



Tietoliikenteen perusteet

Tietoturvasta

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



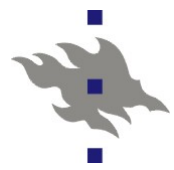
Sisältö

Tietoturva-kurssit:
kryptografian perusteet
IPSec

- Turvavaatimukset
- Uhkia
- Palomuuuri

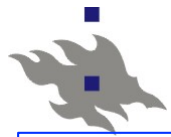
Oppimistavoitteet:

- 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



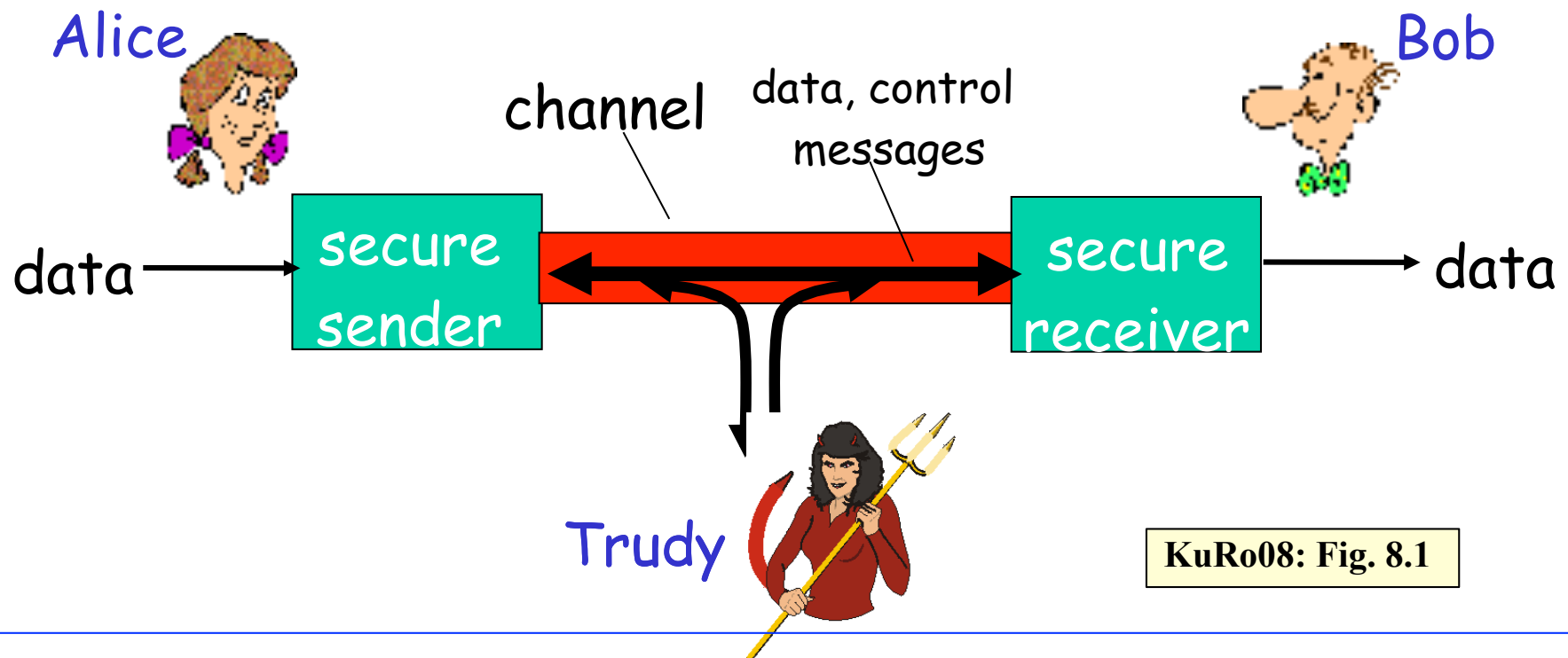
Turvavaatimukset

- **Luottamuksellisuus (confidential, secrecy)**
 - Vain lähettäjä ja vastaanottaja 'ymmärtävät' sanoman sisällön
 - Muu eivät saa välttämättä tietoa edes sen olemassaolosta
 - Salakirjoitus
- **Autentikointi (authentication)**
 - Lähettäjä ja vastaanottaja varmistuvat toistensa identiteeteistä
 - Oikeaksi todentaminen, salakirjoitus
- **Integriteetti, koskemattomuus (message integrity)**
 - Lähettäjä ja vastaanottaja varmoja siitä, ettei sanomaa ole muutettu (siirron aikana ta myöhemmin)
 - Digitaalinen allekirjoitus
- **Palveluiden saatavuus ja suojaus**
 - Palvelut ovat saatavilla käyttötarkoituksen mukaisesti
 - Vain niillä pääsy, joilla lupa käyttää käyttöoikeuksien mukaisesti
 - Käyttäjätunnus ja salasana, tiedostojen / objektien käyttöoikeudet, ...
 - Suojautuminen 'ulkoa' tulevia hyökkäyksiä vastaan (haittaohjelmat, palvelunestohyökkäys) vastaan
 - palomuri, havaitsemis- ja puhdistusohjelmat

Ystävää ja tunkeutuja

Tuttu asetelma reaali maailmasta

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





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

- Järjestelmän tietoturvan määrittää sen tietoturvan kannalta heikoin elementti
- Tietoturva pitää ottaa huomioon alusta asti järjestelmäsuunnittelussa
- Protokollat pitää suunnitella niin että niitä voidaan päivittää (esim. SHA-1 → SHA-256)
- Käytännössä tietoturvaratkaisuita tarvitaan useilla kerroksilla
 - Linkki (WPA, WEP, EAP, 802.1X, 2G/3G)
 - Verkko (IPSec)
 - Välikerroksella HIP (Host Identity Protocol)
 - Kuljetus (TLS)
 - Sovellus (HTTPS, Radius, Diameter, S/MIME, XML Security...)



Kryptoratkaisut

■ Symmetrinen

- Jaetut salasanat

■ Asymmetrinen

- Julkinen avain (public key), salainen avain (private key)

- Julkisten avainten jakelu

- Salaus (A -> B):

- A salaa B:n julkisella avaimella
- B avaa salaisella avaimellaan

- Allekirjoitus:

- A allekirjottaa salaisella avaimellaan
- B tarkistaa allekirjoituksen A:n julkisella avaimella

- Diffie-Hellman avaintenjakoprotokolla

- Yleensä julkisen avaimen kryptoa käytetään symmetrisen avaimen muodostamiseen



Tietoturvasta

Uhkia

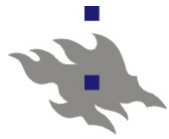
Ch 1.6



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

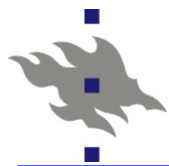
■ Ping

Lähetää kyselyjä valittuihin verkon IP-osoitteisiin

Hengissä olevat koneet vastaavat

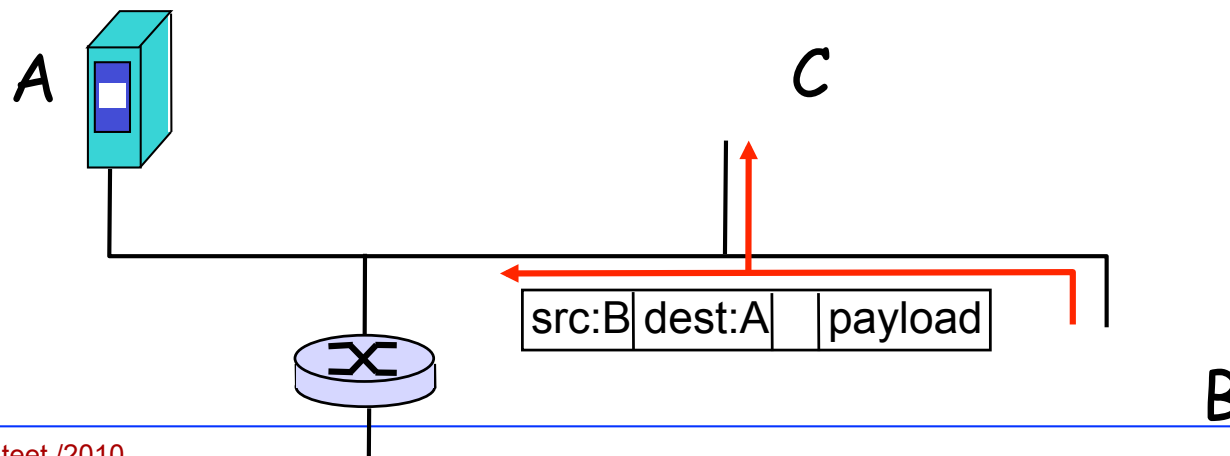
■ Porttiselaus (port scanning)

- Kokeilee systemaattisesti TCP/UDP-yhteyttä koneen portteihin
- Vastauksista saa selville tarjotut palvelut
- 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)

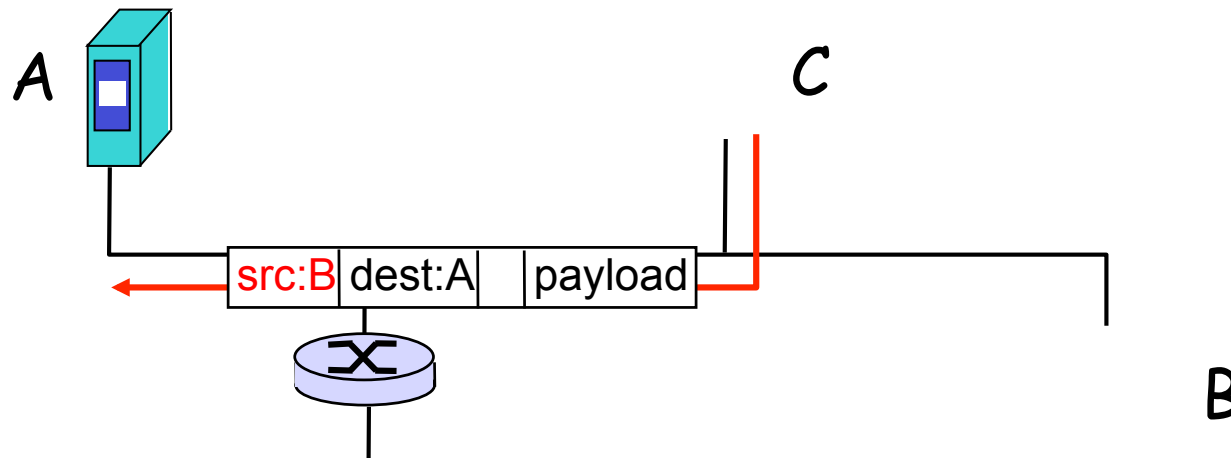
- Tutkii linkkikerroksen kehysten sisältöä
 - Yleislähetys: kaikki kuulevat kaikki kehykset
 - Valikoimattomassa moodissa (promiscuous) toimiva sovitinkortti myös kopioi kaikki kehykset itselleen
 - Kuuntelevan koneen oltava samassa LAN:ssa
- Ohjelmia, joilla paketit voidaan purkaa tekstimuotoon
 - Hyödyllisiä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

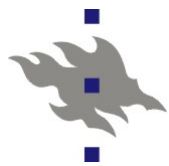




Väärentäminen (spoofing)

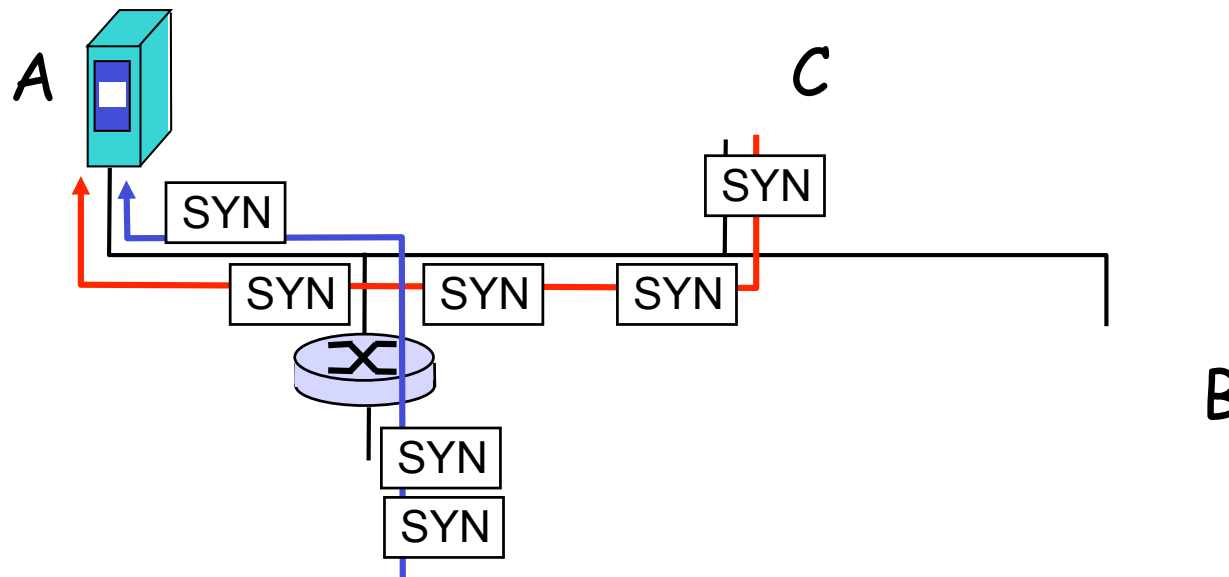
- Vastaanottaja ei voi tietää, kuka on todellinen lähettäjä
- Jokainen, joka kontrolloi koneensa ohjelmistoa (erityisesti KJ:tä) voi väärentää mm. IP-osoitteen
 - Sovellus voi tehdä itse IP-paketin ja ohittaa KJ:n pakettia lähettäessä ('raw' mode)





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





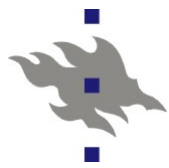
Palvelunestohyökkäys (jatkuu)

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

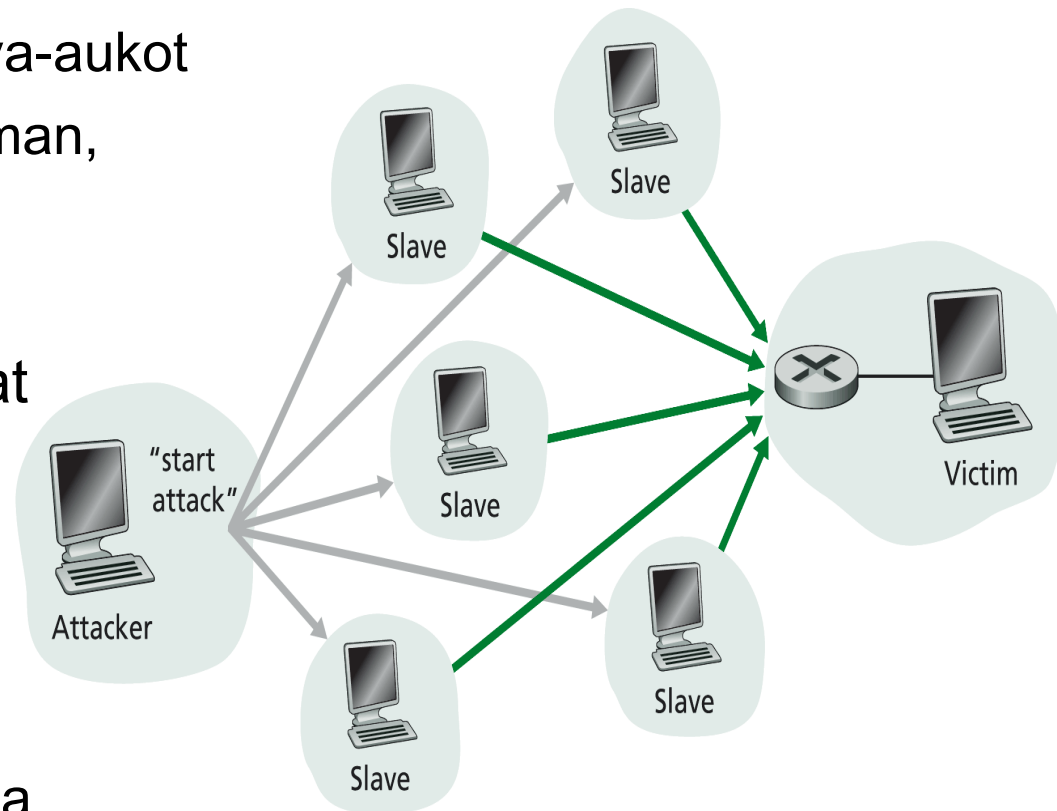
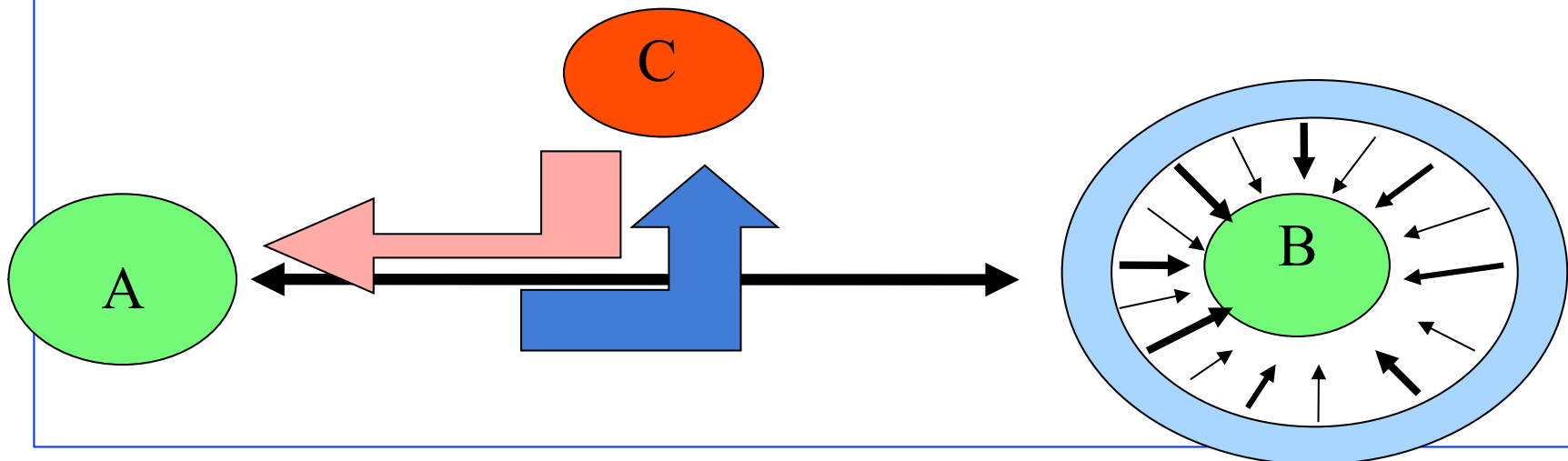


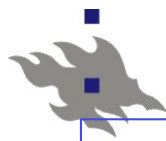
Figure 8.26 ♦ A DDoS attack



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





Haittaohjelma (malware) (1)

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

■ Virus

- Tarvitsee isännän levitäkseen ja vaatii yleensä käyttäjän toimintoa
- Sähköpostin liitetiedosto, joka avataan

Downadup-madon tekijästä
2500000 dollarin palkkio!
MICROSOFT

■ Mato

- Tulee tietoturva-aukosta ja leviää automaattisesti (Sasser)
Slammer (2003 kaatoi 5 nimipalvelijaa))
- Levinneimmät madot kyllä kulkivat sähköpostin liitetiedostoina
 - Morrisin mato (1988), Melissa (1999), Nimda (2001), Sobig (2003), ILoveYou,
- Downadup (2007-2008): hyödyntää Microsoftin Windows-käyttöjärjestelmässä joulukuussa löytynyttä turvareikää, arvaa verkon salasanoja ja tartuttaa USB-muistitikkuja.



Haittaohjelma (2)

■ Troijalainen

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

■ 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



Vastatoimet (2)

■ Palvelunesto

- Vaikea todeta / estää
- Milloin SYN on oikeayhteyspyyntö, millloin osa hyökkäystä?
- Palveluhyökkäyksen havaitsemis- ja estämisjärjestelmät
- SYN cookie (seuraava kalvo)
- ISP Hotline

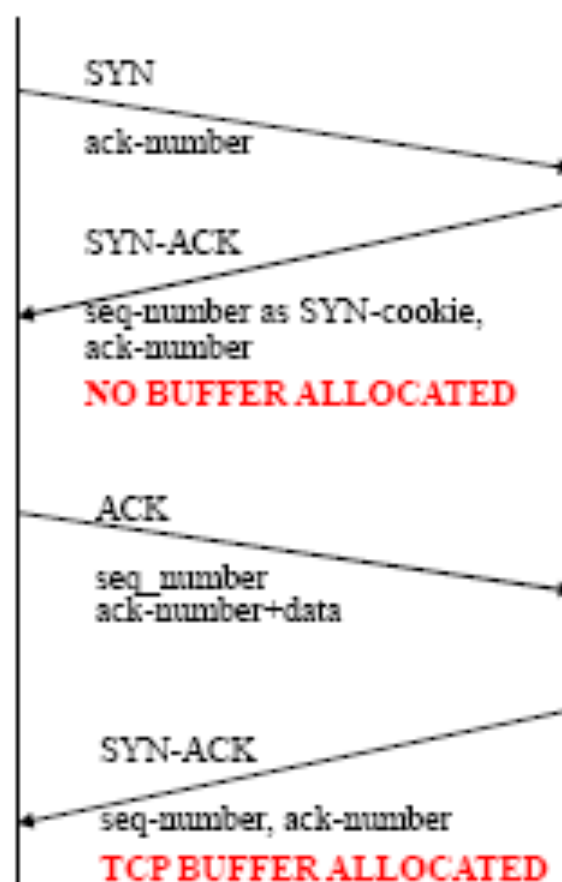
■ Haittaohjelmat

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



SYN Cookies

- Client
 - sends SYN packet and ACK number to server
 - waits for SYN-ACK from server w/ matching ACK number
- Server
 - responds w/ SYN-ACK packet w/ initial SYN-cookie sequence number
 - Sequence number is cryptographically generated value based on client address, port, and time.
- Client
 - sends ACK to server w/ matching sequence number
- server
 - If ACK is to an unopened socket, server validates returned sequence number as SYN-cookie
 - If value is reasonable, a buffer is allocated and socket is opened





Tietoturvasta

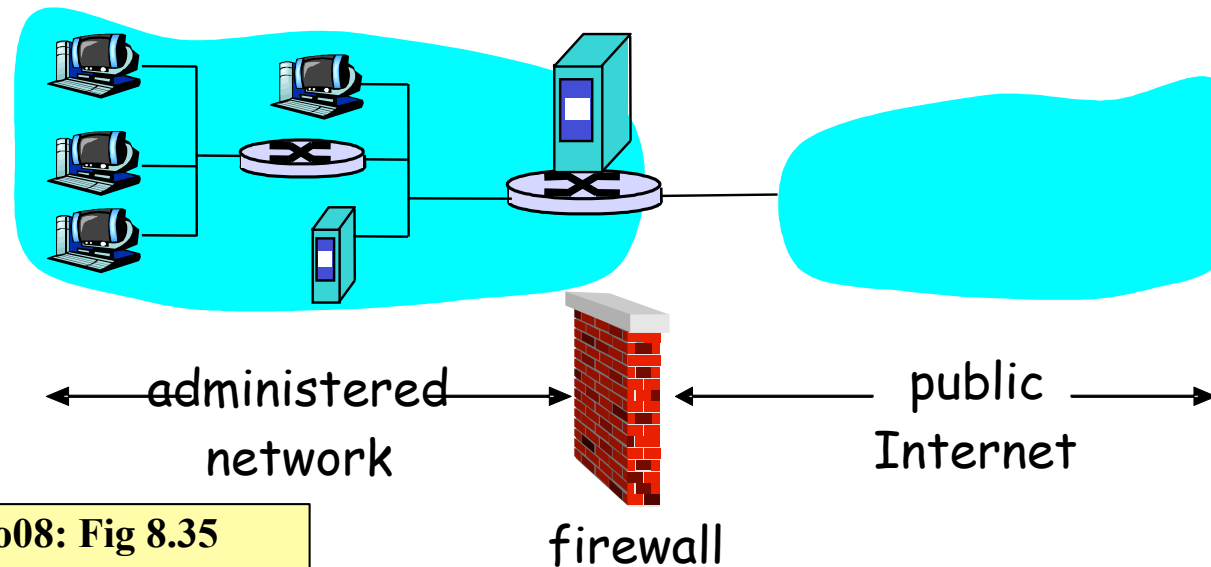
Palomuuuri

Ch 8.9.1

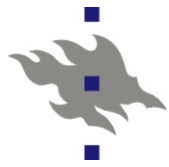


Palomuri (firewall)

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



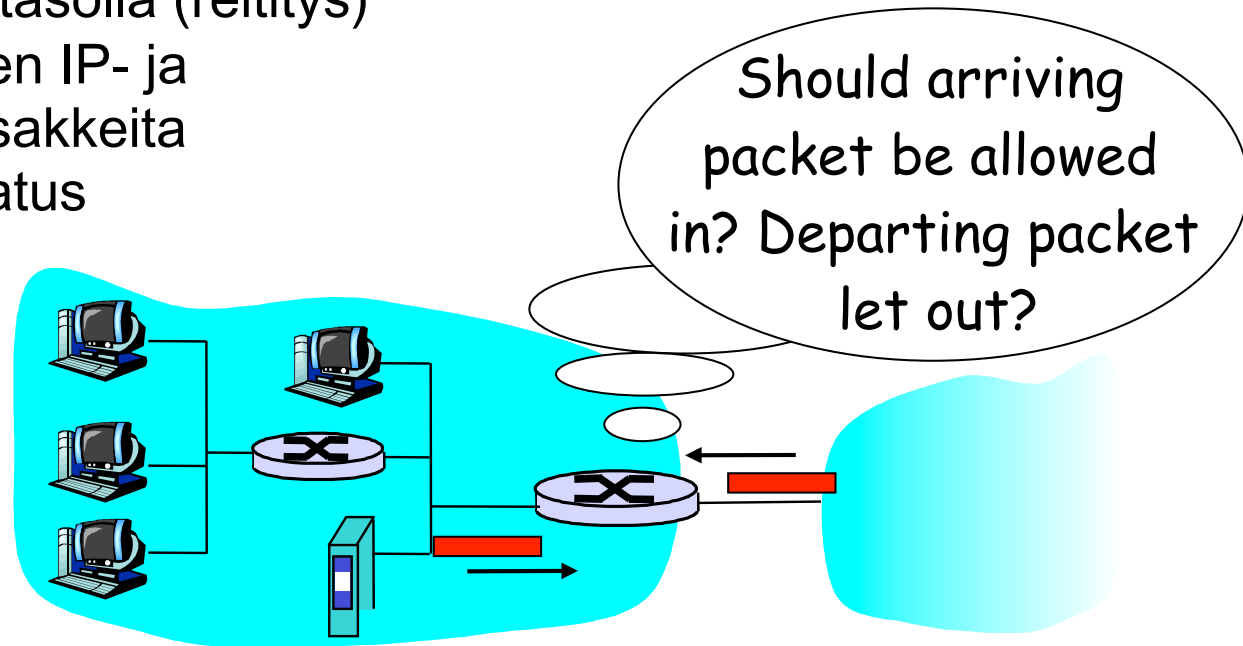
KuRo08: Fig 8.35



Kaksi erilaista palomuuria

■ Paketteja suodattava palomuuuri (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



Palomuri ja suodatus

- Ennalta annetut säännöt suodatukselle
 - Salliiko vai kieltääkö paketin etenemisen

- Säännöt otsakekenttien perusteella
 - Lähettäjän ja vastaanottajan IP-osoite
 - Protokollan tyyppi
 - TCP- ja UDP-porttinumerot
 - Kontrollisanoman (ICMP) tyyppi
 - TCP:n kättelysegmenttien SYN / ACK-bitit

- Eri säännöt lähteville ja tuleville paketeille

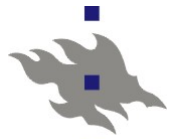
- Eri säännöt eri linkeille



Palomuuuri ja suodatus (jatkuu)

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

- www.cert.org/tech_tips/packet_filtering.html



Tilallinen pakettien suodatus

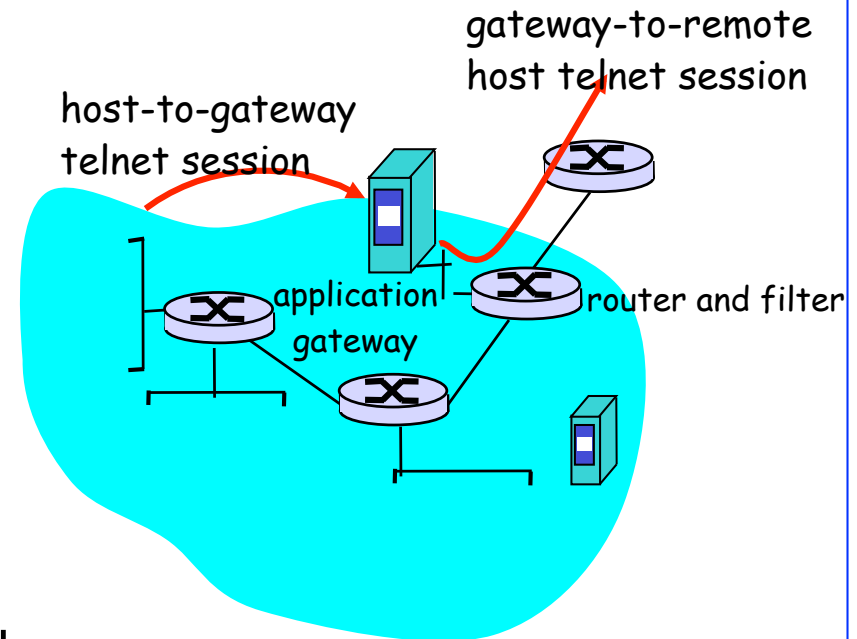
(Stateful packet filter)

- 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
- Suodatus kohdistuu yksittäiseen pakettiin
- **Tilallinen pakettien suodatus**
 - 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
 - Esim. intranetistä lähetetty web-kysely => päästetään vastaus läpi



Sovellustason yhdyskäytävä (Application gateway)

- Kun halutaan hienojakoisempaa suodatusta
 - Esim. Telnet-yhteyden salliminen 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 yhdyskäytäväkoneeseen
 - Autentikoi tarvittaessa
 - Muodostaa yhteyden sisäverkon koneeseen (palomuuuri sallii tämän vain sille)
 - Välittää sanomat sisään/ulos



Kuro08:Fig 8.36



Palomuuuri / Yhdyskäytävä

- Yhteyttä haluavan on osattava ottaa 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 lissensillä 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 tai www.tietoturvakoulu.fi



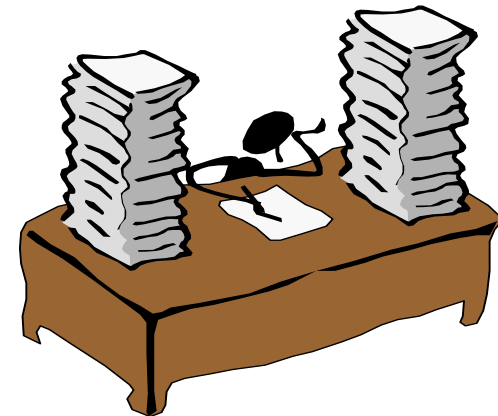
Kertauskysymyksiä

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



Kurssin sisältö

1. Tietokoneverkot ja Internet
Internetin rakenne, terminologiaa
2. Verkkosovelluksia ja sovellusprotokollia
Web, sähköposti, nimipalvelu, tiedostopalvelu, pistokerajapinta
3. Kuljetuskerros: TCP, UDP
yhteydellinen / yhteydetön, ruuhkanhallinta
4. Verkkokerros: IP
reitittimet ja reititys
5. Linkkikerros, lähiverkot
Ethernet, kytkimet
6. Tietoturvasta
Uhkat, palomuuuri





Tentit

- Kurssikoe 14.12. 16-19 A111
- Uusintakoe 25.1. 16-20 A111