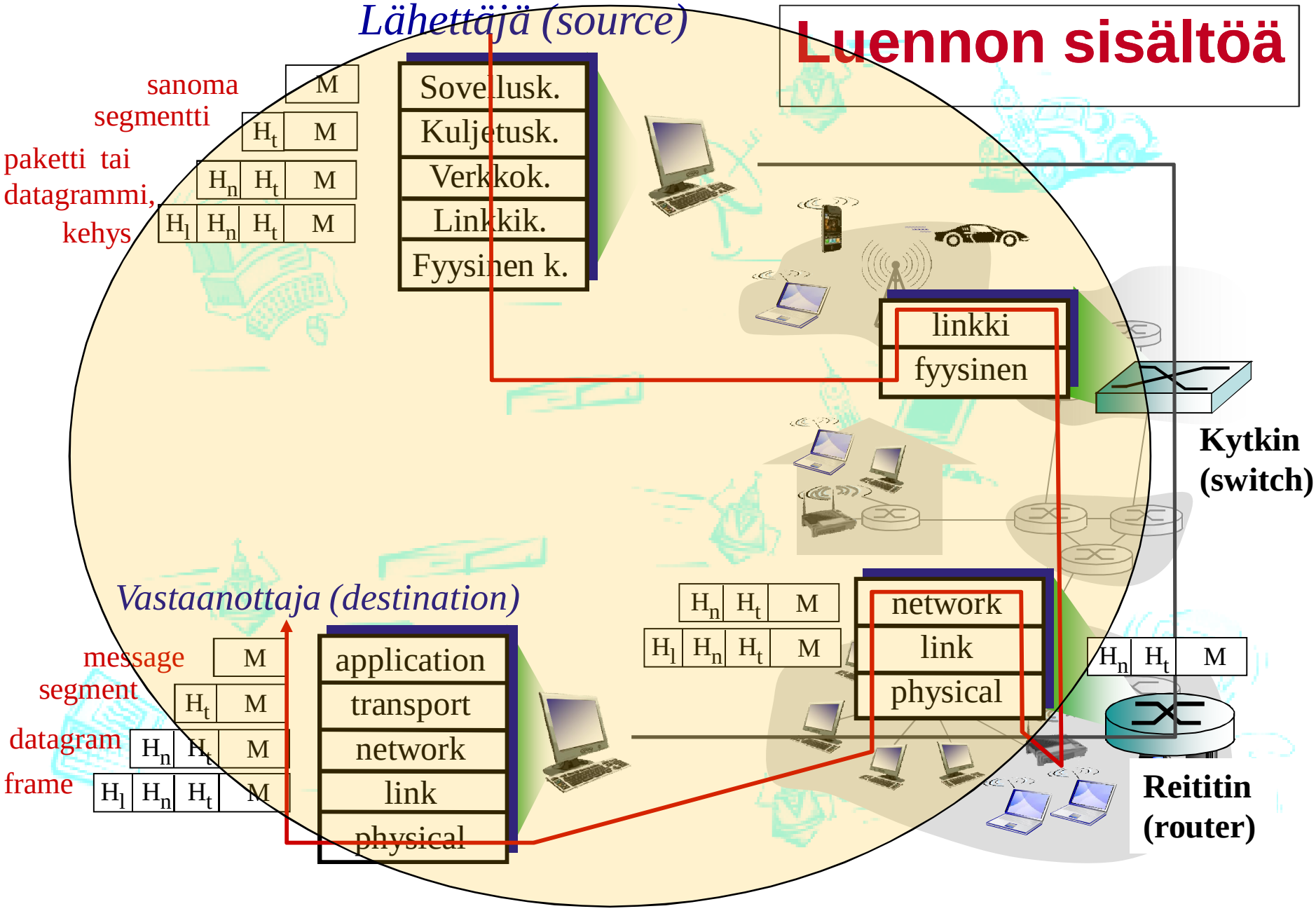
Tietoliikenteen perusteet

Luento 13: Tietoliikenteen turvallisuus: Palomuurit

Syksy 2014, Tiina Niklander

Kurose&Ross: Ch 8

Luennon sisältöä



Sisältö

- **Uhkia ja vastatoimia**
- **Palomuuri**
- **Tunkeutumisen havaitseminen (IDS)**
- **WEP (torstain luennolta)**

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

UHKIA

Ch 1.6

Hyökkääjän toimia?

- Koputtelee koneen portteja (mapping)
  - Turva-aukkojen löytämiseksi ja koneen valtaamiseksi
- Salakuuntelee (eavesdropping, sniffing)
  - Sieppaa sanoman matkalla ja tutkii sisällön
- Väärentää, “peukaloi”, “tekeytyy” (impersonation, spoofing)
  - Vaihtaa paketin tietoja, esim. IP-osoitteen
  - Tekeytyy toiseksi osapuoleksi
- 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)

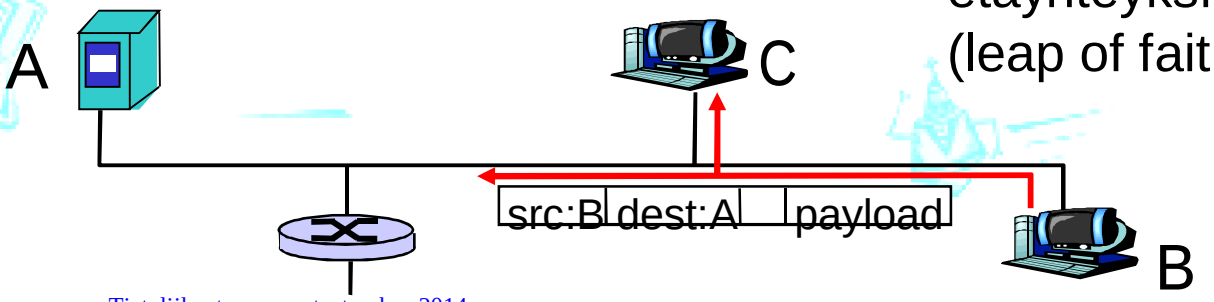
- Kaivelee ensin taustatietoja
  - IP-osoitteista, käyttöjärjestelmistä, verkko-ohjelmista
- Hyödyntää sitten tunnettuja turva-aukkoja
- Ping
  - Lähettää kyselyjä valittuihin verkon IP-osoitteisiin
  - Hengissä olevat koneet vastaavat

Koputtelu ja kartoitus (mapping)

- Porttiselaus (port scanning)
  - Kokeilee systemaattisesti TCP/UDP-yhteyttä koneen portteihin
  - Vastauksista saa selville tarjotut palvelut
  - Onko niissä tunnettuja turva-aukoja?
    - 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 (muutama vuosi sitten)

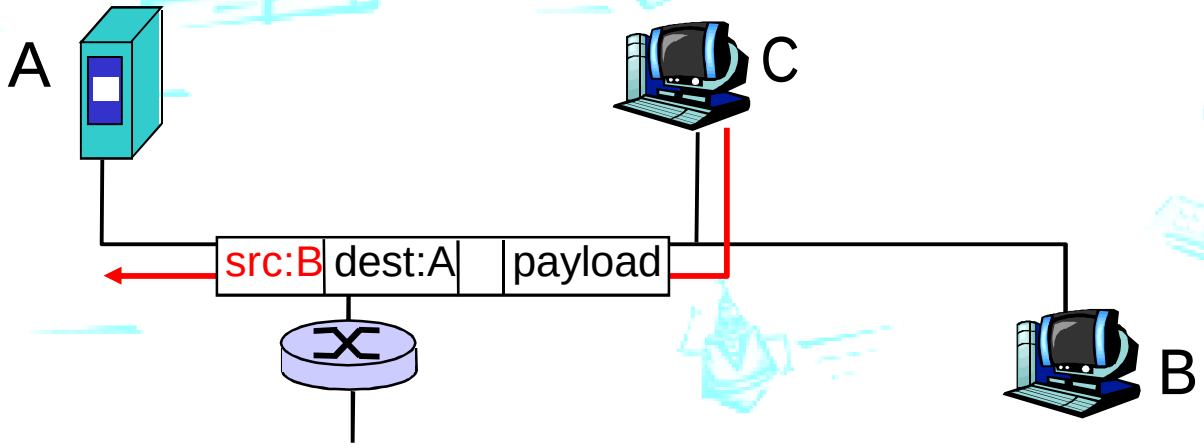
Salakuuntelu (packet sniffing)

- Tutkii linkkikerroksen kehysten sisältöä
  - Yleislähetys: kaikki kuulevat kaikki kehykset
  - Valikoimattomassa moodissa (promiscuous) toimiva sovitinkortti 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)



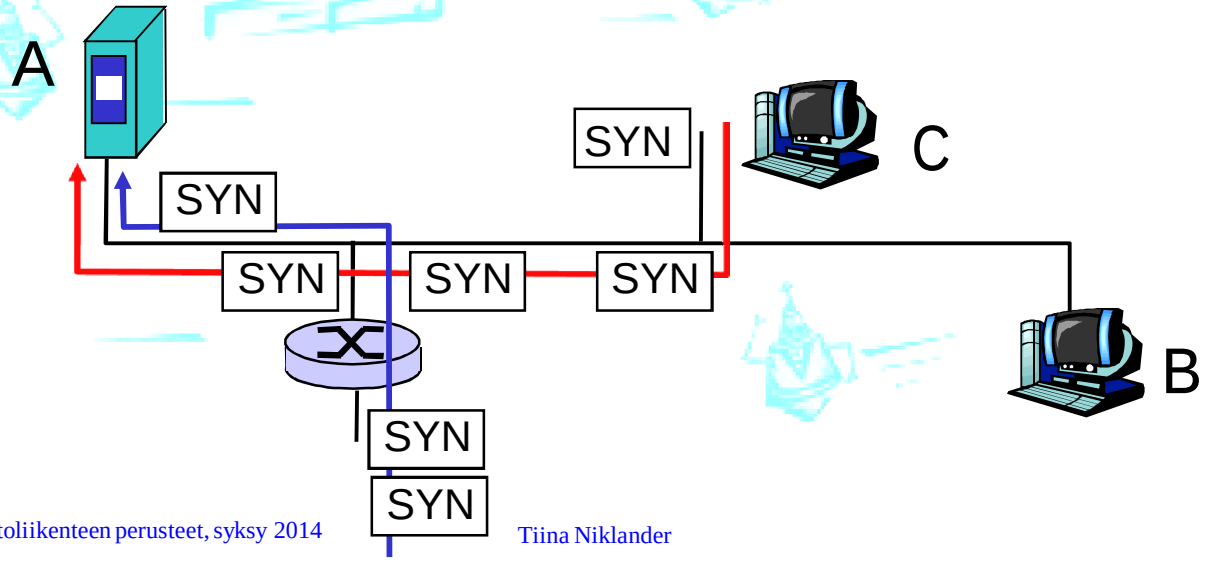
Väärentäminen (spoofing)

- 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/kellonaikaa
- Kaapatut koneet aloittavat samaan aikaan hyökkäyksen uhrin kimppuun hajautetusti
  - IP-osoitteet peukaloituja (harvoin)

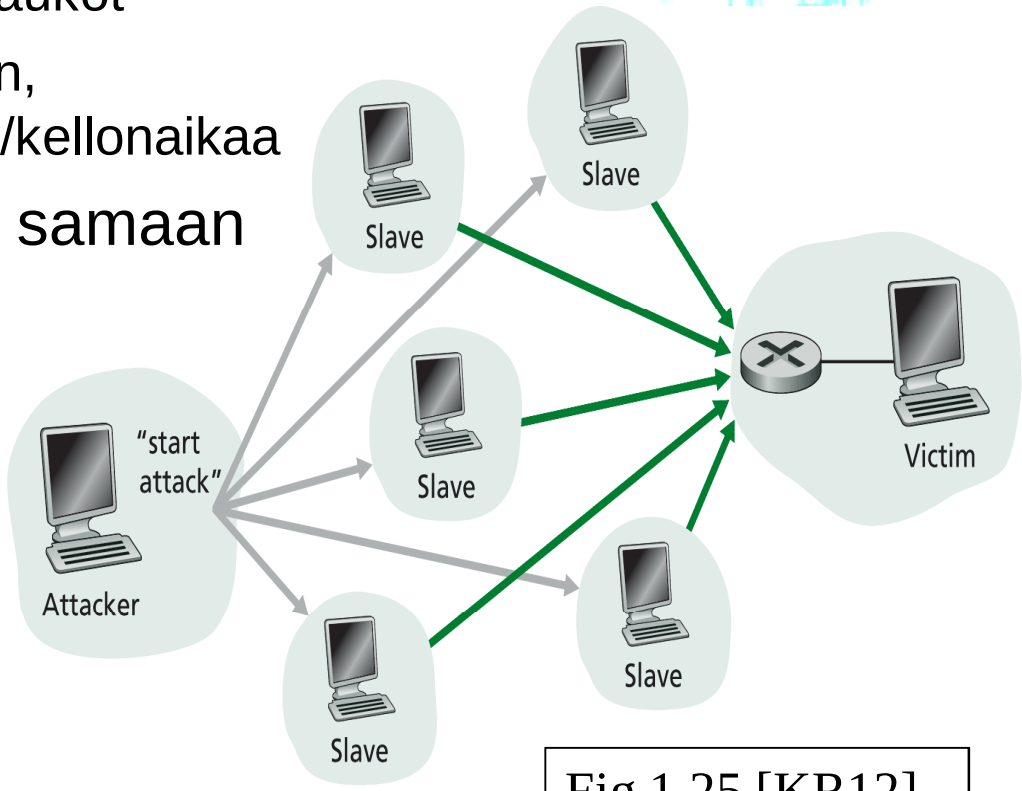
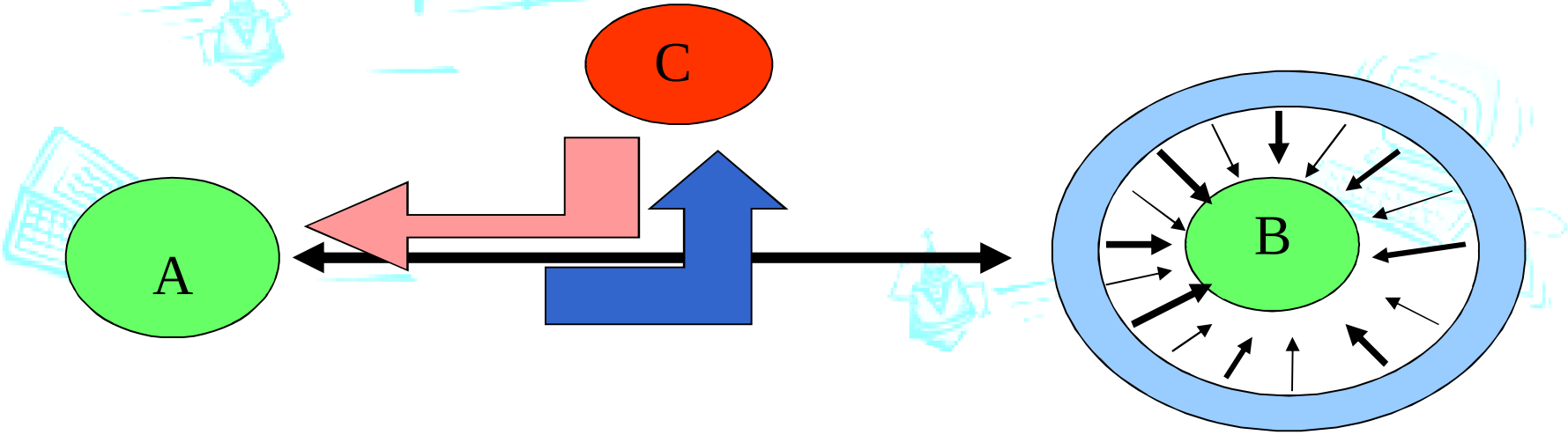


Fig 1.25 [KR12]

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

- **Mato**
  - Tulee tietoturva-aukosta ja leviää automaattisesti (Sasser) Slammer (2003 kaatoi 5 nimipalvelijaa))
  - Levinneimmät madot kulkivat sähköpostin liitetiedostoina
    - Morrisin mato (1988), Melissa (1999), Nimda (2001),Sobig (2003), ILoveYou,
  - Downadup (2007-2008): hyödyntää Microsoftin Windows-käyttöjärjestelmässä löytynyttä turvareikää, arvaa admin 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,
    - avata takaportin tai muun haavoittuvuuden tietojärjestelmään
    - tehdä tiedonhakua, tietojen tuhoamista tai vastaavaa jopa jättämättä mitään jälkiä.

Vastatoimet? (1)

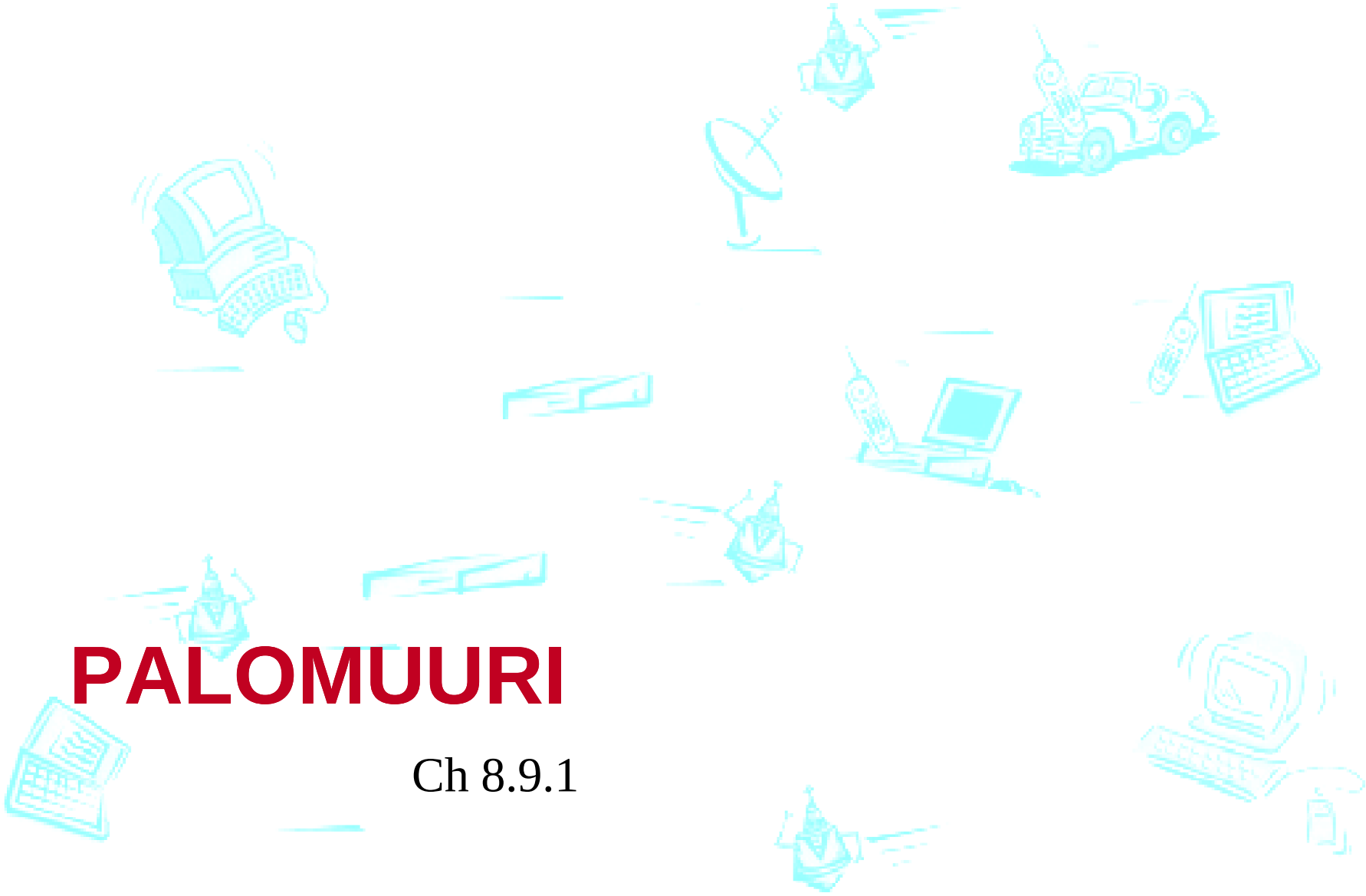
Pidä KJ:n turvapäivitykset ajan tasalla!

- 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)

HYVÄ TIETOLÄHDE:
www.cert.org

- Palvelunesto
  - Vaikea todeta / estää
  - Miloin SYN on oikea yhteyspyyntö, millloin osa hyökkäystä?
  - Hyökkäyksen havaitsemis- ja estämisjärjestelmät
  - SYN cookie
  - ISP Hotline
- Haittaohjelmat
  - Turva-aukkopäivitysten asentaminen heti
  - Varovaisuus sähköpostiliitteiden kanssa
  - Älä asenna tai käytä ’tuntemattomia’ ohjelmia
  - Käytä palomuuria ja virustorjuntaohjelmia



PALOMUURI

Ch 8.9.1

Palomuuri (firewall)

Palomuuri

Suodattaa (*filter*) liikennettä organisaation oman verkon (intranet) ja julkisen Internetin välillä. Päästää osan liikenteestä sisäverkkoon ja estää loput.

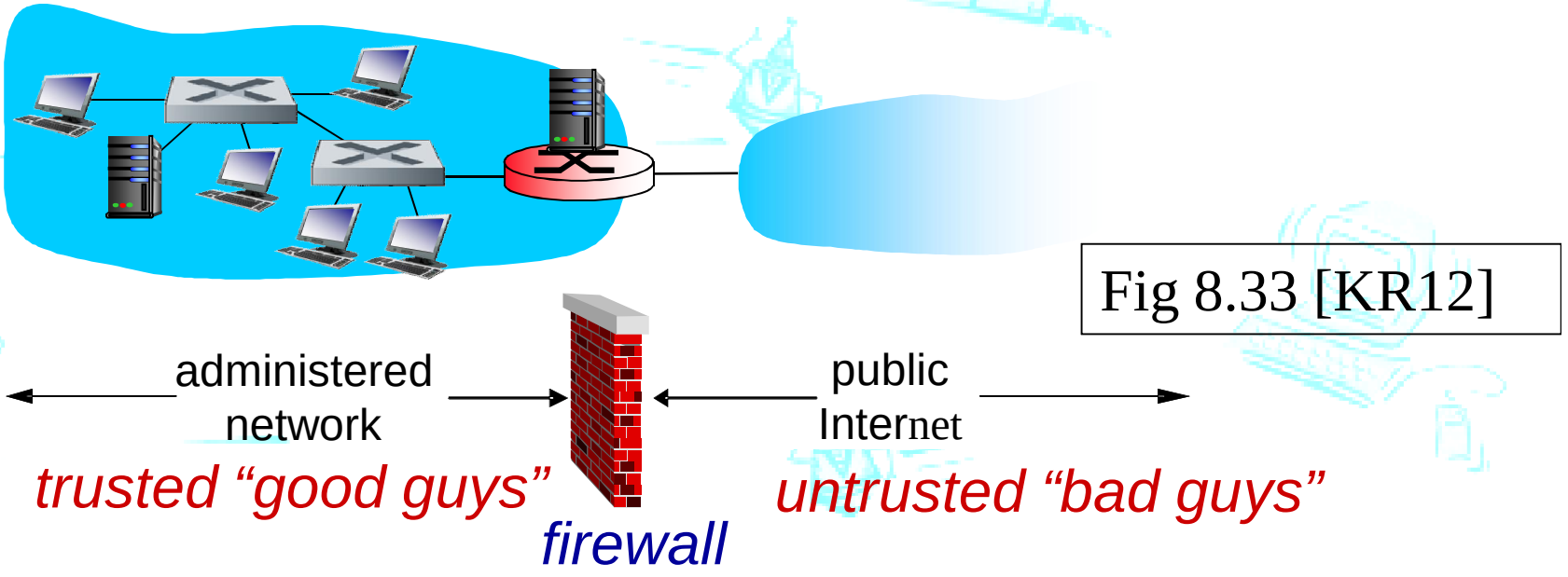


Fig 8.33 [KR12]

Miksi palomuureja?

Suojaa palvelunestohyökkäyksiltä:

- SYN tulvituksessa hyökkääjä yrittää luoda paljon vaillinaisia TCP-yhteyksiä, jolloin resursseja ei jää oikeille yhteyksille

Estää luvattoman sisäverkon tietojen lukemisen/muuttamisen

- esim. Hyökkääjä vaihtaa organisaation kotisivun sisällön

Sallii vain oikeiden käyttäjien pääsyn sisäverkkoon

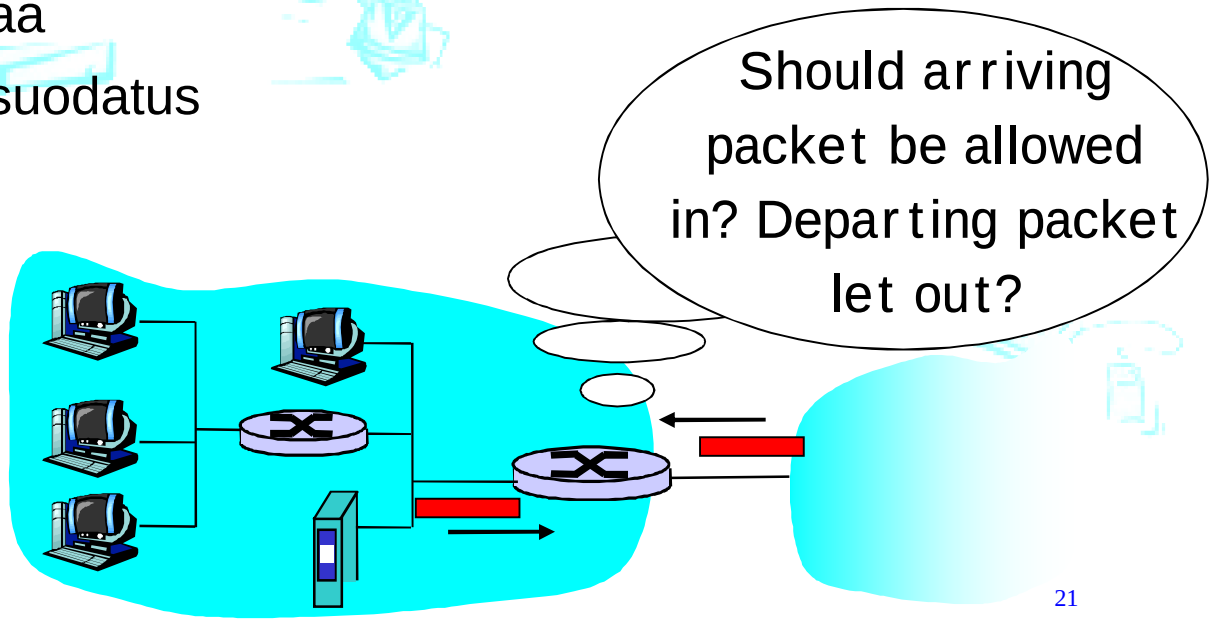
- joukko tunnistettuja käyttäjiä / palvelimia

Kaksi (tai kolme) palomuurityyppiä:

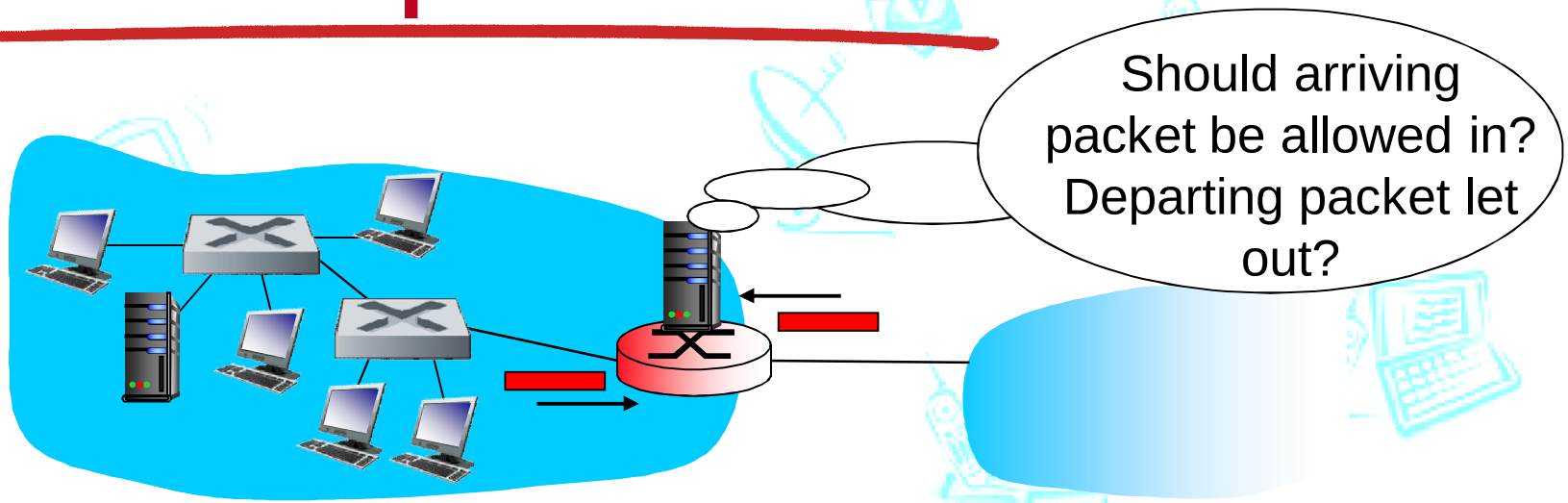
- Paketteja suodattava palomuuri (packet filtering)
  - Tilaton (stateless)
  - Tilallinen (stateful)
- Sovellustason yhdyskäytävä (application-level gateway)

Palomuurityypit

- **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



Tilaton pakettien suodatus



- Sisäverkko yhdistetty internetiin *reitittimen ja palomuurin yhdistelmällä (router firewall)*
- Reititin *suodattaa paketin kerrallaan,* sallii etenemisen tai pudottaa paketin
  - Ennalta määritellyt säännöt

Suodatussäännöistä

- 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

Esimerkkejä säännöistä

- Esim 1: Estä IP-pakettien liikenne (sisään/ulos), jos protokolla = 17 tai portti = 23
  - Palomuuri 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
  - Palomuuri hävittää kaikki ulkoa tulevat TCP-yhteyspyyntöpaketit
  - Oman verkon koneet voivat silti ottaa yhteyttä organisaation ulkopuolisiin palveluihin

Lisää esimerkkejä (tilaton suodatus)

Policy	*Firewall Setting*
No outside Web access.	Drop all outgoing packets to any IP address, port 80
No incoming TCP connections, except those for institution's public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
Prevent Web-radios from eating up the available bandwidth.	Drop all incoming UDP packets - except DNS and router broadcasts.
Prevent your network from being used for a smurf DoS attack.	Drop all ICMP packets going to a "broadcast" address (e.g. 130.207.255.255).
Prevent your network from being tracerouted	Drop all outgoing ICMP TTL expired traffic

Pääsynvalvontalistat (Access Control Lists, ACL)

- Taulukollinen sääntöjä (toimenpide+ehdot), joita sovelletaan järjestyksessä alusta loppuun. Esimerkkitaulu saapuville paketeille

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

Tilallinen pakettien suodatus
(Stateful packet filter)

- Säännöillä on hankala toteuttaa monimutkaisia estopolitiikkoja
  - Sääntöjä tarvitaan helposti paljon, jopa tuhansia
  - Niitä käydään läpi jossain järjestyksessä => väärä järjestys voi aiheuttaa ongelmia / virheitä paketin käsittelyssä
- Suodatus kohdistuu yksittäiseen pakettiin
  - Päästää tarpeettomasti läpi paketin porttiin 80, jossa ACK, silloinkin kun todellisuudessa TCP-yhteys puuttuu

action	source address	dest address	protocol	source port	dest port	flag bit
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK

Tilallinen pakettien suodatus
(Stateful packet filter)

- *Tilallinen pakettien suodatus(stateful packet filter):* pitää kirjaa kaikkien TCP-yhteyksien tilasta
  - Suodatin tietää, mitkä TCP-yhteydet ovat käytössä
  - Taulukko voimassa olevista TCP-yhteyksistä
  - SYN, SYNACK ja ACK => yhteys muodostetaan
  - FIN-paketit => yhteys puretaan / poistetaan,
  - Purku myös ajastimella, jos ei käytetä (60 s)
  - Esim. intranetistä lähetetty web-kysely => päästetään vastaus läpi

Tilallinen pakettien suodatus

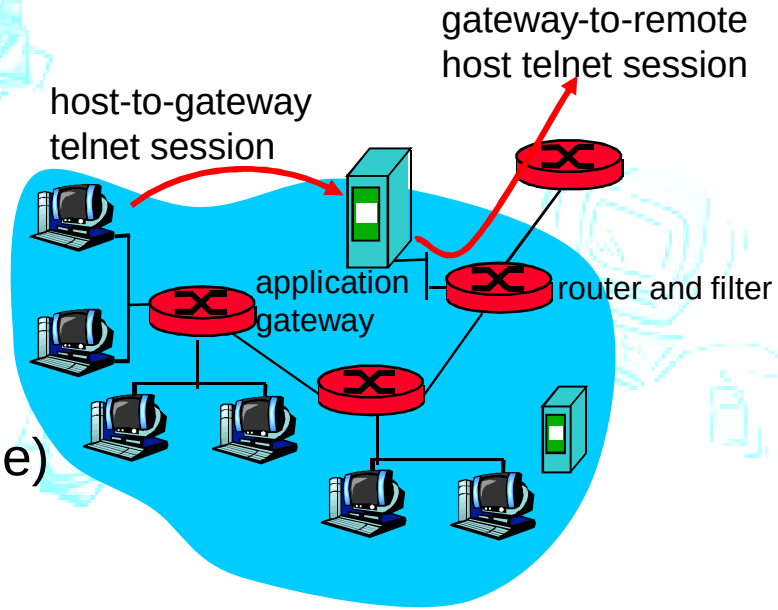
- Pääsynvalvontalistoihin (ACL) mukaan myös tieto pitääkö yhteyksien tilataulu (connection state table) tarkistaa ennen paketin hyväksymistä

action	source address	dest address	proto	source port	dest port	flag bit	check conxion
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	X
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	X
deny	all	all	all	all	all	all	

Sovellustason yhdyskäytävä
(Application gateway)

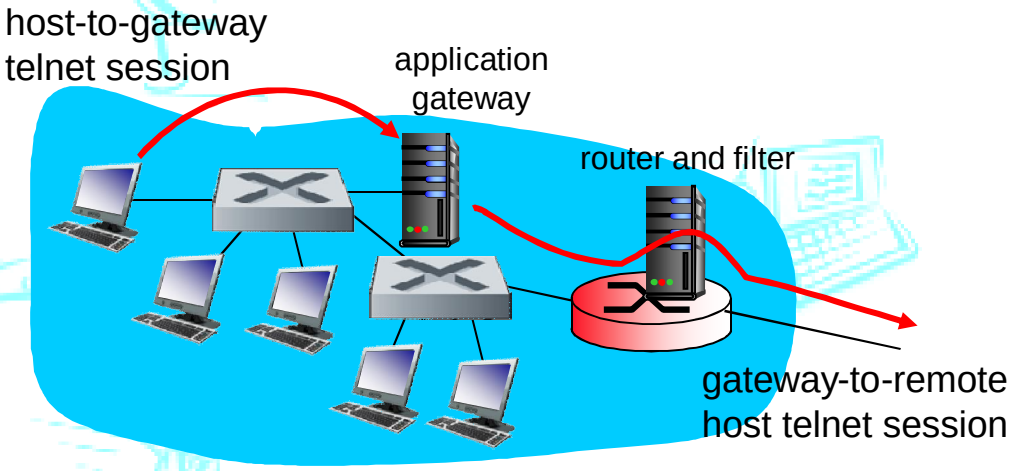
- **Kun halutaan hienojakoisempaa suodatusta**
  - Esim. Telnet-yhteyden salliminen tunnetuille käyttäjille, mutta näiden identiteetti on ensin todennettava
  - Tähän pelkkä IP/TCP/UDP-otsakkeiden tutkiminen ei riitä
- **Toimii välittävänä koneena (relay) sisäverkon ja Internetin välissä**
  - Eri sovelluksilla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

Fig 8.34 [KR12]



Sovellustason yhdyskäytävä

- Suodattaa paketteja sekä sovellusprotokollan että IP/TCP/UDP kenttien avulla.
- *Esim:* sallii valikoitujen sisäisten käyttäjien telnet- yhteydet ulos.



1. Vaatii kaikkia telnet-käyttäjiä käyttämään yhdyskäytävää.
2. Oikeutetuille käyttäjille muodostaa telnet-yhteyden kohdekoneelle. Yhdyskäytävä välittää tietoa näiden päätepisteiden välillä.
3. Reititin/palomuuri estää kaikki ulospäin menevät telnet-yhteydet, jotka eivät tule yhdyskäytäväkoneelta.

Palomuuri / 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!

Tasapainoilua tietoturvan tason ja ulkoisten yhteyksien määrän välillä

Tunkeilijan havaitsemisjärjestelmät (intrusion detection systems, IDS)

- Tavoitteena havaita alkaneita hyökkäyksiä
- Lähinnä kerää tietoa verkon liikenteestä

- *Tunkeilijan havaitsemisjärjestelmä (IDS)*
  - *Pakettien sisällöllinen analysointi:* Tutkii paketin datasisältöä, esim. etsii tunnettujen virusten tai hyökkäysten sormenjälkiä yms muita etukäteen tunnettuja malleja (pattern)
  - Tutkii korrelaatioita. Useiden pakettien suhteita, esiintymistä, yms. Etsii tilastollisia poikkeamia normaalista liikenteestä
    - Koputtelu, porttiskannaus (port scanning)
    - Verkon rakenteen selvitys (network mapping)
    - Palvelunestohyökkäys (DoS attack)

Tunkeilijan havaitsemisjärjestelmä

- Paljon erilaisia IDS-toteutuksia.
- **Snort** – avoimen lähdekoodin toteutus

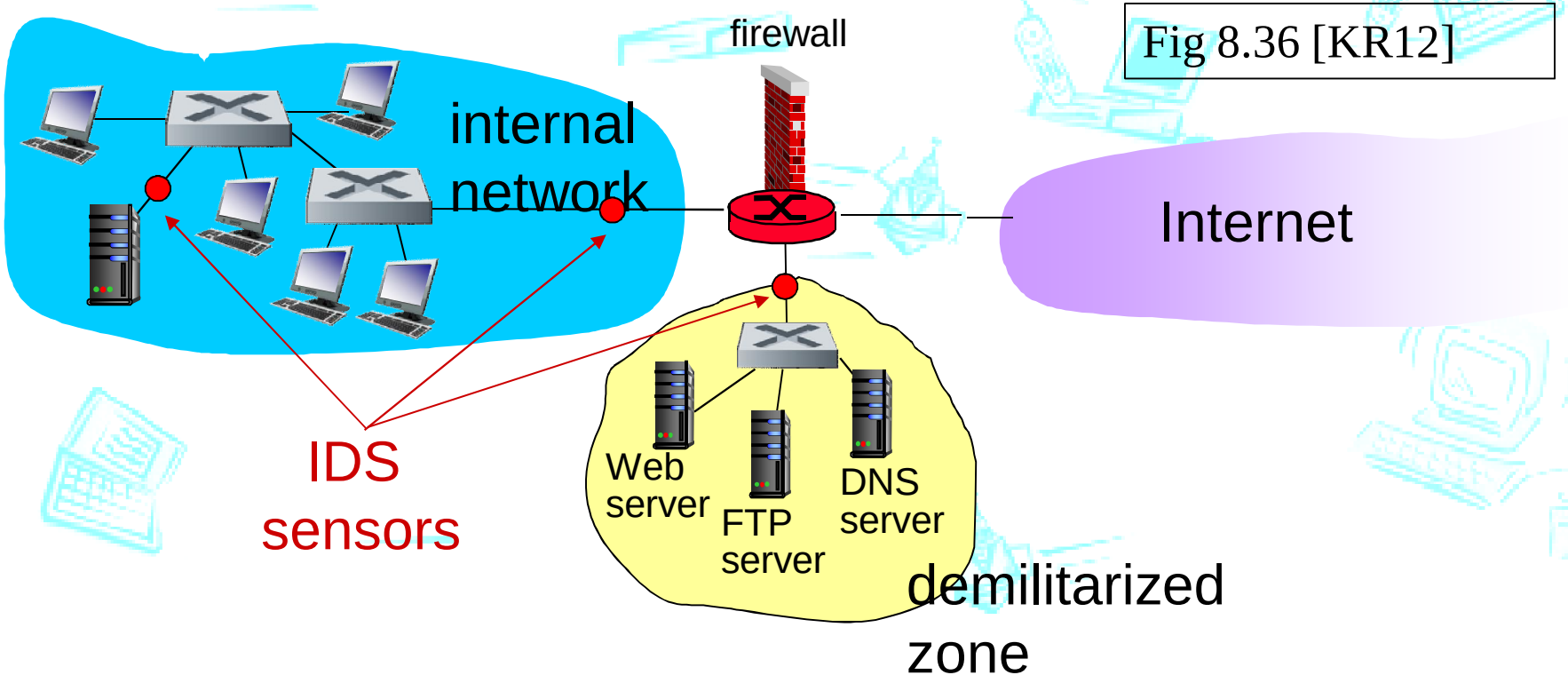


Fig 8.36 [KR12]

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://ohjelmistojakelu.helsinki.fi -antivirus
- Muitakin ilmaisia ohjelmia löytyy

- Viestintäviraston kyberturvallisuuskeskus:
  - Seuraa tiedotuksia: https://www.viestintavirasto.fi/tietoturva.html
  - Myös www.tietoturvaopas.fi vie samalle sivulle

LINKKIKERROS: WEP

WEP

- ÄLÄ KÄYTÄ, jos haluat suojatun yhteyden!
  - Suojausmenetelmä murrettu jo 2001
  - Nopeampi purkualgoritmi jo 2007
  - Myös WPA on murrettu
- Valitse linkkikerrokselle vahvin tarjolla oleva!
- WEP parempi kuin ei mitään, mutta vain hiukan

- Käytämme esimerkkinä, koska se on riittävän yksinkertainen kuvaamaan linkkikerroksen salauksen toimintaidean

WEP lähtökohta

- Symmetrisen avaimen salaus
  - Luottamuksellisuus (confidentiality)
  - Käyttöoikeus (end host authorization)
  - Tiedon eheys
- Jokainen paketti salataan erikseen
  - Kun tunnetaan avain ja salattu paketti, voidaan paketti purkaa vaikka edellinen paketti olisikin kadonnut (siis ei ketjuteta kuten Cipher Block Chaining(CBC))
- Tehokkuus
  - Toteutettavissa laitteistolla tai ohjelmistolla

Symmetrinen jonosalaus (symmetric stream cipher)

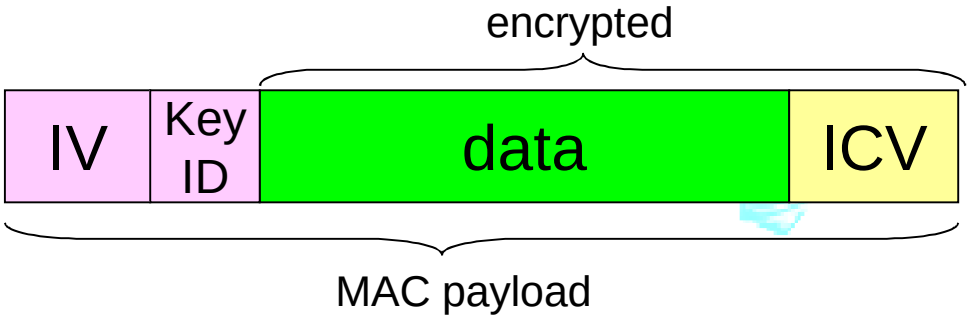
- *Yhdistetään tavuittain (kukin tavu erikseen) jonosalaimen ja selväkielisen viestin tavut salatuksi viestiksi*
- Jonosalausta käytetään tilanteissa, joissa salauksen on oltava nopeaa ja reaaliaikaista tiedon synnyn kanssa
- Jonosalausta ei pidetä täysin turvallisena
- WEPin käyttämä RC4 on tunnetuin

Jonosalaus ja pakettien riippumattomuus

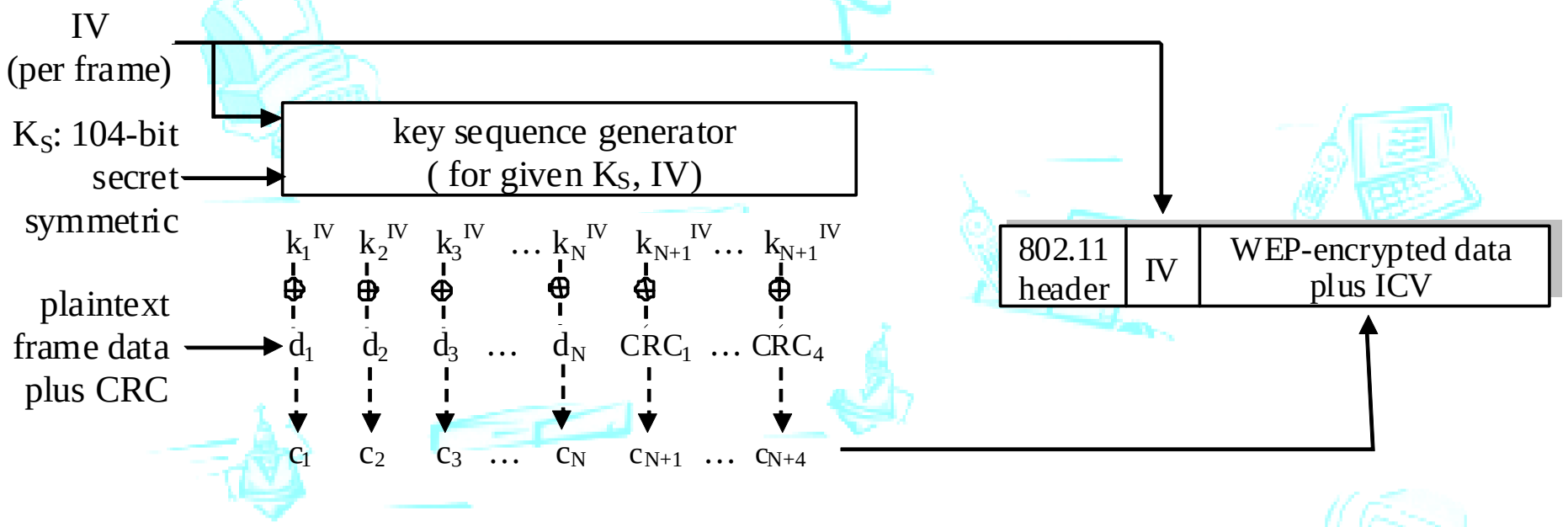
- Kukin paketti salataan erikseen, ei saa ketjuttaa
- Jos kehykselle n+1 käytetään jonosalainta siitä kohtaa mihin kehyksen n jälkeen jäätiin, eivät kehykset olekaan salattuina riippumattomia
- WEP: generoidaan jonosalain kullekin paketille erikseen käyttäen syötteenä avainta ja paketin omaa uutta alustusvektoria (initialization vector, IV)

WEP salaus (1)

- Lähettäjä laskee datalle eheystarkisteen (Integrity Check Value, ICV)
- Kummallakin käytössä 104-bittinen jaettu avain
- Lähettäjä luo 24-bittisen alustusvektorin (IV), katenoi sen avaimen kanssa ja saa näin 128-bittisen avaimen
- Lähettäjä vielä katenoi mukaan avaintunnisteen keyID (8-bittinen)
- 128-bittinen avain on siemen näennäissatunnaislukuja tuottavalle funktiolle, nämä luvut muodostavat jonosalaimen
- Kehyksen data ja eheystarkiste salataan käyttäen RC4:ää
  - Jonosalaimen ja data(+ICV)n tavut XOR:illa yhteen
  - 802.11 Kehyksen data-alueelle (payload): IV, KeyID ja salattu data+ICV



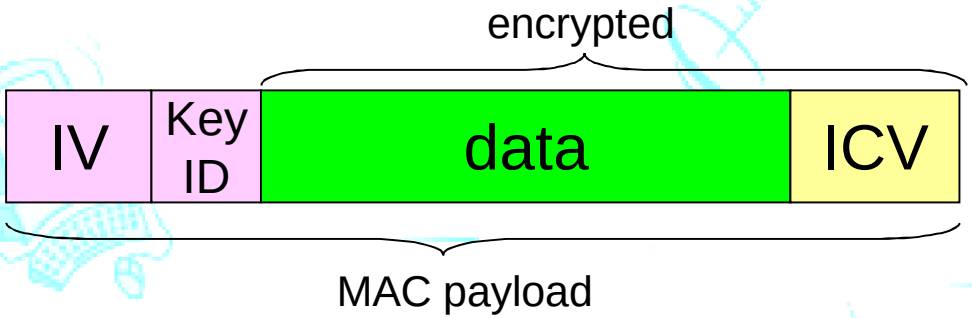
WEP salaus (2)



uusi IV kullekin kehykselle

m(i) = ith unit of message
ks(i) = ith unit of keystream
c(i) = ith unit of ciphertext
c(i) = ks(i) ⊕ m(i) (⊕ = exclusive or)
m(i) = ks(i) ⊕ c(i)

WEP salauksen purku



- Vastaanottaja erottaa IV:n
- Muodostaa avaimesta ja IV:stä siemenen näennäissatunnaislukugeneraattorille ja saa jonosalaimen
- XOR puretaan vain tekemällä se uudelleen, eli XOR (salattu data, jonosalain)
- Tarkistaa datan eheystarkisteen ICV
  - HUOM: datan eheyden käsite on hiukan erilainen kuin allekirjoituksissa ja viestien todentamisessa (MAC).

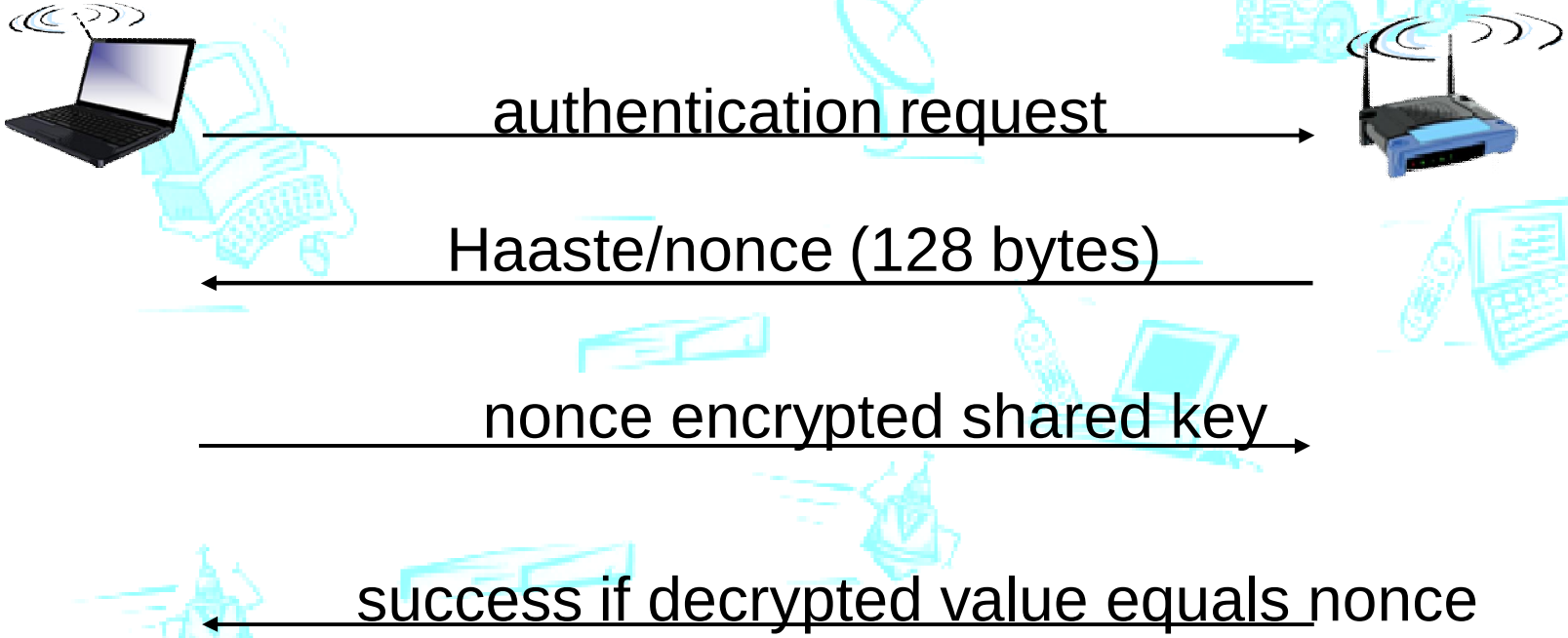
Vastapuolen todentaminen haasteella

Haaste: numero (R) jota *käytetään vain kerran*

Kuinka todentaa Alicen "olemassaolo": Bob lähettää haasteen R. Alicen täytyy palauttaa haaste R salattuna jaetulla salaisella avaimella

Alice on olemassa ja koska Alice on ainoa joka tietää salaisen avaimen, vastapuolen täytyy olla Alice!

WEP todentaminen



Huom:

- Kaikki tukiasemat (AP) eivät käytä, vaikka WEP käytössä
- Tukiasema kertoo todentamistarpeen merkkikehyksessä
- Tehdään ennen yhdistämistä (association)

802.11 WEP salauksen murtaminen

Turva-aukko (security hole):

- 24-bittinen IV, yksi IV kehyksessä, -> IV:n uudelleenkäyttö
- IV siirretään salaamatta -> IV:n uudelleenkäyttö voidaan havaita

Hyökkäys:

- Hyökkääjä houkuttelee lähettäjän lähettämään jokin tunnettu viesti $d_1\ d_2\ d_3\ d_4$ …
- Hyökkäjä havaitsee: $c_i = d_i$ XOR k_i^{IV}
- Hyökkääjä tietää $c_i\ d_i$, joten voi laskea k_i^{IV}
- Hyökkääjä tietää nyt jonosalaimen $k_1^{IV}\ k_2^{IV}\ k_3^{IV}$ …
- Kun IV käytetään uudelleen, hyökkääjä voi purkaa viestin!

802.11i = WPA2: parannetaan turvallisuutta

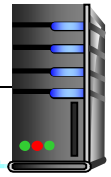
- Otetaan käyttöön vahvempi salausmenetelmä
  - Näitä on paljon tarjolla
  - WPA2:ssa käytössä AES –lohkosalaus
- Huolehditaan avaintenjakelusta
- Käyttäjän todentaminen ei tukiaseman tehtävä, vaan erillinen toiminnallisuus
- WPA2 on nykyinen käytössä oleva langattomien yhteyksien salausmenetelmä
  - Käytä tätä – muut liian heikkoja!

802.11i: nelivaiheinen toiminta

STA: client station

AP: access point

wired network



AS: Authentication server

1 Discovery of security capabilities

2 STA and AS mutually authenticate, together generate Master Key (MK). *AP serves as "pass through"*

EAP

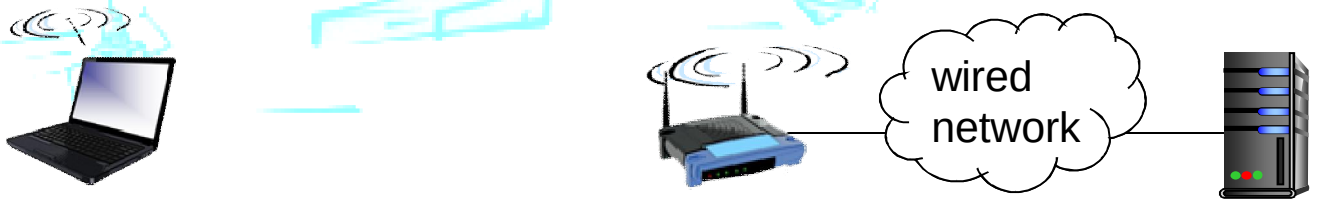
3 STA derives Pairwise Master Key (PMK)

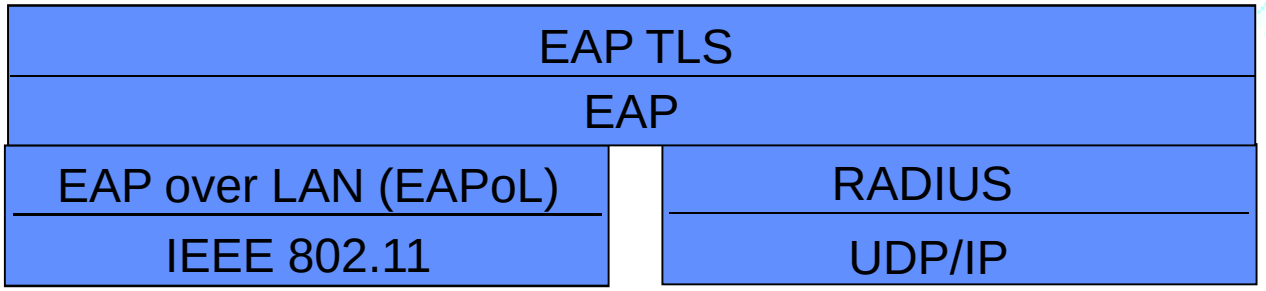
3 AS derives same PMK, sends to AP

4 STA, AP use PMK to derive Temporal Key (TK) used for message encryption, integrity

Laajennettava autentikointiprotokolla (extensible authentication protocol, EAP)

- EAP: (langattomien) asiakkaiden ja todentamispalvelimen välinen protokolla
- EAP voidaan välittää erillisten linkkien yli
  - Mobiililaitteelta tukiasemalle: EAP over LAN
  - Tukiasemalta autentikointipalvelimelle: RADIUS over UDP





WPA2:n heikkous

- Koskee vain WPA2:n käyttöä laitteissa, jossa on myös **Wi-Fi Protected Setup (WPS)**
- Wikipediasta suoraan: ”A major security flaw was revealed in December 2011 that affects wireless routers with the WPS PIN feature, which most recent models have enabled by default. The flaw allows a remote attacker to recover the WPS PIN in a few hours with a brute-force attack and, with the WPS PIN, the network's WPA/WPA2 pre-shared key.[4] Users have been urged to turn off the WPS PIN feature,[5] although this may not be possible on some router models.”
- Suunnitteluvirhe, ainoa suojautumiskeino: Estä WPS!

Verkon tietoturva - yhteenveto

Perustekniikat…...

- kryptografia (symmetrinen salaus ja julkisen avaimen järj.)
- Viestien eheys ja viestinnän luottamuksellisuus
- Osapuolien todentaminen

…. käytössä useissa erilaisissa protokollatoteutuksissa

- Turvallinen sähköposti
- secure transport (SSL&TLS)
- IPsec
- 802.11 (WPA2)

operational security: firewalls and IDS

Kertauskysymyksiä

- Kryptografian periaatteet?
- Symmetrisen avaimen / julkisen avaimen salaus?
- Avaintenvaihtoprotokollat?
- Salaus ja suojausprotokollat?
- Palomuuri?
- Tietoturvan uhat?
- Suojautusmiskeinoja?

ks. kurssikirja s. 770-772