## Krüpto rakendamine võrguturbes

- Ülevaade
- SSL, TLS
- SSH
- Meili signeerimine ja krüptimine
  - MIME krüptoraamistik
  - PGP
- Virtuaalsed privaatvõrgud
  - IPSec





## Krüptimine — konfidentsiaalsuse tagamiseks

- SSL/TLS — senine *de facto* standard
- SSH — konkurent SSL-le
- IPSec — standard IP tasemele
- PGP — (meili) krüptimine ja signeerimine
- S/MIME — MIME lisandused krüptimiseks ja signeerimiseks
- Kerberos
- Secure RPC
- . . .





## SSL, TLS

- SSL — *Secure Sockets Layer*
- Kiht TCP ja rakenduste vahel, loob TCP laadse "toru"
- Toru sees saab rääkida muid protokolle (HTTP, LDAP, IMAP, POP3, telnet, . . . )
- Toru kumbagi otsa saab autentida sertifikaadi abil
- Torus liikuvad andmed krüptitakse
- Torus liikuvad andmed võib ka pakkida (RLE, zlib)
- TLS (*Transport Layer Security*) — SSLv3-st arenenud IETF standard





## SSH

- SSH — *Secure SHell*
- Samuti TCP ja rakenduse vahel
- Osapoolte vahel on krüptitud ja võibolla ka pakitud sisuga toru
- Serverit autenditakse avaliku võtme järgi
- Klienti võib autentida kliendi võtme abil, kliendimasina võtme abil või parooli abil (interaktiivselt)
- SSH ühenduse sisse tekitatakse mitu virtuaalset kanalit (näiteks teine toru X jaoks)
- On olemas mähkurid mitmete varasemate käskude turvaliseks asendamiseks

## SSL protokollist

- Kumbki saadab oma versiooninumbri ja toetatud šifrite nimekirja
- Server saadab oma serdi (ja küsib kliendi serti, kui soovib)
- Klient autendib serverit sertifikaadi järgi (veebi puhul kontrollib ka serdi seest domeeninime)
- Klient arvutab peamise võtme senise info järgi
- Klient saadab serverile selle võtme (krüptituna serveri avaliku võtmega)
- Kliendi autentimise puhul saadab klient ka oma serdi ja ühe tüki signeeritud andmeid ja server kontrollib neid
- Peamisest võtmest genereeritakse vahetatavad sessioonivõtmed
- Kumbki osapool kinnitab teisele, et hakkab genereeritud võtmete abil andmeid vahetama; andmevahetus võib alata





## Meili signeerimine ja krüptimine — MIME

- S/MIME — *Secure/Multipurpose Internet Mail Extensions*
- MIME tüüpide ja reeglite komplekt signeerimise ja krüptimise lisamiseks
- MIME jaoks on defineeritud üldine signeerimise ja krüptimise raamistik (tüübid `multipart/signed` ja `multipart/encrypted`)
- S/MIME defineerib rakenduse sellele raamistikule: `application/pkcs7-signature` formaat signatuuride jaoks ja `application/pkcs7-mime` muude vajaduste jaoks
- Need tüübid sisaldavad CMS (*Cryptographic Message Syntax*) objekte (seotud X.509 infrastruktuuriga)





## Meili signeerimine ja krüptimine — PGP

- PGP jaoks on seni kasutatud 3 formaati:
  - PGP oma päised kirja tekstikehas
  - MIME tüübiga `application/pgp` komponent kirja kehaks — halvasti käideldav
  - MIME krüptoraamistikus formaadid `application/pgp-signature`, `application/pgp-encrypted`, `application/pgp-keys`





## VPN — virtuaalsed privaatvõrgud

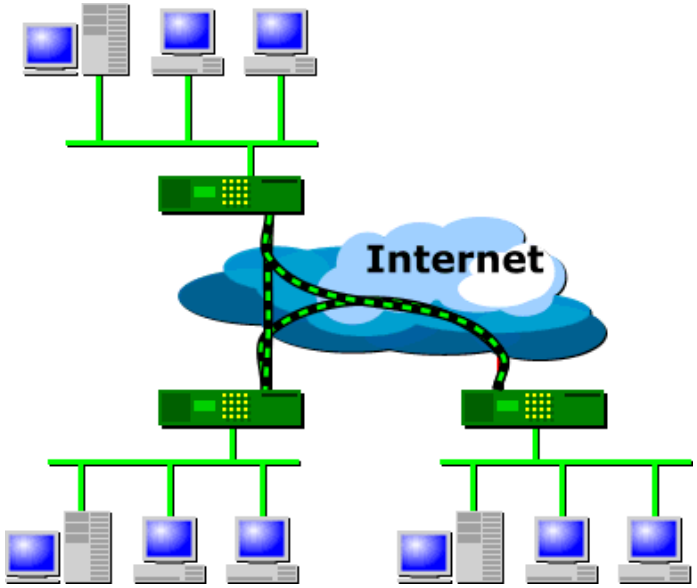
VPN idee: teeme üle Interneti krüptitud tunnelid oma kahe või enama võrgu vahel

- Tihti odavam kui eraldi ühendus osakondade vahel
- Internet on tänapäeval niikuinii olemas
- Võrreldes eriliiniga puudub siin reeglina garanteeritud ribalaius
- Tihti summaarselt lihtsam kui iga vajalikku teenust eraldi turvata

Mitu taset:

- Palju kohtvõrke kokku
- Üksikud (mobiilsed) kaugtöökohad väljaspool firma võrke
- Extranet — turvalised kanalid partneritega

## VPN loogiline skeem








## VPN tehnoloogiline külg

- Üldine idee: krüptitakse IP paketid ära ja kapseldatakse saadud andmekogum uuesti mingisse paketti (harilikult IP või UDP).
- Alguses oli igal tegijal oma protokollistik
- IPSec — algselt IPv6 lisavõimalus, kuid jõudis juurutamisse ka IPv4 ajal. Praeguse aja *de facto* formaat erinevate süsteemide vahel IP pakettide krüptimiseks.
- IPSec lubab suvalisel hostide või ruuterite paaril omavahel krüptitult (ESP) ja/või autenditult (AH) andmeid vahetada.
- 1999. a. kinnitati ka ametlik võtmevahetuse protokoll IKE (*Internet Key Exchange*) — selle abil saavad kaks masinat, mis teineteisest varem midagi ei teadnud, standardsel meetodil sessioonivõtmed kokku lepitud ja IPSec+IKE laiema leviku järel peaksid seega suvalised masinad olema võimelised omavahel krüptitult suhtlema.





## VPN: muud lahendused

- SKIP (*Simple Key management for Internet Protocols*)
- PPP üle TCP ühenduse (SSH, SSL, . . . )
- PPTP, L2TP
- L2TP + IPSec
- CIPE (*Crypto IP Encapsulation*)
- **OpenVPN**
- . . .