne postoji 100% siguran sistem.
Firewall ne znači da smo sigurni.
Sigurnost je proces, a ne krajnje stanje. Dakle, mi svojim naporima, resursima, znanjem, ulaganjem težimo da imamo što sigurniji sistem. Koliko uložimo napora i znanja imamo toliko osiguran sistem. To je direktno proporcionalno.
Sigurnost informacijskih sistema se sastoji od dvije glavne komponente: *Računarska sigurnost* (fokusirana na hardver i djelomično softver. Kako da se u široj slici osigura sigurnost) i *informacijska sigurnost* (fokusirana na zaštitu podataka. Kako da u slici jednog sistema se fokusiramo da zaštitimo konkretne podatke?).
Cilj sigurnosti je prije svega da se izgradi sistem koji je otporan na maliciozna ponašanja, a maliciozno je nešto što je štetno. Također se fokusiraju na namjerne ili slučajne propuste, a akcenat je na namjerne.
Da bi se postigla sigurnost koriste se alati, procesi i metode.
Malicioznost u IT-u : Prevare/krađe, Špijunaža, Sabotaže, Spam, Ilegalne aktivnosti, Vandalizam, Elektronski rat (Warfare).
Informacijska sigurnost je bitna među: Poslovnom okruženju, Medicinskim institucijama, Strateška infrastruktura, Vojne instalacije, Kućanstva, Cloud okruženja, IoT, Smart Cities, Društvo (eSociety) u cjelini.
Elementi informacijske sigurnosti su :
Confidentiality (Povjerljivost) – Kriptografija ; prevencija neautorizovanog čitanja informacija.
Integrity (Integritet) – Kriptografija; detekcija neautorizovanog pisanja informacija.
Availability (Dostupnost) – Kontinuitet poslovanja; Podaci trebaju biti dostupni kada su potrebni.

Stavke povjerljivosti : Data protection (moji podaci samo meni), Anonimnost/untracebility (da nas se ne može pratiti; VPN servisi, THOR), Unlinkability (da se određeni proces ne može vezati za korisnika direktno, pa se koriste GUID i cookies da to osiguraju), Pseudonymity (da smo online pod nekim nickame za koji samo mi znamo koga predstavlja; bez anonimnosti ovo nema smisla), Unobservability (da budemo totalni izolovani iz sistema.

Stavke integriteta i dostupnosti : Authenticity, Non -repudiation (da se tačno zna sa koje lokacije je nešto došlo), Audit (osigurava logiranje svih aktivnosti korisnika do tih detalja da se može svaka akcija rekonstruisati), Intrusion detection (mehanizam vještačke inteligencije, zaključuje da li se neko ponašanje korisnika u sistemu tretira kao sumnjivo ili ne), Rollback (vraćanje na prijašnje stanje, rekonstrukcija bilo koje stanja u sistemu nakon što je došlo do promjene)

2. Sigurnosni protokoli

Protokol je niz vrlo jasnih i precizno definisanih koraka koji definišu pravila i ponašanje unutar nekog sistema. Vodič kako se ponašamo u nekom okruženju. Protokol nije nešto što je usko vezano za IT ali se tu mnogo koristi.

Sigurnosni protokol je niz koraka koji osigurava zaštitu infomracijskih resursa. Tu se uglavnom misli na to kako da osiguramo podatke. Sigurnosni protokoli su vezani za komunikaciju, mada to nije pravilo. Većina implementacija je vezana za mrežu.
Postoje razni problemi na koje je potrebno obratiti pažnju. Teško je predvidjeti sve moguće scenarije u implementaciji i dizajnu protokola, tj. Kada se pravi neki protokol mi ne vidimo budućnost ne vidimo šta dolazi, i mi na osnovu iskustava pravimo dizajn protokola. Stvari koje nisu vidljive u fazi izrade se ne mogu ugraditi. Problem se obično vidi u trenutku kada je nastao, znači greške i propusti se teško mogu primjetiti. Implementacija protokola je kompleksna. Zavisi mnogo od softvera i hardvera. Veliki broj sigurnostnih problema je nastao zbog greške u protokolu i potrebno je konstantno vršiti monitoring i raditi provjere. Open source zajednica je vrlo dobro rješenje.

IFF protokol – Identify Friend or Foe (Prijatelj ili Uljez)
IFF propust – MIG in the Middle (Na pola puta)

Idealan protokol bi trebao da ima 4 stavke:

- Sveobuhvatan – da svi zahtjevi budu ispunjeni i što bolje definisani
- Efikasan – da bude minimalan footprint, minimalni zahtjevi po pitanju mrežnog prometa i procesiranja pojedinih dijelova
- Robustan – da je otporan na napade i izmjene u sistemu
- Jednostavan – da je lagan za implementaciju, korištenje, nadogradnju, prilagođavanje i fleksibilan.

Teško je u potpunosti zadovoljiti sve navedene elemente.

Komponente sigurnosnih protokola u IT : *Kontrola pristupa, Enkripcija, Upravljanje ključevima, Integritet sadržaja*

Kontrola pristupa (Access Control) je autentifikacija i autorizacija. Autentifikacija je provjera identiteta korisnika, servisa, resursa (Ko si ti i da li si zaista to ti?). Autorizacija je provjera prava pristupa.
Enkripcija je kombinacija različitih metoda, algoritama, alata, gdje se nešto iz čitljivog pretvara u nečitljivo i obrnuto (dekripcija). Glavnu stvar igra ključ u kombinaciji sa algoritmom koji radi enkripciju. Kriptografija se sastoji od dva osnovna tipa: *Simetrična* (koristi jedan ključ za šifrovanje i dešifrovanje) i *Asimetrična* (imamo dva ključa, jedan za šifrovanje, jedan za dešifrovanje).
Stenografija je skrivanje sadržaja.

Upravljanje ključevima je proces koji je usko vezan za kriptografiju. Rješava problem distribucije ključeva između učesnika u komunikaciji. Skoro svaki sigurnosni protokol u IT ima ovu komponentu. Obično se osigurava kombinacijom simetrične i/ili asimetrične enkripcije.

Integritet sadržaja je jako bitan u komunikaciji. Da li je došlo do promjene izvornog sadržaja?, Da li komuniciramo sa pravom osobom?, Ko je garant komunikacije?
Napadi: Man in the middle, ARP poisoning, Session hijacking.

TCP/IP je osnova današnje komunikacije na internetu. Nastao je jako davno i nije predvidio mnogo toga i predstavljao je polaznu tačku za mnogo sigurnosnih problema.
SSH je kreiranje sigurne komunikacije između nas i servera. Primjenjuje kriptografiju u nesigurnim mrežnim okruženjima. Primarno je konzolni interfejs. Zamjena za Telnet.
SFTP je najpoznatiji protokol za razmjenu fajlova. Tradicionalni FTP nije siguran jer je u clear tekst formatu i jer su fajlovi vidljivi u transportu i na serveru. SFTP rješava ove probleme primjenom kriptografije.
TLS/SSL protokol koji omogućava sigurnu komunikaciju. SSL je stara verzija, a TLS je njegov nasljednik. Zasniva se na asimetričnoj enkripciji. (https://)
IPSec/PPTP- ova dva protokola se koriste za uspostavu VPN saobraćaja. VPN omogućuje proširenje internih LAN mreža preko interneta. Kreira enkriptovani tunel između dvije tačke u komunikaciji. Danas se VPN korisni za anonimno surfanje internetom.

3. Kontrola pristupa

...implementacija protokola na konkretnim situacijama. U osnovi se sastoji iz Autentifikacije (Ko si ti i da li si to zaista ti) i Autorizacije (Šta smiješ da radiš).

Postoji više načina Autentifikacije, a neke od njih su : čovjek prema računaru (programu) i računar – računar.
Kontrola pristupa se još posmatra kao metoda prikupljanja elemenata digitalnog dokaza o aktivnostima korisnika.

Autentifikacija

Da li si to zaista ti? Kako da program to zna? Ako se neko prijavi kao ja, to nisam zaista ja i u tim trenucima se javljaju stvari koje nisu konzistentne. Da bi se osiguralo da li smo to zaista mi, postoje sljedeće metode/tehnike, koje u kombinaciji podižu sigurnost sistema:

1. Nešto što samo mi znamo – lozinka
2. Nešto što samo mi imamo – smartcard, token, generator vrijednosti
3. Nešto što nas predstavlja – otisak prsta, iris scanner

Nešto što samo mi znamo

Lozinka je najčešći elemenat za sigurnost. Obično lozinke sadržavaju naš JMBG, važne datume iz života, kućne ljubimce i slično, što nije najbolja praksa.
Problema sa lozinkama ima jako puno. Sve lozinke ispod 8 karaktera su nesigurne, to je minimum, te što je veća sa kombinacijom brojeva, slova, znakova to je lozinka bolja.

Nešto što samo mi imamo

Uređaj ili predmet u našem posjedu.

Nešto što nas predstavlja

U ovo spada biometrija : Otisak prsta, Svojeručni potpis, Prepoznavanje lica, Prepoznavanja glasa, Prepoznavanje kretanja.

Biometrija u autentifikaciji

Biometrija je mnogo sigurnija zamjena za lozinke. Ovo je postao standard u sigurnosti. Međutim ova tehnologija još nije dostigla vrhunac.
Idealna biometrija treba da bude univerzalna, tj primjenjiva na svakoga, međutim to nije tako. Ne možemo biti sigurni da bude različita, tj. da nema duplikata (npr. Jednojajčani blizanci), da je stalna, tj. da su osobine atributa onog ašto se provjerava da se ne mijenja tokom vremena, da je lako prikupljiva, da bude sigurna.
Biometrija radi na principu Identifikacije i Autentifikacije.
Identifikacija je komparacija one-to-many (npr. Baza podataka otisaka prstiju).
Autentifikacija je komparacije one-to-one (npr. Laptop sa skenerom prsta)
Postoje određene greške u biometriji. **Stopa prevare vs. Stopa uvrede** (Prevara – trudy je autentificirana (pogrešno) kao Alisa, a Uvreda (Alisa nije autentificirana kao Alisa)). U biometriji, smanjenje jedne strane vodi ka porastu suprotne.
99% prepoznavanje govora -> mala prevara, velika uvreda
30% prepoznavanja govora -> velika prevara, mala uvreda

Biometriju je teško falsifikovati. Bolja od lozinke. Često pogriješi. Upotreba limitirana na uređaju specijalne namjene.

Autorizacija

Šta smiješ da radiš?
Nakon što smo dokazali da smo to zaista mi, ide lista permisija. Odnosi se na akcije autentificiranih korisnika.
Kroz matricu prava pristupa se definiše skup subjekata, skup objekata, skup privilegija i ona opisuje kontrolu pristupa na pojedine subjekte.

Nivoi autorizacije su preuzeti iz US Deparment of Defense (DoD) i koristi 4 nivoa:

- TOP SECRET
- SECRET
- CONDIFENTIAL
- UNCLASSIFIED

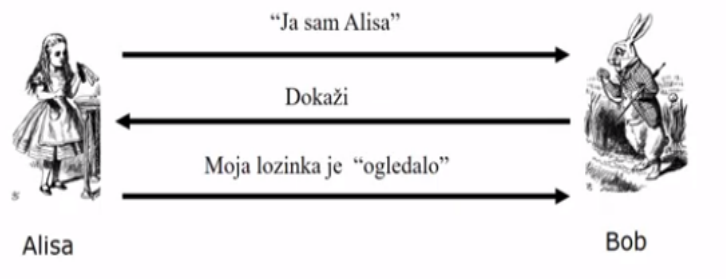
Svako u svom okruženju treba da podijeli poslovne procese na ove kategorije.

Case study (Autentifikacijski protokol)

Kako greške u autentifikaciji mogu dovesti do nekih napada i kako ih korigujemo?

Alisa treba da dokaže svoj identitet Bobu, međutim oni mogu biti ljudi i/ili računari. Može biti i mutual, da Bob mora da dokaže ko je on. Problemi su razni, autentifikacija na stand-alone računare je relativno jednostavna, međutim, danas rijetko ćemo naći situaciju da se logiramo negdje što je offline. Obično je to nešto što je mrežno i samim time napadač može svašta da uradi.

Jednostavna autentifikacija



Ovo je u konceptu, jednostavno i efikasno. Međutim, jako je problematično, i ovo važi samo ako je računar offline. Jedino tada je ovo sigurno. U mreži je podložno replay napadu (da neko „čuje" podatke i samo ih ponovi tako što se predstavi kao ti)

Malo bolja autentifikacija

Hashovana lozinka (Hash je jednosmjerna funkcija koja uzima varijabilni ulaz i daje fiksni izlaz). Cilj je da se lozinka ne vidi kada putuje mrežom, ali je ovo meta ponavljanja.

Challenge – Response

Ponavljanje se može spriječiti upotrebom challenge-response metode. Extra sloj u sigurnosti i treba da obezbijedi još nešto pored lozinke, što se svaki put mijenja. Kako svaki put? To je **Nonce** (number used once), dakle informacija koja se koristi samo jednom. Poznato kao one-time password generatori. To je recimo token uređaj koji svaki put generiše random 8 cifara. I samim time kada u hashu ide lozinka i NONCE, svaki put je hash drugačiji, tako da onaj koji prati komunikaciju, neće moći da uradi replay napad.

4. Kriptografija I

...jedan dio puno veće oblasti koja se naziva kriptologija. To je naučna disciplina kreiranja i razbijanja „tajnih kodova", gdje je kriptografija ustvari kreiranje istih, a kriptoanaliza razbijanje.

Cipher (šifra) ili cryptosystem (kriptosistem) se koriste za encrypt (enkriptovanje) plaintext-a (otvorenog texta). Rezultat ovog šifrovanja je ciphertext (šifrovani tekst). Obrnuti proces je decrypt (dekriptovanje) šifrovanog teksta.

Key (ključ) se koristi za konfigurisanje kriptosistema. Postoje dva osnovna tipa kriptosistema:

Kriptosistem sa Symmetric key (simetrični ključ) gdje se koristi isti ključ za enkriptovanje/dekriptovanje

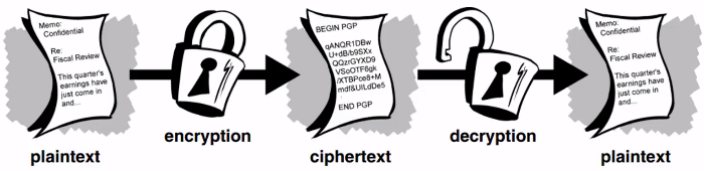
Kriptosistem sa Public key (javni ključ) za enkriptovanje, i private key (privatni ključ) za dekriptovanje.

Osnovni kripto principi su sljedeći :

- Sistem je potpuno poznat napadaču
- Samo je ključ tajan
- Kripto algoritam nije tajan

- Poznato još kao Kerckhoff-ov princip (sistem kao sistem ne treba da predstavlja tajnost, jer u slučaju da sistem bude otuđen, to ne bi trebalo da bude smetnja)

Iskustvo je pokazalo da su tajni algoritmi imali mnogo slabih tačaka. Prva od njih je što svi misle da je bio tajan, ali tajni algoritam nikada nije dugo ostao tajan.
Otvorenost? Prije će se pronaći slabost i ispraviti. Ovdje se koristi **RSA**. Kako on pravi ključ nije tajno ali sastojci ključa su tajni.
Osnovni model:



Cezarova šifra je radila tako što alfabet je bio pomjeren za tri mjesta udesno. Međutim to ne mora biti samo 3, već može biti n. Ako govorimo o engleskoj abecedi može ići do 25.

Napadač zna da je korištena metoda jednostavne zamjene, znamo da je ključ n, ali ne znamo koji n (on zavisi od jezika jer nema svaki jezik isti broj slova), kako pronaći ključ?
Ako je engleski, onda imamo 26 kombinacija i testirati ih sve. Bosanski jezik ima 30 opcija.
Ako to nije jednostavna zamjena, nego bilo koja permutacija slova, tada imamo 26 !>2^88 mogućih ključeva.
Postoji mali backdoor, gdje posmatranjem šifrovanih tekstova, može se primjetiti frekvencija korištenja slova.
Kriptosistem je siguran ako je najbolji mogući napad kombinacija svih mogućih opcija – Brute force.
Kriptosistem nije siguran ako postoji bilo koji napad zaobilaznim putem – Backdoor.

One – Time pad enkripcija
Pad je ključ koji ima isto slova ili više koliko i originalna poruka.
Gubi se frekvencija ponavljanja.
Različit ključ u one time padu može da da više smislenih informacija koje stvaraju konfuziju.
Ova enkripcija je sigurna ali samo ako se pad koristi jednom i slučajno. Ako koristimo svaki put isti pad može se pronaći pattern i to biti osnova za razbijanje.
Metoda dvostruke transpozicije, x koristimo da popunimo prazan prostor. Miješamo redoslijed redova i kolona, mijenja se položaj matrice. Ključ nije neki broj ili pad, sada je ključ matrica koja će omogućiti da se šifra vrati u izvorni oblik.

Venona je najpoznatiji primjer enkripcije u historiji koja je koristila metodu one time pad.
Šifrovanje putem knjige kodova je drugi primjer. Korištena knjiga kodiranih riječi (predefined) npr Zimmermanov telegram.

Kriptografija poslije WWII
Claude Shannon – otac nauke o informacijskoj teoriji
Digitalizacija – mnogo podataka za zaštititi
Data Encryption Standard (DES)
Public Key priptografija
CRYPTO konferencije
Advanced Encryption Standard (AES)

5. Kriptografija II

Sve je moguće, samo je potrebno mnogo resursa i vremena. Računski je „nemoguće“ jer za neka probijanja ključa bi bilo potrebno vremena više nego procijenjena starost svemira.

Enkripcijski ključevi su zasnovani na slučajnim generatorima bita. Oni su važni, prisutni i neophodni u svim modernim kriptografskim algoritmima. Cilj je da se pronađe **seed** vrijednost koji postaje osnova

za pronalazak ključa i to treba da bude netrivijalan zadatak. Primjeri: Poseban hardver, Korisnička aktivnost, Aktivnost hardvera, Šum iz analogno/digitalnih konvertora, Sadržaj i vrijeme protoka mrežnih paketa, vremenska komponenta.
Sve ovo su pseudo generatori slučajnih vrijednosti.

Hash funkcija je također jedan od temelja kriptografije ali NIJE enkripcija. Zato što kada se nešto hešuje ne postoji reverzni proces. On služi za provjeru integriteta podataka, sadržaja, itd.
Uvijek uzima varijabilni ulaz i daje fiksni izlaz. U kriptografiji se koriste sigurne hash funkcije koje obezbjeđuju jednosmjernost i otpornost na izmjene. Neki od primjera su MD5 i SHA. U MD5 su pronađene kolizije gdje dva različita ulaza daju isti izlaz i to je bilo problem, to bi značilo da ako se desi kolizija da dvije različite lozinke daju isti izlaz i samim time se narušava autentifikacija i autorizacija. Nakon toga on se mijenja sa MD6 i dolaze SHA1 i SHA2.

Simetrična kriptografija koristi stream cipher i block cipher.
Jedan od najpoznatijih primjera kriptografije sa jednim ključem u historiji je *DES Data Encryption* Standard. On nije algoritam, on je standard. Zasnovan je na Lucifer block šifri. Reduciran na 56 bita. Nasljednici: triple DES, G-DES, DES-X, LOKI89, ICE
DES je šifra sa:
64 bitnom dužinom blokova
56 bitnom dužinom ključa
16 ciklusa ponavljanja
48 bita od ključa se koristi u svakom ciklusu (subkey)
Ključ dužine 56 bita je vrlo slab, pa je došlo do potrebe za osnaživanjem DES-a. Kao rezultat toga nastao je *Triple DES* (3DES) sa dužinom od 112 bita.

AES Advanced Encryption Standard nije algoritam, nego napredni oblik enkripcije koji je nastao kao zamjena za DES. Osnova za ovu enkripciju je Rain Doll algoritam. Veličina bloka mu je 128 bita, a dužina ključa 128,192 ili 256 bita.

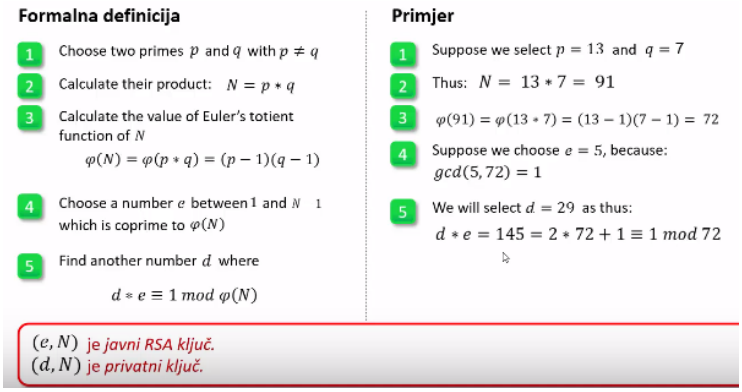
Asimetrična enkripcija radi na principu kriptografije javnog ključa. Problem jednog ključa je razmjena i cilj je postići sigurniji način komunikacije.
Implementacija javnog ključa je nastala kroz **RSA algoritam**. To je najpoznatiji i najjači oblik kriptografije javnim ključem. Zasnovan je na faktorizaciji velikih prim brojeva, da nađemo koja dva broja kada se pomnože daju izlaz. Javni i privatni ključ su par velikih, od 100 do 200 cifrenih, prostih brojeva. RSA koristi brojeve od najmanje 300 cifara i to je skoro neprobojno.
On je potpuno baziran na matematici, koristi 3 jednostavne stvari ali osnova je prim broj :

1. Modul operator
2. Euler – totientova funkcija
3. Euler – Fermatt teorema

Kako radi generisanje ključeva od strane RSA algoritma?

1. Biramo p i q gdje p nije jednako q
2. Radimo p*q i to je N (N=p*q)
3. Eulerova funkcija od broja N
4. Biramo e iz skupa od 1 do N-1, koji je ustvari koprim broj Eulerove funkcije od N
5. Biramo d, d*e = modul operator eulorove funkcije od N

Odavde e je javni RSA ključ, a d je privatni ključ.



Jedan od najvećih problema je protokol za razmjenu ključeva, jer se ključevi nekada u letu mogu kompromitovati. *Diffie-Hellmanov protokol* rješava ovaj problem. HTTPS enkripcije koristi ovaj protokol da se ključevi razmjene. On generiše kriptovani kanal između dvije tačke i tako kreće razmjena ključeva.

Upotreba: Enkripcija fajlova, enkripcija diskova, enkripcija email poruka, HTTPS, chat enkripcija (end2end), tor itd.

6. Mrežna i sistemska sigurnost

Sigurnost sistema se u većini sitacija posmatra kao admin password, i time bi počela i završila priča o sigurnosti. Međutim to je daleko od istine, i to je puno više od toga. Ovo je samo jedna od komponenti ovog segmeta. Sigurnost OS-a zavisi od OS-a, tipa korisnika, tipa baze, servisa itd.
Sam OS se posmatra kao sistemska sigurnost, a sve ostalo što dolazi povrh OS-a, spada u aplikativnu sigurnost. Znači, sistemska sigurnost se odnosi na OS u cjelini bez aplikativnog sloja koji može da ugrozi sistem.

Postoje određene klase OS-a koje nam govore koje je tržište koja je upotreba i gdje je namjenjen taj OS:

- Klasa D – minimalna zaštita (MS DOS, Windows 95,98)
- Klasa C1 – Diskretna zaštita (UNIX)
- Klasa C2 – Kontrolisana zaštita pristupa (UNIX, Linux, Windows NT, 2000, XP, 7, 8, 10)
- Klasa B1 – Uključuje elemente povjerljivosti
- Klasa B2 i B3 – Strukturna i hijerarhijska zaštita sa elementima uzbinjivanja
- Klasa A1 – Vrhunski sistemi (uglavnom vojna rješenja i rela time sistemi gdje se radi o ljudskim životima)

TCB (Trusted Computing Base) je platforma kojoj se vjeruje, na koju se oslanja sve kasnije što dolazi u samom računaru ili sistemu. To je Hardver + Firmware + Softver (Dijelovi navedenih elemenata namijenjenih održavanju sigurnosne politike).
TPM čip je čip za enkripciju i ubrzava je i poboljšava, te je uslov za sigurnost.

Šta je to mrežna sigurnost?
To je odvojena komponenta, van sistema.

Bitno je reći da je mreža zbog svoje obimnosti i rasprostanjenosti korištenja, postala pogodno tlo za testiranje svih malicioznih operacija. Sa druge strane, protokoli na kojima počiva mreža su sigurno pisani ad-hoc, i ostala su mjesta gdje se možda nešto može provući. Sve su učestaliji napadi Dos i Ddos.

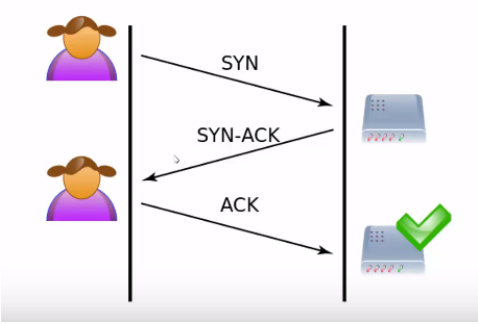
Svaka mreža se bazira uglavnom na TCP/IP protokolu, a samim time ta sigurnost nije na pravom nivou. On nije pisan sa sigurnošću na umu na početku svog nastajanja, tako da su svi elementi urađeni da

zadovolje formu ali suština nije onakva kakva se očekuje. Tako da su mogući različiti napadi: adress spoofing, gubitak izvorne rute, krađa sesija, SYN flooding itd.
Zato je potrebno ovaj protokol „pokrpiti“ različitim servisima npr Firewall.
Firewall može biti hardverski i softverski, i razdvaja LAN i WAN. Firewall nije sigurnost. On po svojoj prirodi mora otvoriti neke tačke koje su potrebne, a svaka ta tačka predstavlja ulaznu osnovu. On je potreban uslov, ali nije dovoljan.
Njegova osnovna namjena jeste da filtrira i nadgleda saobraćaj, pakete, provjerava destinaciju i izvor, logiranje/auditing/alarmiranje i na osnovu toga reaguje.
Problemi su mala ili nikakva zaštita, otežavanje poslovnih procesa, implementacija novih servisa.

Zašto dolazi do mrežnih napada?

Osnovni princip jeste da se uskrate mrežne usluge i servisi. Nekada, ovi napadi imaju neki cilj u pozadini, krađu ili šijunažu, ili možda neki politički razlozi.
Glavni krivac za ove napade je čovjek i njegova naivnost i neznanje, također protokoli koji su loše dizajnirani i implementirani, kao i tehnologija i njeni propusti u softverskim i hardverskim komponentama.
Konkretni napadi:
Dos/DdoS su ista stvar, samo što kod DoS -a sa tačke A napadam tačku B, a DdoS sa više tačaka napad na jednu tačku.
SYN Flooding, ARP Poisoning i Smurfing su sve varijante ovih napada.
Jedini način za odbranu je gašenje rute, gašenje servisa, zvanje nadprovidera.

SYN Flooding je napad koji iskorištava ranjivost TCP/IP-a. Radi se o onome SYN-ACK.



Ovdje je problem kada napadač konstantno traži SYN, ruter kaže ACK a napadač to ignoriše. Ovo je tipični DoS napad gdje preplavljujemo buffer, rutera, switcha i oborimo mrežni servis. Odbrana je *SYN Cookies* koji ne da jednom klijentu da više puta šalje više zahtjeva u jednom periodu, kao i Timeframe limit.

ARP Poisinonig omogućava da se osoba lažno predstavi. Napadač se predstavi kao neko drugi, putem switcha napadač je spoofao adresu tog usera, dakle mapirao je svu MAC adresu, tako da sav promet ide preko napadača i on ga dalje prosljeđuje. Ovoga se jako lako riješiti tako što se uradi IP2MAC maping koji mapira tačno na switchu taj MAC i taj IP i ne postoji mogućnost spoofanja. Također, postoje softveri koji detektuju to vrstu napada, i OS konfiguracija gdje možemo da spriječimo promjenu IP adrese u mreži.

Smurfing je preteća svih DoS i DdoS napada. Ovo je ICMP echo request issue koji je omogućavao da napadač preko svojih zombija radi ping neke stranice i preplavljuje buffer da server padne i pojavi se blue screen of death.