

6. Internetin turvattuus ja palomuuuri

■ Internetin turvaongelmia

- Tietojen keruu turva-aukkojen löytämiseksi ja koneen valtaaminen
- Internetissä kulkevan tiedon tutkiminen
- IP-osoitteen väärentäminen
- Palvelunestohyökkäykset (DOS-hyökkäykset)
- Yhteyden kaappaaminen

■ Palomuuuri

- Paketteja suodattava palomuuuri
- Sovelluskerroksen yhdyskäytävä

■ Salausmenetelmät (ei käsitellä tällä kurssilla)

Tietojen keruu eli kartoitus (mapping)

□ Tavoitteena on saada tietoja

- IP-osoitteista
- käyttöjärjestelmistä
- käytetyistä ohjelmista

ja sitten hyödyntää eri järjestelmien turva-aukkoja.

□ **Ping**

Lähetetään ping-kyselyjä eri osoitteisiin, vastaajat ilmoittavat oman IP-osoitteensa

□ **Porttiselaus** (port scanning) =

systemaattisesti otetaan TCP- tai UDP-yhteyksiä jonkin koneen porttinumeroihin ja vastauksista saadaan selville tarjotut palvelut

Pakettien tutkiminen (packet sniffing)

- **Passiivisesti kuunnellaan linkkikerroksen liikennettä ja tutkitaan kehysten sisältöä**
 - Ethernetissä sovitinkortti tutkii kaikki kehykset
 - Valikoimattomassa moodissa (promiscuous) toimiva sovitinkortti kopioi kaikki kehykset itselleen
 - Valmiita ohjelmia, joilla paketit puretaan
- **Hyödyllinen väline verkon valvojalle, mutta vaarallinen vihamielisissä käsissä**
 - Hyökkääjä etsii erityisesti salasanoja
 - Salasanat syytä aina salakirjoittaa

IP-osoitteen väärentäminen (spoofing)

- Jokainen, joka kontrolloi koneen ohjelmistoa (erityisesti käyttöjärjestelmää) voi väärentää IP-osoitteen datagrammin lähdekenttään!
- **Teknisesti helppo havaita ja estää**
 - Jokainen verkon reunareititin tarkistaa, että lähettäjän IP-osoite tulee oikeasta liitännästä = minne sille lähetetäänkin
 - **Ei voi tehdä pakolliseksi!**

Palvelunestohyökkäys (DoS = Denial of Service)

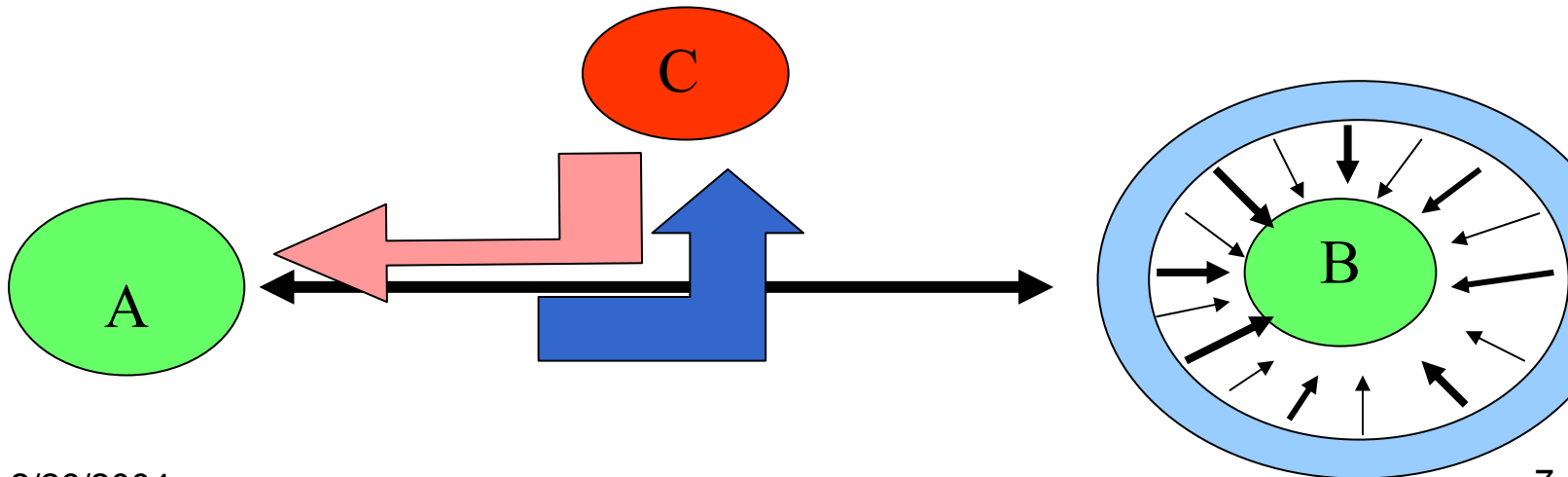
- Kuormitetaan palvelua niin, etteivät 'oikeat' käyttäjät pääse sitä lainkaan käyttämään
 - **SYN-tulvitus** = käyttäen eri IP-osoitteita aloitetaan suuri määrä yhteyksiä lähettämällä 1. SYN-segmentti, mutta ei koskaan päätetä yhteydenmuodostusta ACK:lla; uhrilta loppuu muisti
 - **IP-paloittelu** = lähetetään IP-pakettien osia, jotka vastaanottaja puskuroidaan odottamaan puuttuvia paloja, joita ei koskaan tule => muisti loppuu
 - **Smurf-hyökkäys** = monelle koneelle uhrin IP-osoitteella varustettuja ICMP Echo-request-paketteja; ECHO-vastaukset tukkivat uhrin koneen

Hajautettu DoS-hyökkäys (DDoS)

- Hyökkääjä ottaa ensin haltuunsa ison joukon muita koneita niiden käyttäjien sitä huomaamatta ('orjakoneita')
 - hyökkäysohjelma, joka vain odottaa käskyä
- Kaikki vallatut koneet aloittavat samaan aikaan DDoS-hyökkäyksen uhrin kimppuun.
- Vaikea estää:
 - milloin SYN on oikea yhteyspyyntö, milloin osa hyökkäystä?

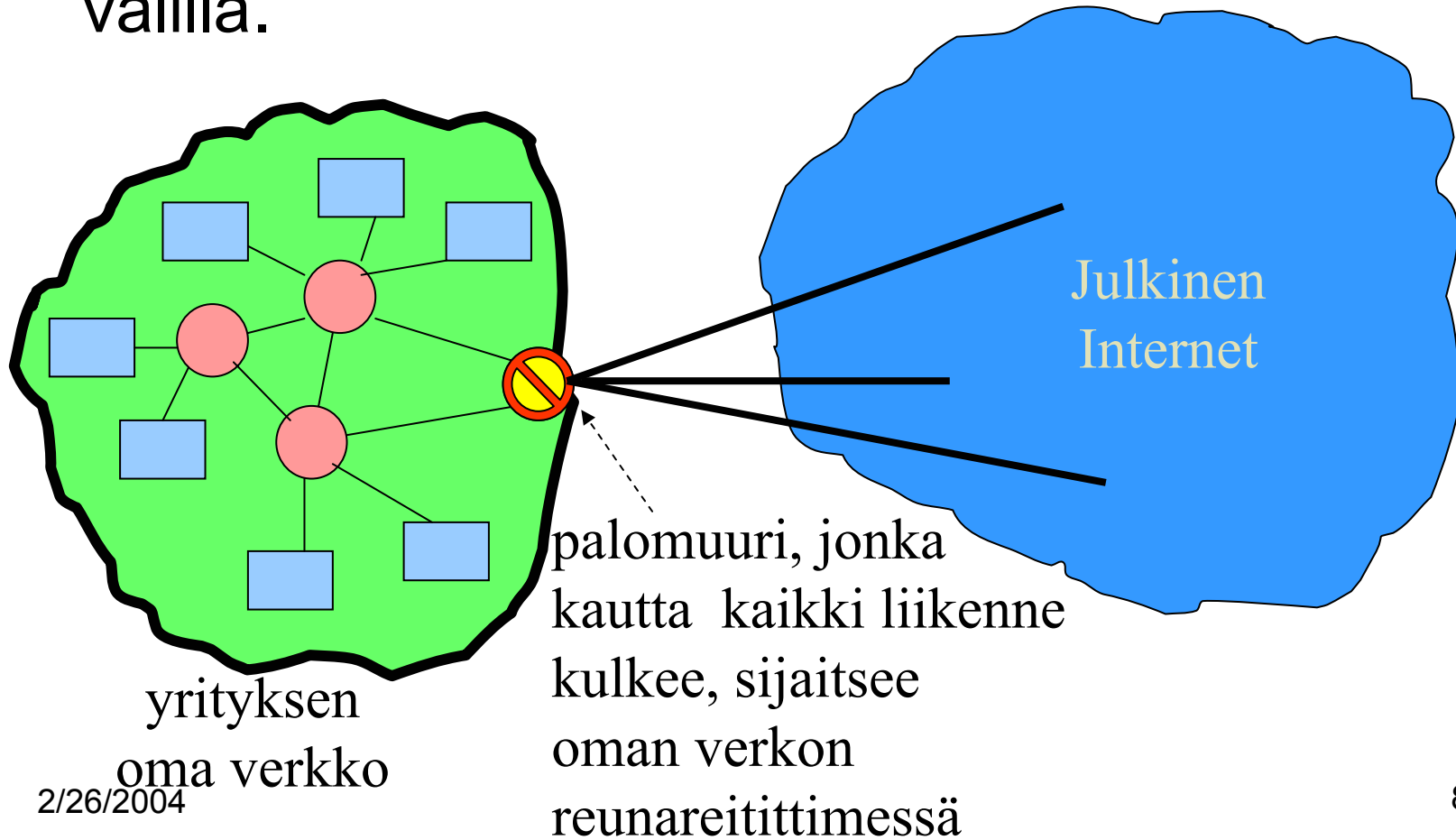
Yhteyden kaappaus (hijacking)

- Kolmas osapuoli C kaappaa itselleen A:n ja B:n välisen yhteyden
 - poistaa B:n pelistä palvelunestohyökkäyksellä
 - tekeytyy itse B:ksi (tuntee jo tavujen numeroinnin)



Palomuuri (firewall)

- Ohjelmisto + laitteisto, jolla valvotaan pääsyä yrityksen oman verkon ja julkisen Internetin välillä.

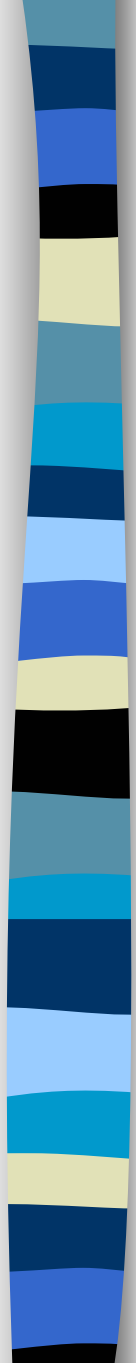


Kaksi erilaista palomuuria:

- **Paketteja suodattava palomuuuri**
 - Toimii verkkotasolla
 - Tutkii pakettien IP- ja TCP/UDP-otsakkeita
 - Karkea lajittelu
- **Sovellustason yhdyskäytävä (gateway)**
 - Toimii sovellustasolla
 - Tutkii sovellusdataa
 - Hienojakoisempi lajittelu

Pakettien suodatus

- Reunareitittimessä (palomuurissa)
 - Datagrammin otsakkeet tutkitaan
 - Päätökset (= sallitaanko vai kielletäänkö paketin lähettäminen) tehdään ennalta annettujen sääntöjen pohjalta. Säännöt pohjaavat otsakekenttien tietoihin:
 - Lähettäjän ja vastaanottajan IP-osoitteisiin
 - TCP- ja UDP-portteihin
 - Kontrollisanoman (ICMP) tyyppiin
 - kättelysanomiin
- Esim. Kielletään UDP-paketit ja Telnet-yhteydet tai Telnet-yhteydet vain tietyistä IP-osoitteista

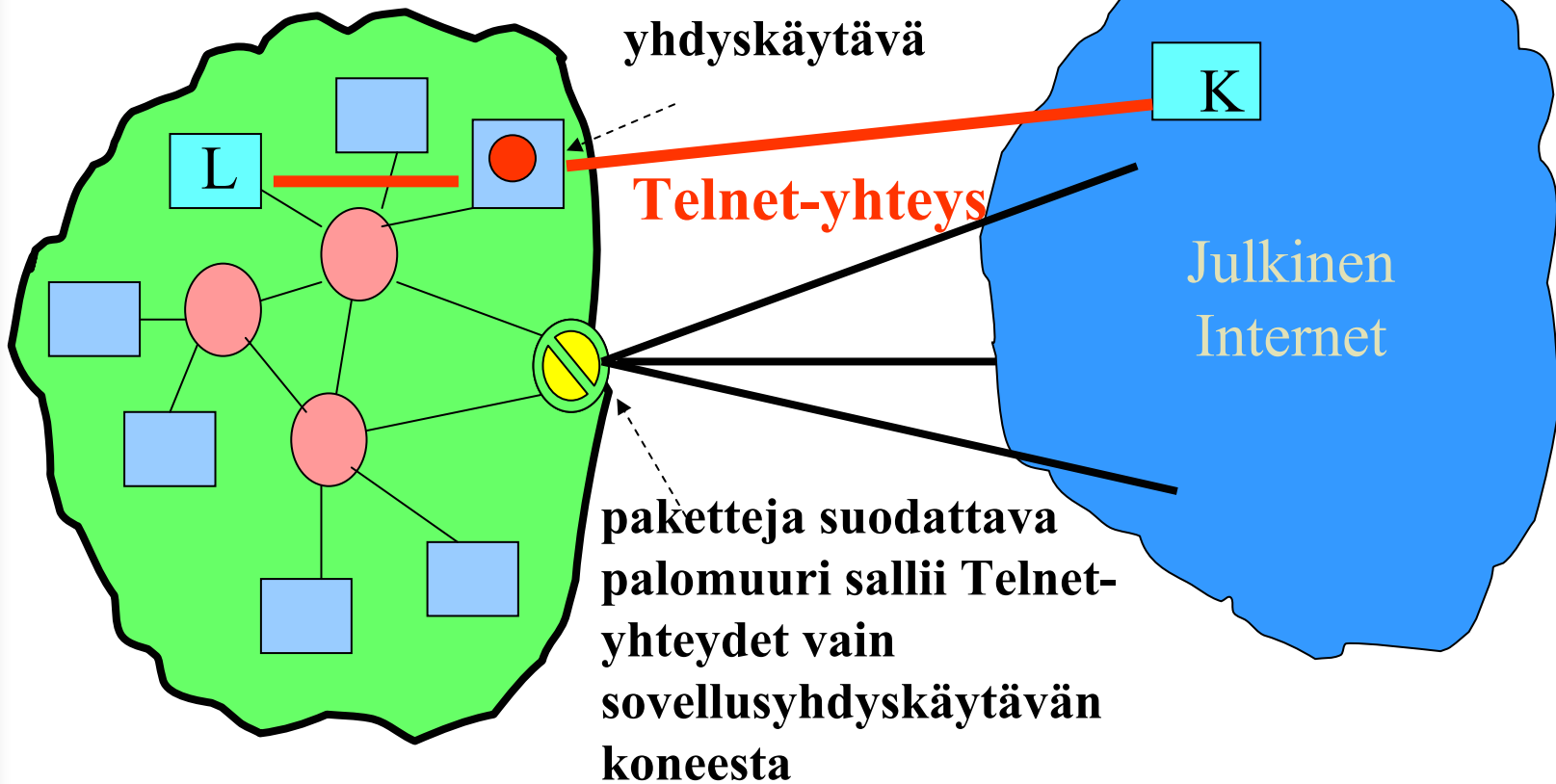
- 
- kieltämällä kaikki paketit, joissa ACK-bitti on 0, estetään ulkoapäin tulevat yhteydenmuodostuspyynnöt (SYN, ACK=0)
 - säännöillä on hankala toteuttaa monimutkaisia estopoliitikoita
 - sääntöjä tarvitaan helposti paljon (jopa tuhansia)
 - niitä käydään läpi jossakin järjestyksessä => väärä järjestys voi aiheuttaa ongelmia eli virheitä pakettien käsittelyssä

Sovellusyhdyskäytävä (Application Gateway)

- Pakettien suodatus ei riitä, jos halutaan hienojakoisempaa suodatusta:
 - Esim. Telnet-yhteyden salliminen tietyille käyttäjille, joiden on ensin todennettava henkilöllisyytensä.
- Sovellusyhdyskäytävä tekee päätökset sovellusprotokollan datasta
 - eri sovelluksilla (esim. SMTP, HTTP) oma yhdyskäytävä
 - => useita erilaisia prosesseja

yrityksen oma
verkko

sovellus-
yhdyskäytävä



Kun kone L haluaa Telnet-yhteyden koneeseen K, sen on ensi otettava Telnet-yhteys sovellusyhdyskäytävään, joka autentikoi käyttäjäm ja tarkistaa käyttöoikeuden. Jos kaikki ok, niin yhdyskäytävä muodostaa Telnet-yhteyden koneeseen K.

Ongelmia:

- jokaiselle sovellukselle oltava oma yhdyskäytävä
- yhdyskäytävä välittää kaiken datan
- asiakkaan on osattava ottaa yhteys yhdyskäytävään ja pystyttävä viestimään sen kanssa
- eri ratkaise kaikkia turvaongelmia
 - IP-osoitteiden ja porttinumeroiden väärentäminen
 - yhdyskäytäväohjelmissa voi olla turva-aukkoja
 - langattomat yhteydet ja soittoyhteydet