V osnovi imamo dva elementa varnosti: - [[Šifriranje]] / Zakrivanje (Vsebine) - [[Celovitost]] / Integrity (Vsebina se ne sme oz. more spremeniti, če pa se je to zelo lahko odkriti)

Varovanje Omrežne Plasti

Torej če uporabljamo tako celovitost, kot šifriranje se pač lahko znebimo napadalnih vektorjev hkrati, tedve komponenti sodelujeta v harmoniji: Napadalec tako lahko podatke samo še **podvaja ali pa zavrže**, *vpogleda nima več zaradi šifriranje in spremeniti jih ne more zaradi celovitosti*.

Prvi tak protokol, ki si ga bomo ogledali za omogočanje bodisi celovitost bodisi šifriranje bodisi oboje je [[IPsec]]. Zanimivijo je, da protokolni sklad deluje tako, ko vplivamo na IP protokol, vplivamo posredno tudi na vse ostale protokole in podatke, ki se preko njega prenašajo. Torej če zaščitimo IP plast oz. protokol, potem ščitimo tudi tiste, ki se po njem prenašajo: - TCP - UDP - ICMP - OSPF - ....

IPsec ponuja grajenje VPN omrežji, Virtual Private Network. Posledica tega VPN-ja je, da kljub temu da vse naprave, ki v njem sodelujejo, vidijo drug drugega, kot v istem LAN-u, so te lahko geografsko narazen tudi po več tisoč kilometrov, prav tako je med njimi lahko celoten internet.

![[Pasted image 20230111192051.png]] Pri tem VPN-ju imamo lahko torej: - device-to-device - device-to-network - network-to-network Dejansko so vsi VPN-ju device-to-device saj jih vzpostavimo na vstopnih točkah omrežij, vendar če pogledamo na malce višjem logičnem nivoju potem lahko več naprav komunicira preko te, ki je povezana, temu network-to-network...

Takemu tunelu se reče tudi IP tunel ali VPN tunel, skozi katerega potuje IPsec promet. Ta implementira dva protokola varovanja:

- **Authentication Header**, ki zagotavlja avtentikacijo izvora in celovitosti podatkov
- **Encapsulation Security Payload**, ki pa zagotavlja avtentikacijo izvora, celovitost *in* zaupnost podatkov

> To zagotovi z digitalnim podpisom paketa. Nad podatki naredimo kriptografsko hash funkcijo, naredimo operacijo z zasebnim ključem in podatke ki jih dobimo so digitalni podpis, ki ga pripnemo paketni glavi.

Prvo je potrebno, če gre za simetrično šifriranje, da imasta obe strani komunikacije isti ključ, tako lahko preverita celovitost podatkov. Hkrati morata obe strani imeti iste parametre šifriranja, katera vrsta šifriranja je uporabljena (DES, 3DES, AES...), ter za katero hash funkcijo gre.

Ker je IP oz. IPsec promet enosmeren, moramo vzpostaviti nekaj, kar združuje promet iz enega vira na en ponor, temu pravimo **Security association**. Ta SA hrani podatke o enosmerni povezavi, kar pomeni da za n povezav potrebno vzpostaviti 2n SA-jev.

SA je opisan v **Security Association Database**, kjer se hranijo podatki o: - 32-bitnem ID-ju SA-ja, imenovan **Security Parameter Index** - Izvorni in ponorni IP SA-ja - Vrsta šifriranja in kljul - Vrsta preverjanja celovitosti in hash funkcija (CMAC-SHA1, HMAC-MD5) - Ključ za avtentikacijo

Ker IPsec ponuja dva protokola za zaščito, se je potrebno odločiti katerega se bo uporabljalo in za kaj. To določa **Security Policy Database**. Ta določa ali naj se datagram ščiti glede na izvorni IP, ponorni IP in tip protokola. Določa kateri SA naj se uporabi ter ***kaj narediti*** z datagramom/segmentom in ***kako*** to narediti.

Seveda pa moramo SAD tudi vzpostaviti, kar pomeni da med dvema entitetama moramo pošiljati občutljive podatke. Temu je bil izumljen in služi protokol [[IKE]].

Varovanje Višjih Plasti

[[SSL]] je protokol, ki zagotavlja to varovanje oz. sedaj novejši TLS. Tako SSL igra nekakšno plast varnosti med aplikacijo in TCP plast: ![[Pasted image 20230111212426.png]] Razlika tukaj na transportni plati namesto na omrežni plasti, je da imamo povezavni način prenosa, *za prenos se vzpostavi povezava*. Torej moramo delati z tokom bajtov in ne običajnimi sporočili. Ključi se bodo morali spreminjati per-session basis, za eno sejo pa imamo množico ključev, to je: - Ključ za šifriranje od A do B in še enega za obratno smer (2 ključa) - Ključ za podpisovanje sporočila od A do B in še enega za obratno smer (2 ključa)

Povezave

- [[Operativna Varnost]]