Tietoliikenteen perusteet

Tietoturvasta

Kurose, Ross: Ch 8.1, 8.6, 8.7

Sisältö

Tietoturva-kurssi:
kryptografian perusteet
IPSec

- **Turvavaatimukset**
- **Uhkia**
- **Palomuuri**

Oppimistavoitteet:
- Osata kuvailla tietoliikenteeseen kohdistuvat riskitekijät ja turvallisuusuhat
- Osata selittää, kuinka palomuuri toimii
- Ymmärtää tietoturvasta sen verran, että osaa huolehtia oman koneen turvallisuudesta

Tietoturvasta

Turvavaatimukset

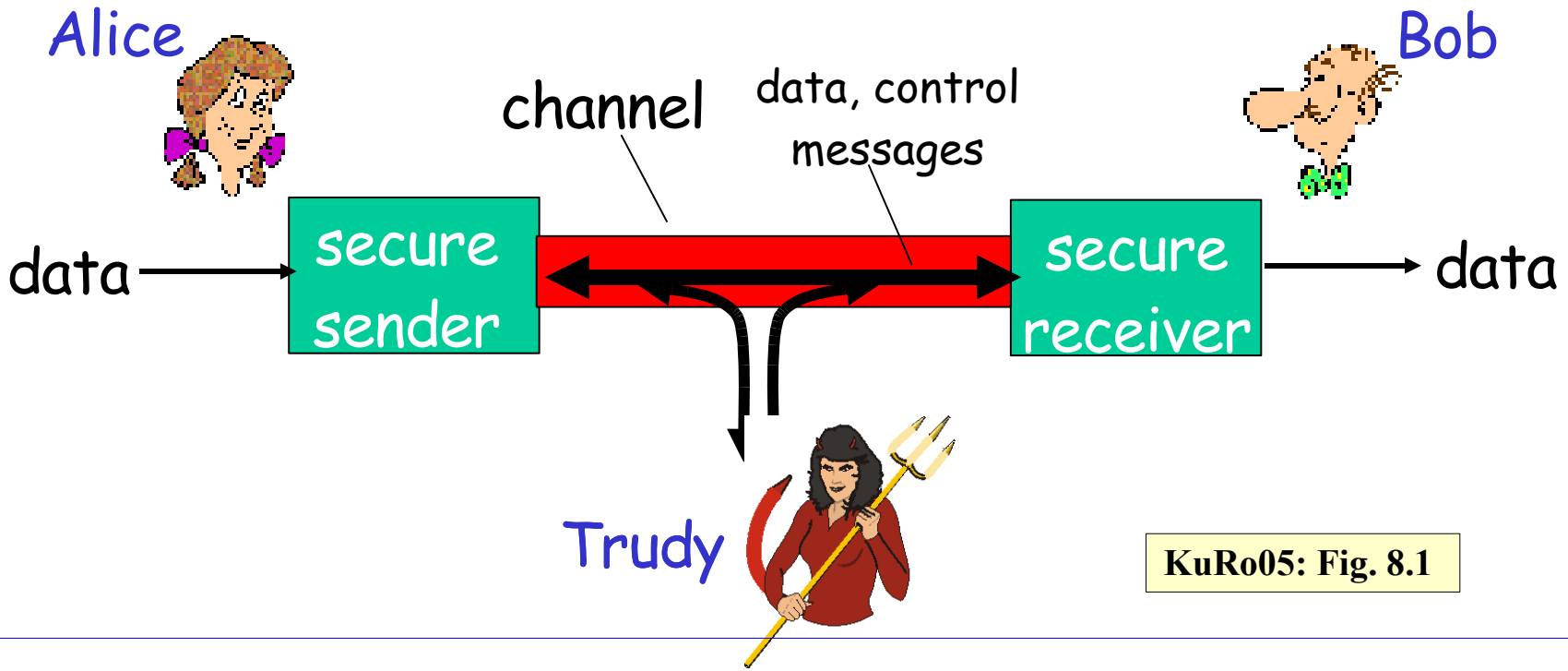
Ch 8.1

Turvavaatimukset

- Luottamuksellisuus (confidential, secrecy)
  - Vain lähettäjä ja vastaanottaja 'ymmärtävät' sanoman sisällön
  - Muu eivät saa välttämättä tietoa edes sen olemassaolosta
  - Salakirjoitus
- Autentikointi (authenticity)
  - Lähettäjä ja vastaanottaja varmistavat toistensa identiteetit
  - Oikeaksi todentaminen, salakirjoitus
- Eheys, koskemattomuus (message integrity)
  - Lähettäjä ja vastaanorraja varmoja siitä, ettei sanomaa ole muutettu (siirron aikana ta myöhemmin)
  - Digitaalinen allekirjoitus
- Pääsynvalvonta (access and availability)
  - Palvelut ovat saatavilla käyttötarkoituksen mukaisesti
  - Vain niilla pääsy, joilla lupa käyttää käyttöoikeuksien mukaisesti
  - Käyttäjätunnus ja salasana, tiedostojen / objektien käyttöoikeudet, ...

Ystävä ja tunkeutuja

- Tuttu asetelma reaalimaailmastakin
  - Bob ja Alice kommunikoivat keskenään (salassa muilta?)
  - Trudy (intruder) voi siepata sanomia: viivästää tuhota, muutella



KuRo05: Fig. 8.1

Kuka Alice, kuka Bob?

- Asiakasprosessi - palvelijaprosessi
  - Ihminen koneen ääressä ja palvelu palvelinkoneessa
- Web-selain ja -palvelija
  - Elektroninen kaupankäynti
  - On-line pankkipalvelu
  - .....
- DNS-kysely ja DNS-palvelu
- Reititystietoja vaihtavat reitittimet
- ....

Tietoturvasta

Uhkia

Ch 8.7

Mitä Trudy puuhii?

- Koputtelee koneen portteja (mapping)
  - Turva-aukkojen löytämiseksi ja koneen valtaamiseksi
- Salakuuntelee (eavesdropping, sniffing)
  - Sieppaa sanoman matkalla ja tutkii sisällön
- Väärentää, “peukaloi”(impersonation, spoofing)
  - Vaihtaa paketin tietoja, esim. IP-osoitteen
- Tehtailee sanomia. “satuilee” (fabrication)
  - Tekee ja lisää liikenteeseen ylimääräisiä sanomia
- Kaappaa yhteyden (hijacking)
  - Vaihtaa oman IP-osoitteen lähettäjän / vastaanottajan tilalle
- Estää palvelun (DoS, Denial of Service)
  - Kuormittaa palvelinta, jotta se ei ehdi palvella oikeita käyttäjiä

Koputtelu ja kartoitus (mapping)

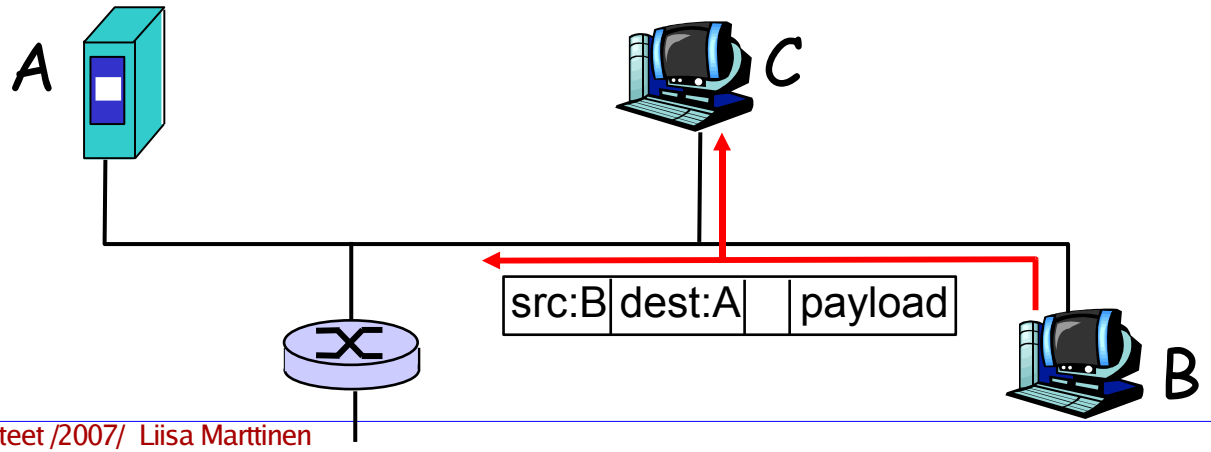
- Kaivelee ensin tietoja
  - IP-osoitteista, käyttöjärjestelmistä, verkko-ohjelmista
- Hyödyntää sitten tunnettuja turva-aukkoja
- Ping

  Lähettää kyselyjä valittuihin verkon IP-osoitteissin

  Hengissä olevat koneet vastaavat
- Porttiselaus (port scanning)
  - Kokeilee systemaattisesti TCP/UDP-yhteyttä koneen portteihin
  - Vastauksista saa selville tarjotut palvelut
  - Onko tunnettuja turva-aukoja?
- www.insecure.org/map/
  - “network exploration and security auditing”

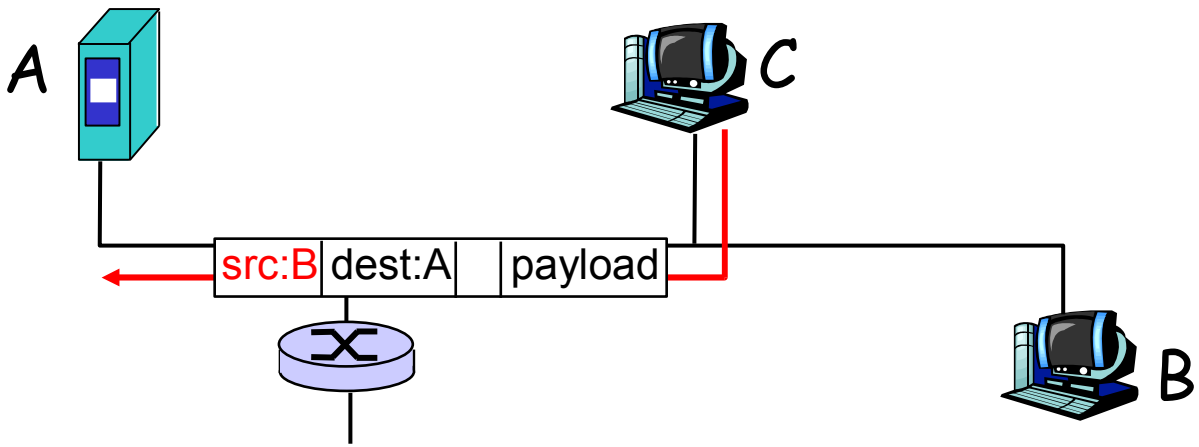
Salakuuntelu (packet sniffing)

- Tutkii linkkikerroksen kehysten sisältöä
  - Yleislähetys: kaikki kuulevat kaikki kehykset
  - Valikoimattomassa moodissa (promiscuou toimiva sovitinkortti myös kopioi kaikki kehykset itselleen
  - Kuuntelevan koneen oltava samassa LAN:ssa
- Ohjelmia, joilla paketit voidaan purkaa tekstimuotoon
  - Hyödyllisiä verkon valvojalle, mutta ...
- Hyökkääjä etsii erityisesti salasanoja
  - Salasanat verkkoon vain salakirjoitettuina
  - Älä käytä telnet:iä etäyhteyksiin, käytä ssh:ta



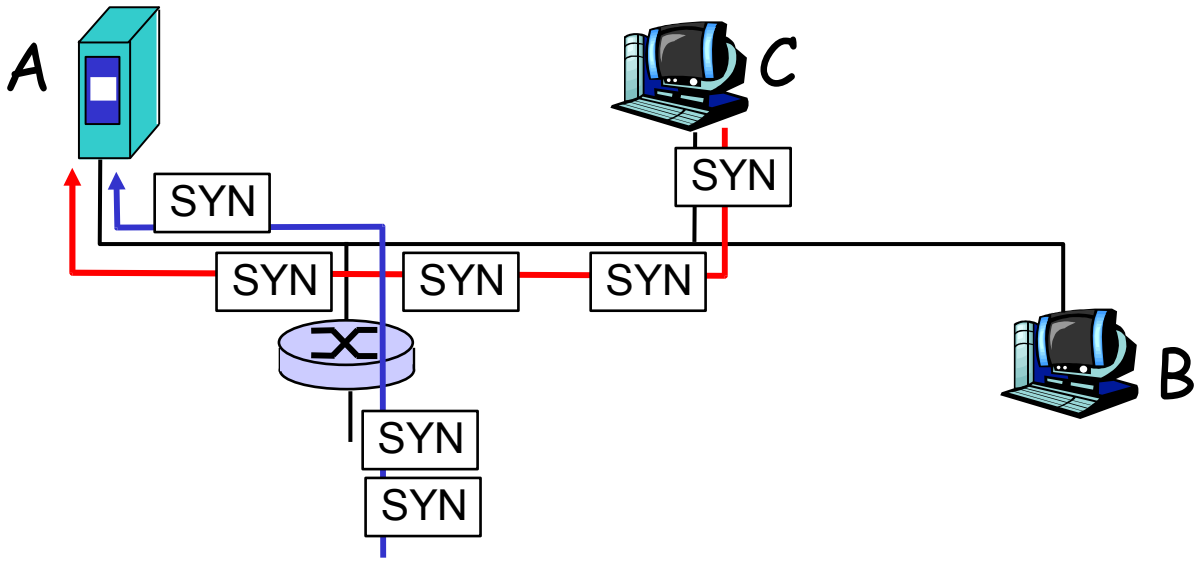
Väärentäminen (spoofing)

- Vastaanottaja ei voi tietää, kuka on todelinen lähettäjä
- Jokainen, joka kontrolloi koneensa ohjelmistoa (erityisesti KJ:tä) voi väärentää mm. IP-osoitteen
  - Sovellus voi tehdä itse IP-paketin ja ohittaa KJ:n pakettia lähettäessä ('raw' mode)



Palvelunestohyökkäys (DoS)

- Kuormittaa palvelua, jotta oikeat käyttäjät eivät pääse lainkaan käyttämään
- SYN-tulvitus
  - Pakottaa uhrin suuriin määriin TCP-yhteydenmuodostuksia
    - Lähettää SYN-segmenttejä, mutta ei ACK-segmenttejä
    - Uhri varaa puskuritilaa, muisti voi loppua
  - Väärentää lähteen IP-osoitteen



Palvelunestohyökkäys (jatkuu)

- IPv4-paloittelu
  - Lähettää runsaasti IP-pakettien osia (M=1), mutta ei lainkaan sitä viimeistä palaa (M=0).
  - Vastaanottaja puskuroi ja jää odottamaan puuttuvia paloja
    - Muisti loppuu
- Smurf-hyökkäys
  - Lähettää suurelle määrälle koneita uhrin IP-osoitteella varustettuja ICMP Echo request -paketteja ja niihin tulevat vastaukset tukkivat uhrin koneen.

Hajautettu DoS-hyökkäys (DDoS)

- Hyökkääjä ottaa ensin haltuun ison joukon koneita niiden omistajien huomaamatta
  - Koputtelee ja löytää turva-aukot
  - Asentaa hyökkäysohjelman, joka vain odottelee käskyä /kellolyömää
- Kaapatut koneet aloittavat samaan aikaan hyökkäyksen uhrin kimppuun
  - Hajautetusti
  - IP-osoitteet peukaloituina

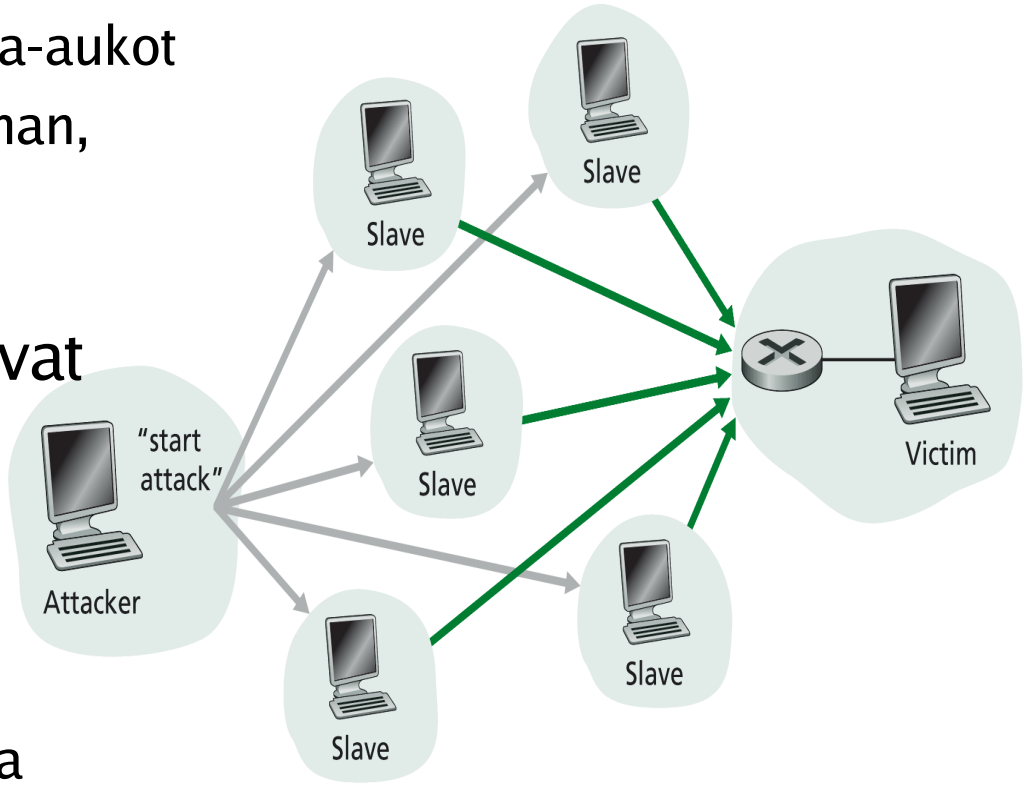
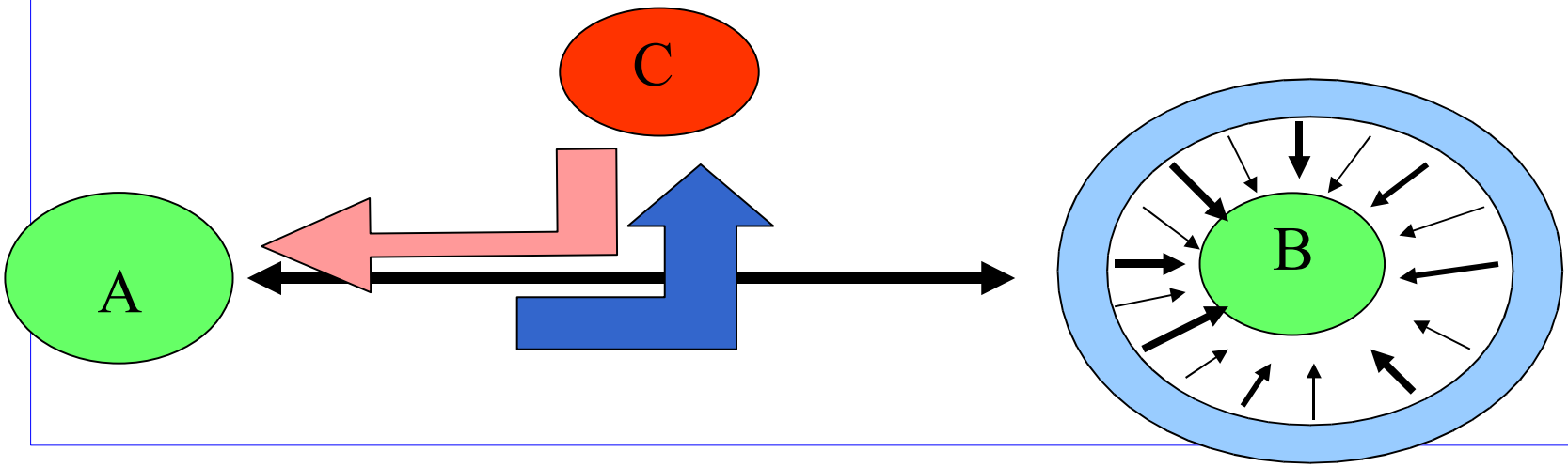


Figure 8.26 ♦ A DDoS attack

Yhteyden kaappaus (hijacking)

- Hyökkääjä C kaappaa itselleen A:n ja B:n välisen yhteyden
  - Kuuntelee ensin yhteyttä ja selvittää mm. Tavunumeroinnin, kuittausnumeroinnin, ikkunan koon, ...
  - Poistaa B:n pelistä palvelunestohyökkäyksellä
  - Tekeytyy itse B:ksi
  - Oltava fyysisesti kytkettynä linkkiin



Vastatoimet?

Pidä KJ:n turvapäivitykset ajan tasalla!

- Koputtelu
  - Käytä palomuuria
  - Seuraa liikennettä, reagoi, jos normaalista poikkeavaa
  - Seuraa aktiviteettia (IP-osoite, porttien koputtelu)
- Salakuuntelu
  - Käytä kaksipisteyhteyksiä Ethernet-kytkin keskittimen sijasta
  - Salakirjoitus
  - Tarkista, ettei verkkokortti ole promiscuous-moodissa
- IP-osoitteen väärentäminen
  - Lähetysverkossa helppo havaita ja estää
  - Yhdyskäytäväreititin voi tarkistaa, että lähettäjän IP-osoite kuuluu lähettävään verkkoon (ingress filtering)
  - Tutkimista ei voi tehdä pakolliseksi
- Palvelunesto
  - Vaikea todeta / estää
  - Miloin SYN on oikeayhteyspyyntö, millloin osa hyökkäystä?

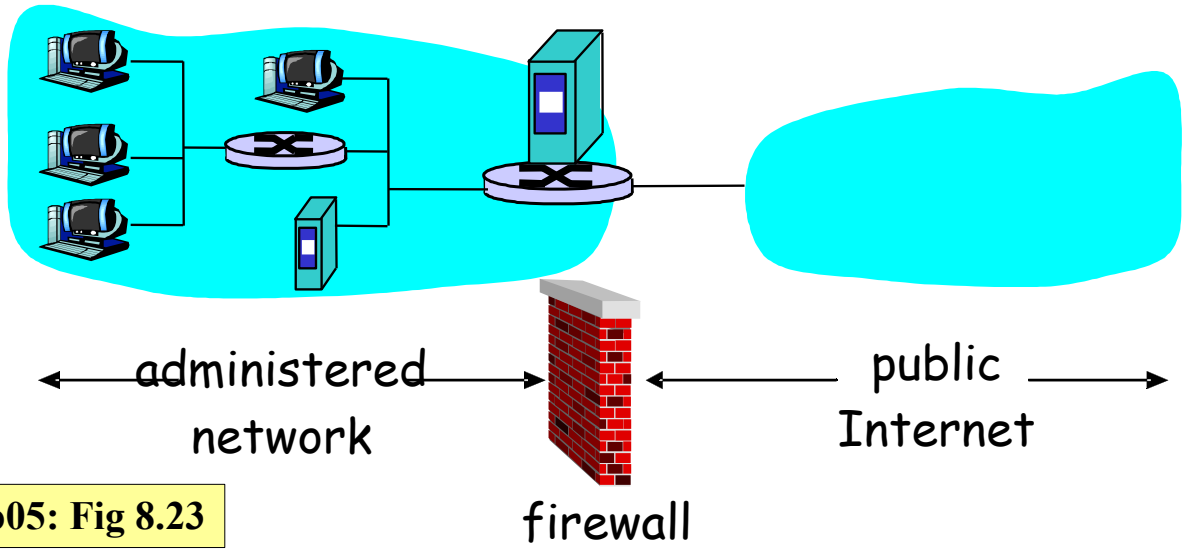
Tietoturvasta

Palomuuri

Ch 8.6

Palomuuri (firewall)

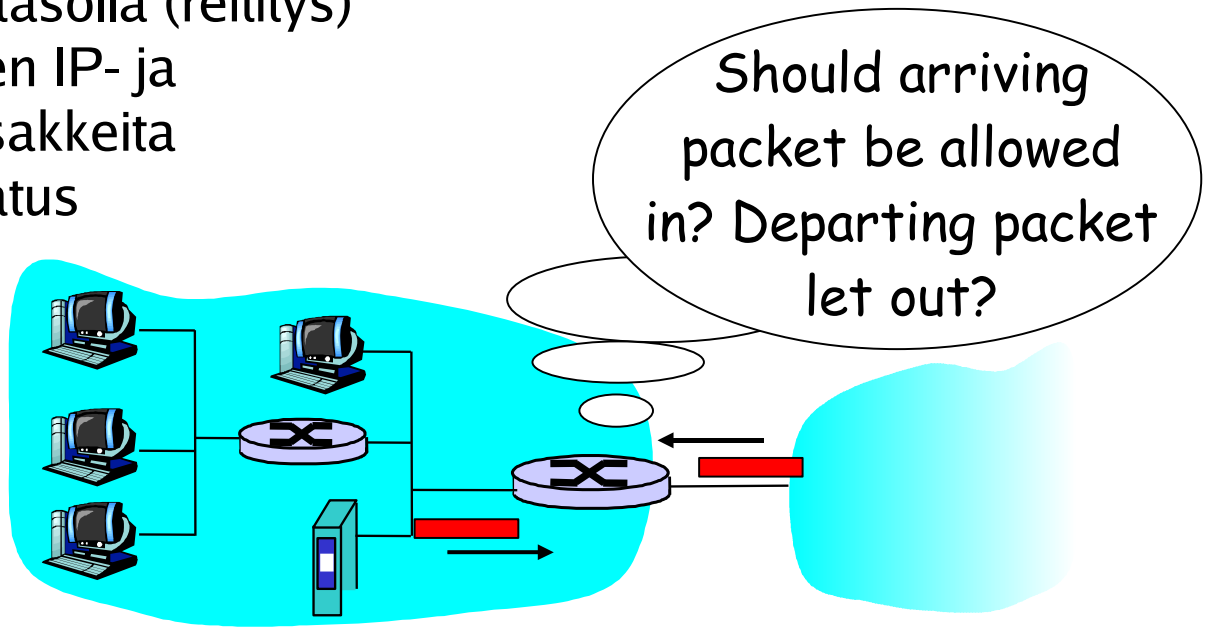
- Ohjelmisto + laitteisto
- Suodattaa (filteroi) liikennettä organisaation oman verkon (intranet) ja julkisen Interbetin välillä
  - Osa IP-paketeista pääsee palomuurin läpi, osa ei



KuRo05: Fig 8.23

Kaksi erilaista palomuuria

- Paketteja suodattava palomuuri (packet filtering firewall)
  - Toimii verkkotasolla (reititys)
  - Tutkii pakettien IP- ja TCP/UDP-otsakkeita
  - Karkea suodatus



- Sovellustason yhdyskäytävä (application-level gateway)
  - Toimii sovelluskerroksella välittäjänä (relay)
  - Tutkii sovellusdataa
  - Hienojakoisempi suodatus

Palomuuri ja suodatus

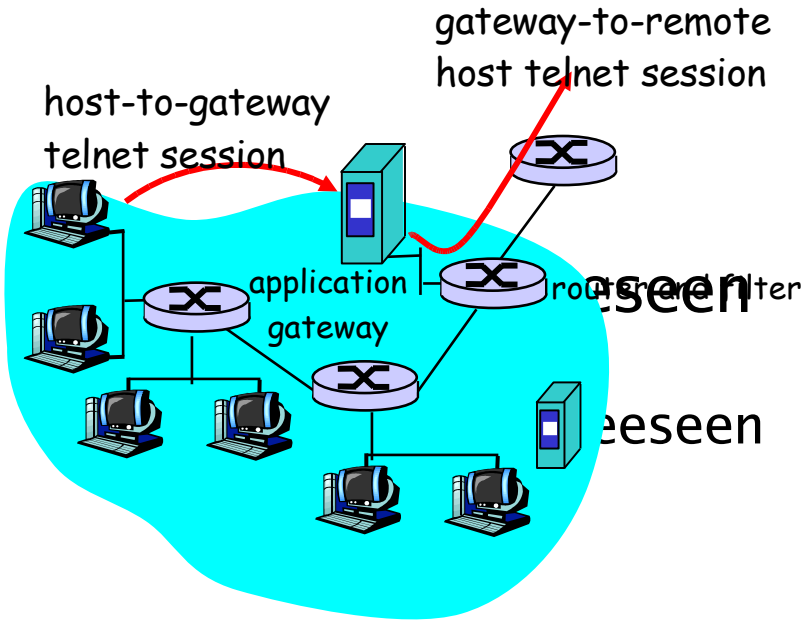
- Ennalta annetut säännöt sodatukselle
  - Salliiko vai kieltääkö paketin etenemisen
- Säännöt otsakekenttien perusteella
  - Lähettäjän ja vastaanottajan IP-osoite
  - TCP- ja UDP-porttinumerot
  - Kontrollisanoman (ICMP) tyyppi
  - TCP:n kättelysegmenttien SYB / ACK-bitit
- Säännöillä on hankala toteuttaa monimutkaisia estopoliitikoita
  - Sääntöjä tarvitaan helposti paljon, jopa tuhansia
  - Niitä käydään läpi jossain järjestyksessä => väärä järjestys voi aiheuttaa ongelmia / virheitä paketin käsittelyssä

Palomuuri ja suodatus (jatkuu)

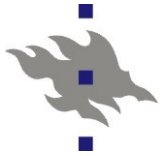
- Esim 1: Estä IP-pakettien liikenne (sisään/ulos), jos protokolla = 17 tai portti = 23
  - Palomuuri hävittää kakki UDP-paketit ja estää telnet-yhteydet
- Esim 2: Estä sellaisten tulevien TCP-pakettien liikenne, joissa ACK = 0
  - Vain ensimmäisessä segmentissä SYN = 1, ACK = 0
  - Palomuuri hävittää kaikki ulkoa tulevat TCP-yhteyspyyntöpaketit
  - Oman verkon koneet voivat silti ottaa yhteyttä organisaation ulkopuolisiin palveluihin
- www.cert.org/tech_tips/packet_filtering.html

Yhdyskäytävä

- Kun halutaan hienojakoisempaa suodatusta
  - Esim. Telnet-yhteyden saalliminen tunnetuille käyttäjille, mutta näiden identiteetti on ensin todettava (autentikointi)
  - Tähän pelkkä IP/TCP/UDP-otsakkeiden tutkiminen ei riitä
- Toimii välittävänä koneena (relay) sisäverkon ja Internetin välissä
  - Eri sovelluksilla oma yhdyskäytäväprosessinsa
  - Esim. IMAP, SMTP, HTTP
- Ulkoa yhteys ensin
  - Autentikoi tarvittaessa
  - Muodostaa yhteyden sisäverkon (palomuuri sallii vain sille)
  - Välittää sanomat sisään/ulos



Kuro05:Fig 8.24



Palomuuri / Yhdyskäytävä

- Yhteyttä haluavan on osattava otta yhteyttä yhdyskäytävään
  - Esim. Web-selaajalle on kerrottava proxy-palvelimen osoite
- Ei auta kaikkiin turvaongelmiin
  - IP-osoitteiden ja porttinumeroiden väärentäminen
  - Yhdyskäytäväohjelmissa voi olla turva-aukkoja
  - Langattomat yhteydet ja soittoyhteydet

Myös hyvin ylläpidetyt järjestelmät kärsivät hyökkäyksistä!

Käytännön ohjeita

Käytä palomuuria
Huolehdi KJ:n päivityksistä
Käytä virustorjuntaa
Hävitä haittaohjelmat

- Uusi kone
  - Älä kytke verkkoon ennenkuin olet ottanut palomuurin käyttöön
  - Päivitä käyttöjärjestelmä heti
- Yliopiston lisenssillä saat koneellesi F-Securen ja Symantecin virustorjunta- ja palomuuriohjelmat
  - https://www.helsinki.fi/atk/ohjelmajakelu/
- Muitakin ilmaisia ohjelmia löytyy
- Lue lisää esim. “Jokakodin tietoturvaopas”
  - www.tietoturvaopas.fi Ja www.tietoturvakoulu.fi

Kertauskysymyksiä

- Mitä ominaisuuksia halutaan turvalliselta yhteydeltä?
- Millaisia uhkia verkkoihin (koneisiin, tietoliikenteeseen ja palveluihin) kohdistuu?
- Miten eri uhkiin pyritään varautumaan?
- Mikä on DoS? Entä DdoS?
- Miten palomuuri toimii? Mihin sitä käytetään?