

# Tietoliikenteen perusteet

## Tietoturvasta

Kurose, Ross: Ch 1.6, Ch 8.1, Ch 8.9.1



# Sisältö

Tietoturva-kurssit:  
kryptografian perusteet  
IPSec

- n Turvavaatimukset
- n Uhkia
- n Palomuuuri



## Oppimistavoitteet:

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



# Tietoturvasta

## Turvavaatimukset Ch 8.1

# Turvavaatimukset

## n Luottamuksellisuus (confidential, secrecy)

- n Vain lähettäjä ja vastaanottaja 'ymmärtävät' sanoman sisällön
- n Muu eivät saa välttämättä tietoa edes sen olemassaolosta
  - Salakirjoitus

## n Autentikointi (authentication)

- n Lähettäjä ja vastaanottaja varmistuvat toistensa identiteeteistä
  - Oikeaksi todentaminen, salakirjoitus

## n Eheys, koskemattomuus (message integrity)

- n Lähettäjä ja vastaanottaja varmoja siitä, ettei sanomaa ole muutettu (siirron aikana ta myöhemmin)
  - Digitaalinen allekirjoitus

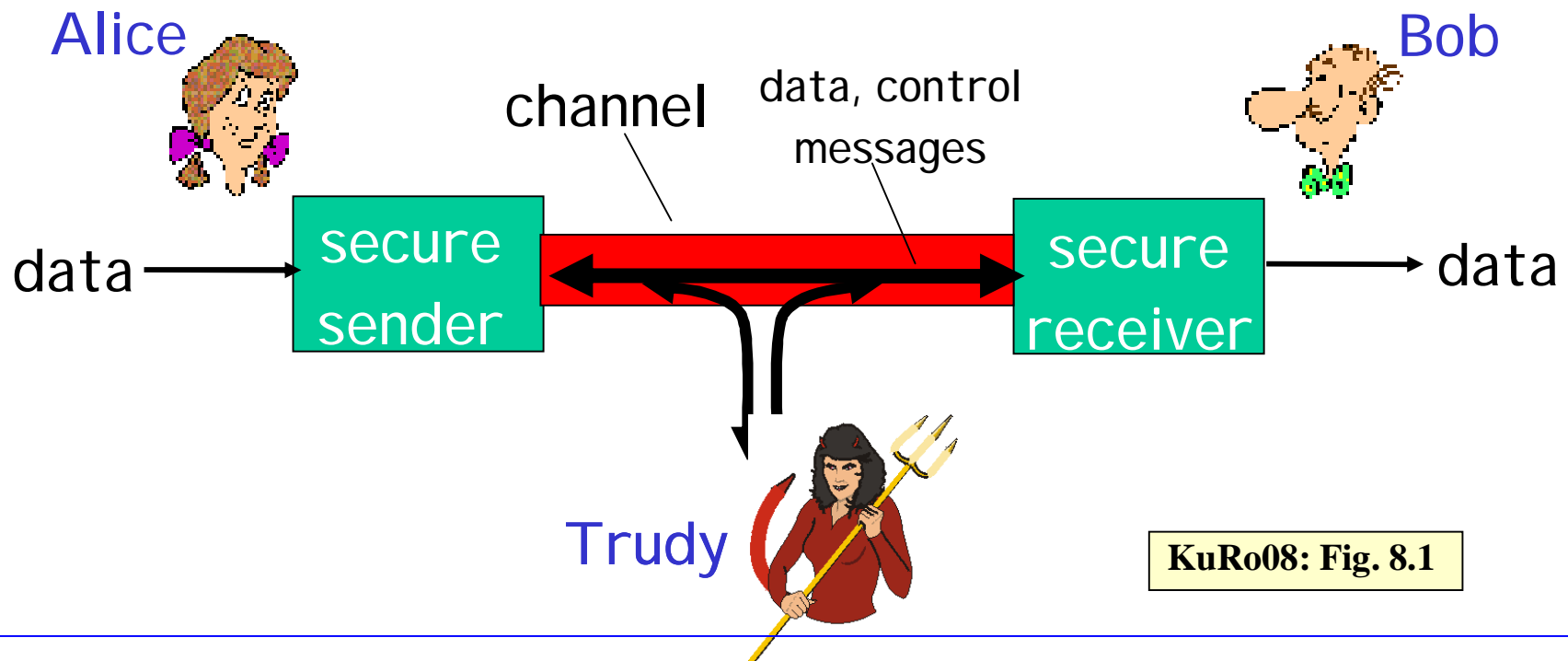
## n Palveluiden saatavuus ja suojaus

- n Palvelut ovat saatavilla käyttötarkoituksen mukaisesti
- n Vain niillä pääsy, joilla lupa käyttää käyttöoikeuksien mukaisesti
  - Käyttäjätunnus ja salasana, tiedostojen / objektien käyttöoikeudet, ...
- n Suojautuminen 'ulkoa' tulevia hyökkäyksiä vastaan (haittaohjelmat, palvelunestohyökkäys) vastaan
  - palomuuuri, havaitsemis- ja puhdistusohjelmat

# ▪ Ystävää ja tunkeutuja

## n Tuttu asetelma reaali maailmasta

- n Bob ja Alice kommunikoivat keskenään (salassa muilta?)
- n Trudy (intruder) voi siepata sanomia: nuuskia, kerätä tietoa
- n Trudy voi muunnella, tuhota ja lisätä sanomia





## Kuka Alice, kuka Bob?

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



# Tietoturvasta

**Uhkia**

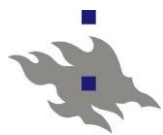
**Ch 1.6**

# Mitä Trudy puuhii?



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





## Koputtelu ja kartoitus (mapping)

### n Kaivelee ensin tietoja

- n IP-osoitteista, käyttöjärjestelmistä, verkko-ohjelmista

### n Hyödyntää sitten tunnettuja turva-aukkoja

### n Ping

Lähetää kyselyjä valittuihin verkon IP-osoitteisiin

Hengissä olevat koneet vastaavat

### n Porttiselaus (port scanning)

- n Kokeilee systemaattisesti TCP/UDP-yhteyttä koneen portteihin

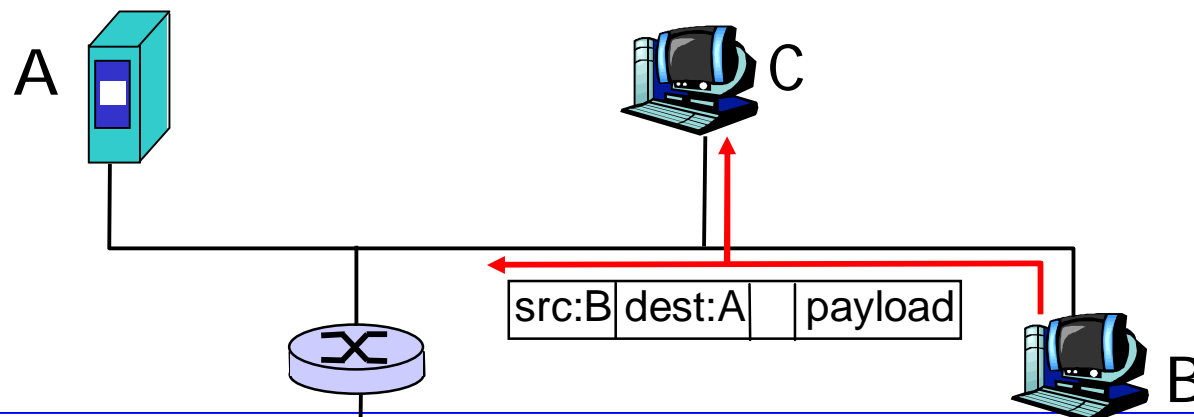
- n Vastauksista saa selville tarjotut palvelut

- n Onko niissä tunnettuja turva-aukkoja?

- Firefox-selain 27.3.08, Facebook 25.3.08, Sampo Pankki, Applen Quicktime Player, FlashPlayer turva-aukkojen paikkausta
- Internet Explorer 7, DNS, BGP, ...
- Linux-päivityksen turva-aukko=>laitoksen salasanojen vaihto

# Salakuuntelu (packet sniffing)

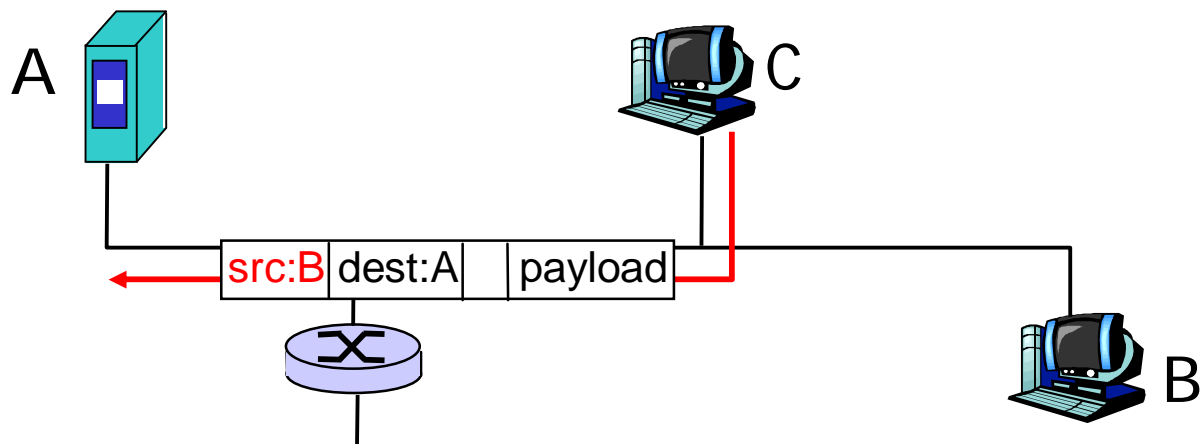
- n Tutkii linkkikerroksen kehysten sisältöä
  - n Yleislähetys: kaikki kuulevat kaikki kehykset
  - n Valikoimattomassa moodissa (promiscuous) toimiva sovitinkortti myös kopioi kaikki kehykset itselleen
  - n Kuuntelevan koneen oltava samassa LAN:ssa
- n Ohjelmia, joilla paketit voidaan purkaa tekstimuotoon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





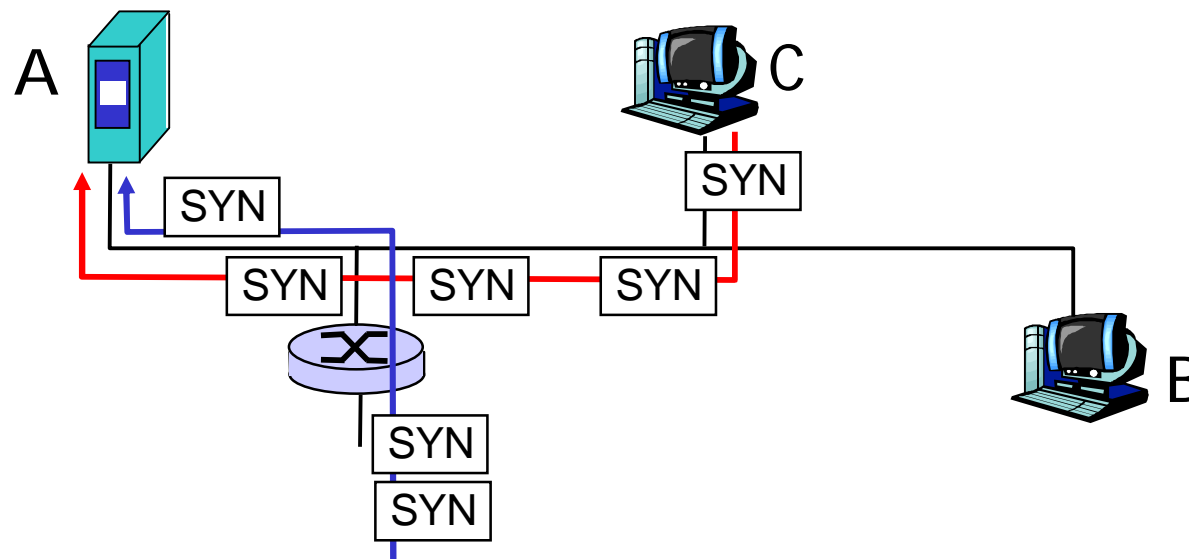
## Väärentäminen (spoofing)

- n Vastaanottaja ei voi tietää, kuka on todellinen lähettäjä
- n Jokainen, joka kontrolloi koneensa ohjelmistoa (erityisesti KJ:tä) voi väärentää mm. IP-osoitteen
  - n 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)

### n IPv4-paloittelu

- n Lähettää runsaasti IP-pakettien osia ( $M=1$ ), mutta ei lainkaan sitä viimeistä palaa ( $M=0$ ).
- n Vastaanottaja puskuroidaan ja jää odottamaan puuttuvia paloja
  - Muisti loppuu

### n Smurf-hyökkäys

- n 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 /kellolyömiä
- Kaapatut koneet aloittavat samaan aikaan hyökkäyksen uhrin kimppuun
  - Hajautetusti
  - IP-osoitteet peukaloituina (harvoin)

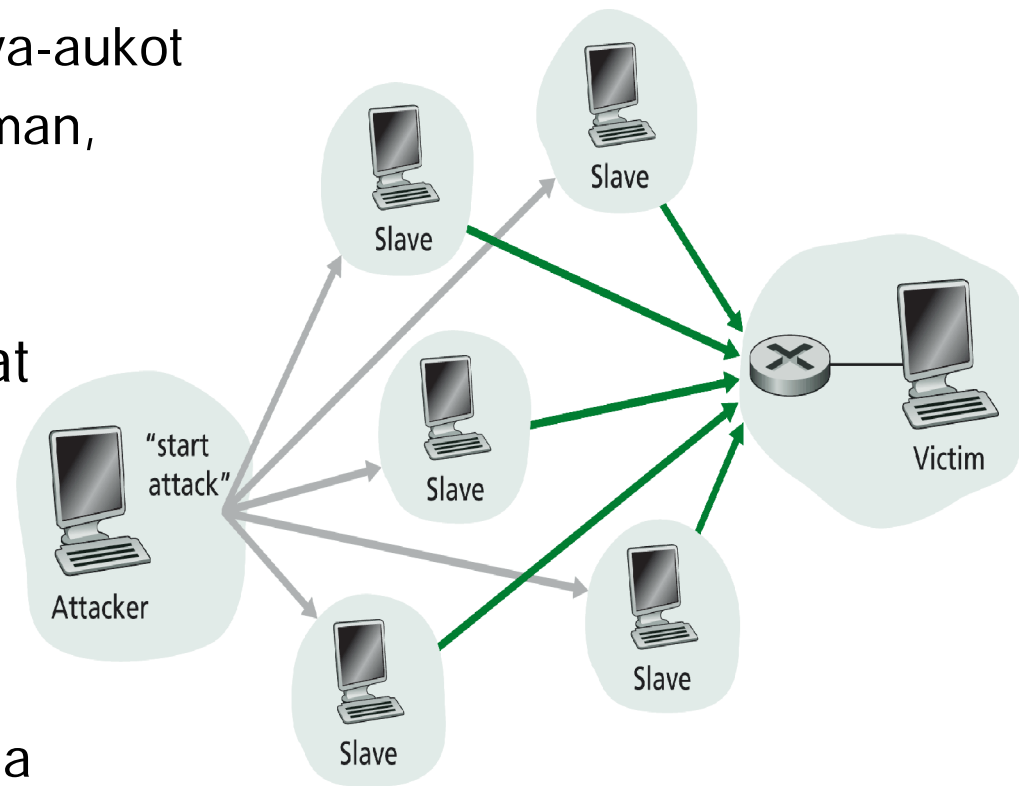
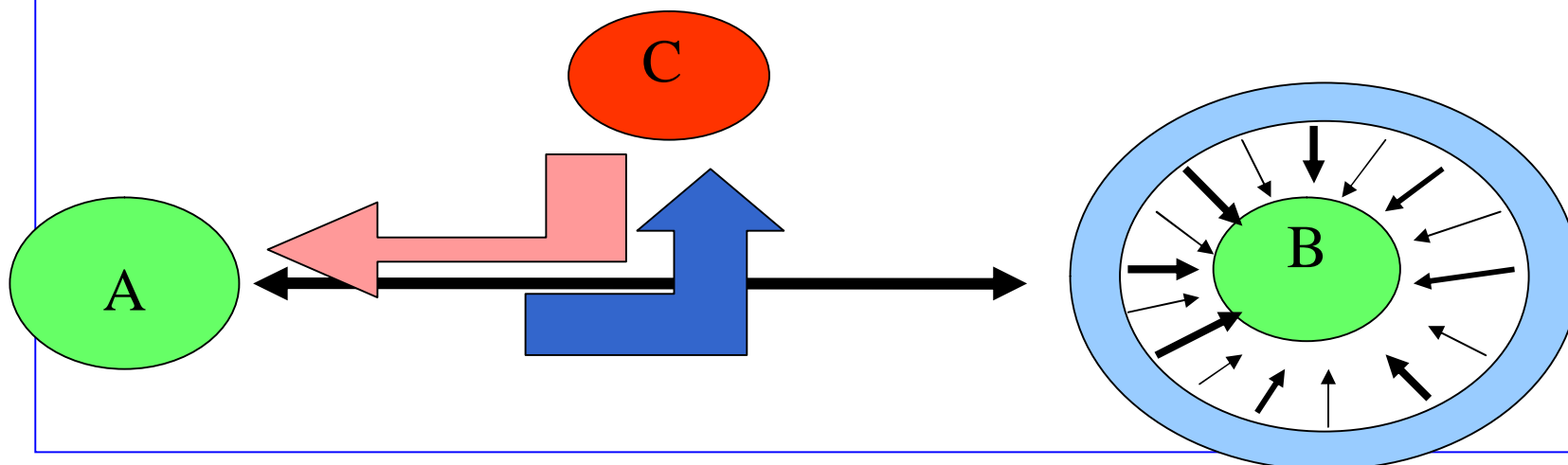


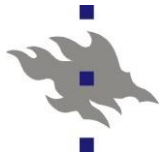
Figure 8.26 ♦ A DDoS attack



## Yhteyden kaappaus (hijacking)

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





# Haittaohjelma (malware) (1)

n itseään monistava: kun on saastuttanut yhden koneen, pyrkii levittämään kopioitaan muihin koneisiin

## n Virus

n Tarvitsee isännän levitäkseen ja vaatii yleensä käyttäjän toimintoa

n Sähköpostin liitetiedosto, joka avataan

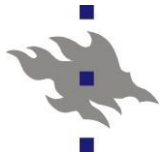
## n Mato

n Tulee tietoturva-aukosta ja leviää automaattisesti (Sasser)

n Levinneimmät madot kyllä kulkivat sähköpostin liitetiedostoina

- Morrisin mato (1988), Melissa (1999), Nimda (2001), Sobig (2003), ILoveYou, Slammer (2003 kaatoi 5 nimipalvelijaa)





## Haittaohjelma (2)

### n Troijalainen

n on ohjelma, joka sisältää myös jotakin muuta kuin käyttäjä uskoo sen sisältävän. Suorittaa kyllä jonkun hyödyllisen toiminnon

n Mutta lisäksi se voi

- käynnistää viruksen, madon,
- avaa takaportin tai muun haavoittuvuuden tietojärjestelmään
- tehdä tiedonhakua, tietojen tuhoamista tai vastaavaa jopa jättämättä mitään jälkiä.



## Vastatoimet? (1)

Pidä KJ:n  
turvapäivitykset  
ajan tasalla!

### n Koputtelu

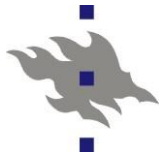
- n Käytä palomuuria
- n Seuraa liikennettä, reagoi, jos normaalista poikkeavaa
- n Seuraa aktiviteettia (IP-osoite, porttien koputtelu)

### n Salakuuntelu

- n Käytä kaksipisteyhteyksiä Ethernet-kytkin keskittimen sijasta
- n Salakirjoitus
- n Tarkista, ettei verkkokortti ole promiscuous-moodissa

### n IP-osoitteen väärentäminen

- n Lähetysverkossa helppo havaita ja estää
- n Yhdyskäytäväreititin voi tarkistaa, että lähettäjän IP-osoite kuuluu lähettävään verkkoon (ingress filtering)
- n Tutkimista ei voi tehdä pakolliseksi



## Vastatoimet (2)

### n Palvelunesto

- n Vaikea todeta / estää
- n Milloin SYN on oikeayhteyspyyntö, milloin osa hyökkäystä?
- n Palveluhyökkäyksen havaitsemis- ja estämisjärjestelmät

### n Haittaohjelmat

- n Turva-aukkopäivitysten asentaminen heti
- n Varovaisuus sähköpostiliitteiden kanssa
- n Älä asenna tai käytä 'tuntemattomia' ohjelmia
- n Käytä palomuuria ja virustorjuntaohjelmia



# Tietoturvasta

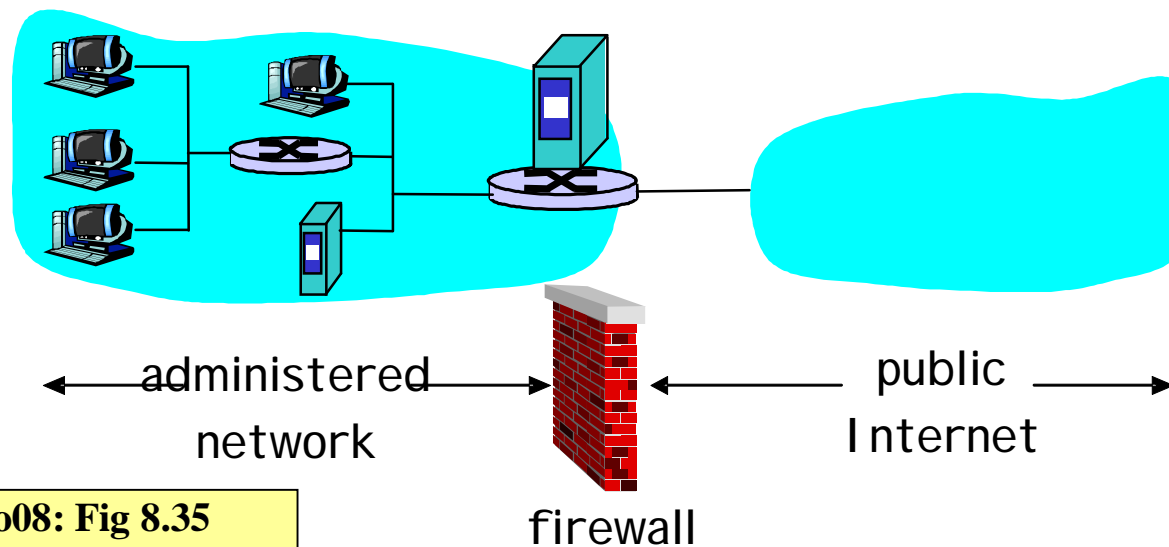
## Palomuuuri

Ch 8.9.1



## Palomuri (firewall)

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



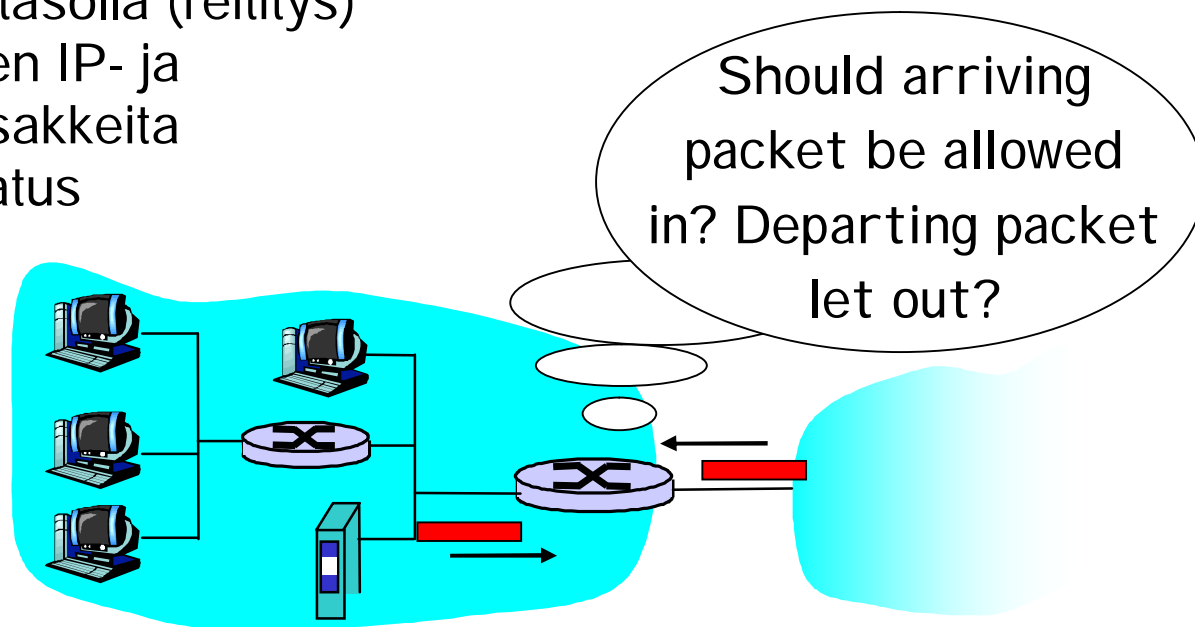
KuRo08: Fig 8.35



## Kaksi erilaista palomuuria

### n Paketteja suodattava palomuuuri (packet filtering firewall)

- n Toimii verkkotasolla (reititys)
- n Tutkii pakettien IP- ja TCP/UDP-otsakkeita
- n Karkea suodatus



### n Sovellustason yhdyskäytävä (application-level gateway)

- n Toimii sovelluskerroksella välittäjänä (relay)
- n Tutkii sovellusdataa
- n Hienojakoisempi suodatus



# Palomuuuri ja suodatus

- n Ennalta annetut säännöt suodatukselle
  - n Salliiko vai kieltääkö paketin etenemisen
  
- n Säännöt otsakekenttien perusteella
  - n Lähettäjän ja vastaanottajan IP-osoite
  - n Protokollan tyyppi
  - n TCP- ja UDP-porttinumerot
  - n Kontrollisanoman (ICMP) tyyppi
  - n TCP:n kättelysegmenttien SYN / ACK-bitit
  
- n Eri säännöt lähteville ja tuleville paketeille
  
- n Eri säännöt eri linkeille



## Palomuuuri ja suodatus (jatkuu)

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





# Tilallinen pakettinen suodatus

(Stateful packet filter)

- n Säännöillä on hankala toteuttaa monimutkaisia estopoliitikoita
  - n Sääntöjä tarvitaan helposti paljon, jopa tuhansia
  - n Niitä käydään läpi jossain järjestyksessä => väärä järjestys voi aiheuttaa ongelmia / virheitä paketin käsittelyssä
- n Suodatus kohdistuu yksittäiseen pakettiin
- n **Tilallinen pakettien suodatus**
  - n Suodatin tietää, mitkä TCP-yhteydet ovat käytössä
    - SYN, SYNACK ja ACK => yhteys muodostetaan
    - FIN-paketit => yhteys puretaan / poistetaan, jos ei käytetä (60 s)
    - Taulukko voimassa olevista TCP-yhteyksistä
  - n Esim. intranetistä lähetetty web-kysely => päästetään vastaus läpi

# ■ Sovellustason yhdyskäytävä (Application gateway)

## n Kun halutaan hienojakoisempaa suodatusta

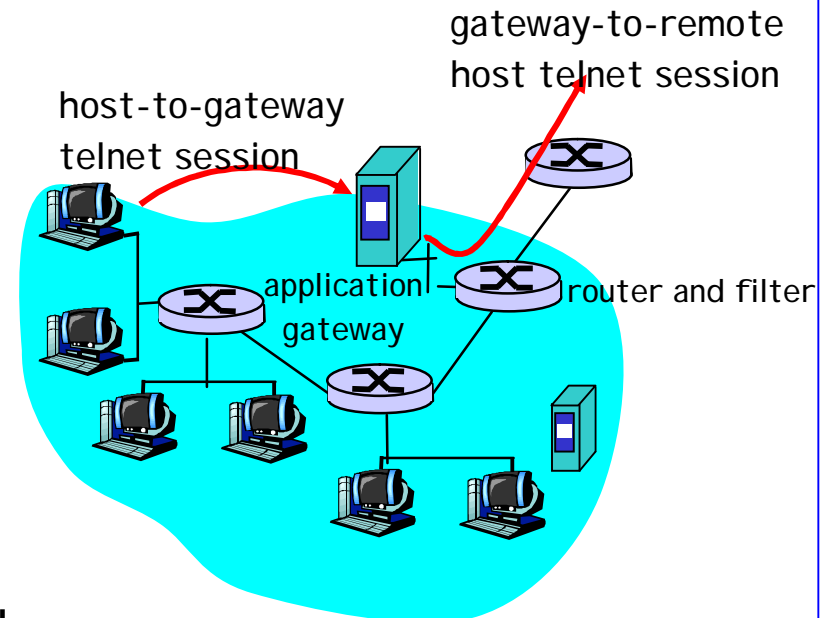
- n Esim. Telnet-yhteyden salliminen tunnetuille käyttäjille, mutta näiden identiteetti on ensin todettava (autentikointi)
- n Tähän pelkkä IP/TCP/UDP-otsakkeiden tutkiminen ei riitä

## n Toimii välittävänä koneena (relay) sisäverkon ja Internetin välissä

- n Eri sovelluksilla oma yhdyskäytäväprosessinsa
- n Esim. IMAP, SMTP, HTTP

## n Ulkoa yhteys ensin yhdyskäytäväkoneeseen

- n Autentikoi tarvittaessa
- n Muodostaa yhteyden sisäverkon koneeseen (palomuri sallii tämän vain sille)
- n Välittää sanomat sisään/ulos



Kuro08:Fig 8.36



## Palomuuuri / Yhdyskäytävä

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

Myös hyvin ylläpidetyt järjestelmät kärsivät hyökkäyksistä!



## Käytännön ohjeita

Käytä palomuuria  
Huolehdi KJ:n päivityksistä  
Käytä virustorjuntaa  
Hävitä haittaohjelmat

### n Uusi kone

- n Älä kytke verkkoon ennenkuin olet ottanut palomuurin käyttöön
- n Päivitä käyttöjärjestelmä heti

### n Yliopiston lisenssillä saat koneellesi F-Securen ja Symantecin virustorjunta- ja palomuuriohjelmat

- n <https://www.helsinki.fi/atk/ohjelmajakelu/>

### n Muitakin ilmaisia ohjelmia löytyy

### n Lue lisää esim. "Jokakodin tietoturvaopas"

- n [www.tietoturvaopas.fi](http://www.tietoturvaopas.fi) tai [www.tietoturvakoulu.fi](http://www.tietoturvakoulu.fi)



# Kertauskysymyksiä

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