

Langattomat lähiverkot - tietoturvaratkaisut

Toni Sallanmaa

Langattomat lähiverkot

- ▶ Määritelty IEEE 802.11 –standardissa, eri versioita
- ▶ Käyttävät radioverkkoa siirtomediana
- ▶ Koostuvat tukiasemista ja asiakkaista
- ▶ Verkko ei ole luotettava, siirtomedia jaetaan
- ▶ Verkko tunnustetaan SSID-nimellä

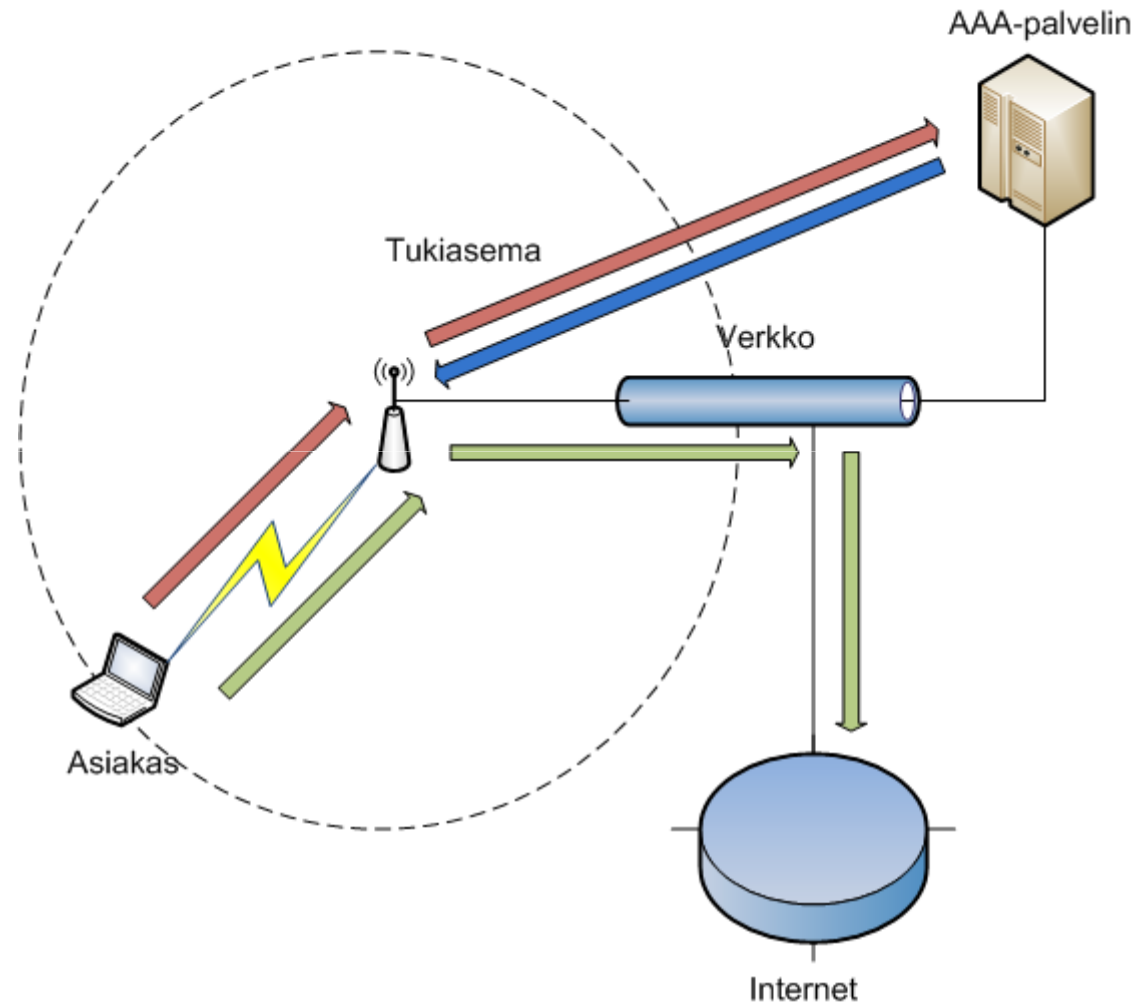


Tietoturvaratkaisut (I)

- ▶ Fyysinen turva puuttuu
- ▶ Salainen SSID-nimi, staattinen IP-osoite ja MAC-suodatus
- ▶ Wired Equivalent Privacy (WEP), puutteellinen toteutus, nopeasti murrettavissa
- ▶ 802.1X porttiantentikaatio käyttää AAA-palvelinta ja toimii WLAN-suojauksien kanssa



802.1X-porttiautentikaatio



Tietoturvaratkaisut (II)

- ▶ WPA on rakennettu WEP:n pohjalta ja sisältää samat algoritmit, myös Pre-Shared Key –tila
- ▶ WPA2 on uusi toteutus ja sisältää paremmat algoritmit, ei taaksepäin yhteensopiva
- ▶ HTTP-autentikointi toimii palomuurin avulla, hyvä vain rajatuissa tilanteissa
- ▶ Palvelunestohyökkäykset, Man in the middle, session hijacking, MAC spoofing



Käyttötapaukset (I)

- ▶ Esimerkkitapauksia
- ▶ Kotikäyttäjät
 - ▶ Vähän salattavaa tietoa, helppo liitettävyys verkkoon, vähän rahaa käytettävissä, helppo ylläpito
 - ▶ Salainen SSID, MAC-suodatus ja staattinen IP liian vaikeita
 - ▶ WEP liian heikko turvaltaan
 - ▶ WPA tai WPA2 PSK-tilassa hyvä ratkaisu



Käyttötapaukset (II)

▶ Yrityskäyttäjät

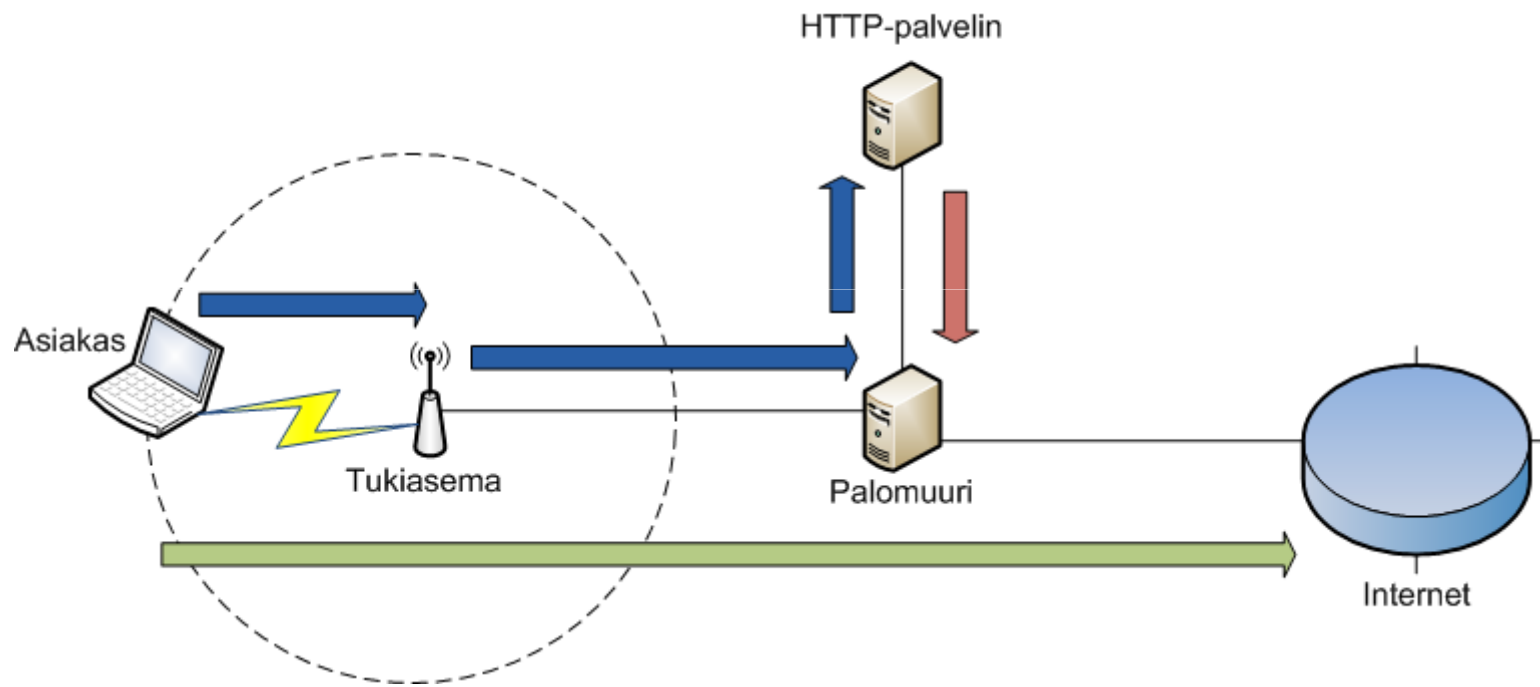
- ▶ Salattavaa tietoa, ylläpitohenkilöstö, verkon saatavuus, verkkoliikenne täytyy salata
- ▶ Ratkaisutapoja: Ei verkkoa tai VPN-rajoitettu verkko
- ▶ WPA ja WPA2, myös AAA-palvelimella

▶ Kahvilat ja vastaavat palveluntarjoajat

- ▶ Internetpalvelu vain oheistuote
- ▶ Ei tarvetta salata verkkoliikennettä, liikenteen rajoittaminen, maksamattomat asiakkaat
- ▶ HTTP-autentikaatio, WPA tai WPA2



HTTP-autentikaatio



Yhteenveto

- ▶ Paljon puutteellisia ratkaisuja
- ▶ WPA ja WPA2 yleensä riittävän varmoja, muut murrettavissa helpommin
- ▶ 802.1X tarjoaa käyttäjäkohtaisen palvelun
- ▶ Suojaus vaadittavan tietoturvan ja kustannusten mukaan

