Langattomien verkkojen tietosuojapalvelut

Juha Kalm

Valvoja: Prof. Jorma Jormakka

Ohjaaja: FM Kari Lehtinen

Sisältö

- Työn tausta & tavoitteet
- Käytetty metodiikka
- Työn lähtökohdat
- IEEE 802.11 –verkkojen tietoturva
- Keskeiset tulokset
- Demonstraatiojärjestelmä
- Oman työn osuus
- Johtopäätökset

Työn tausta

- Langattomien verkkojen käyttö yleistyy jatkuvasti
- Entisten piirikytkentäisten verkkojen sijaan uudet verkot useimmiten pakettikytkentäisiä
- Sekä paikalliset langattomat verkot, että etätyöyhteydet ja niihin liittyvät päätelaitteet suojattava
- Ratkaisun tulee olla riippumaton access mediasta (WLAN, GPRS, UMTS etc.)

Työn tavoitteet

- Kartoittaa olemassa olevat tekniikat langattomien verkkojen turvaamiseksi
- Valita ratkaisu, annettujen reunaehtojen puitteissa, jatkokehittelyä varten
- Rakentaa ja raportoida valittu ratkaisu

Käytetty metodiikka

- Reunaehtojen määrittely
- Kirjallisuustutkimus
- Olemassa olevan järjestelmän evaluointi
- Demonstraatiojärjestelmän suunnittelu, rakennus ja evaluointi

Työn lähtökohdat 1/2

- Langattomien verkkojen avoin luonne aiheuttaa ongelmansa
  - Selkeät rajat puuttuvat
    - Liikenteen kuuntelu useissa tapauksissa helppoa
    - DoS –hyökkäyksien esto lähes mahdotonta, mutta havaitseminen tyypillisessä tapauksessa helppoa
  - Pääsynvalvonta ja salaus kriittisiä, koska itse verkkoa on käytännössä mahdotonta erottaa ympäristöstä

Työn lähtökohdat 2/2

- Etäyhteyskäyttö on yleistynyt
  - Etenkin pakettikytkentäiset yhteydet yleistyneet
    - Perinteiset soittosarjat eivät ole käyttökelpoisia
    - Pakettikytkentäisten verkkojen fyysinen terminointi yrityksen omaan tietoliikenneverkkoon ei ole usein taloudellisesti järkevää
  - Uudet matkapuhelinteknologiat mahdollistavat entistä nopeammat etäyhteydet myös mobiilisti
    - Etätyöyhteyksiä halutaan käyttää myös tienpäältä

IEEE 802.11 –verkkojen tietoturva

- IEEE 802.11b –standardin mukaisia WLAN -verkkoja on käytetty jo vuosia
- WLAN –verkkojen tietoturvataso on havaittu riittämättömäksi
  - -Käyttäjien ja ylläpitäjien toimet
  - -Tekniset rajoitukset
  - -Tekniikassa ilmenneet viat

Käyttäjien ja ylläpitäjien toimet

- Langattomien verkkojen suurimpana tietoturvaongelmana on edelleen käyttäjän ja ylläpidon toiminta
  - Merkittävä osa liikenteestä salaamatonta
  - Pääsynvalvontalistoja ei ylläpidetä (MAC)
  - Verkkonimi julkisena jne.
- Pahimmassa tapauksessa luvaton käyttö voi tapahtua jopa tahattomasti

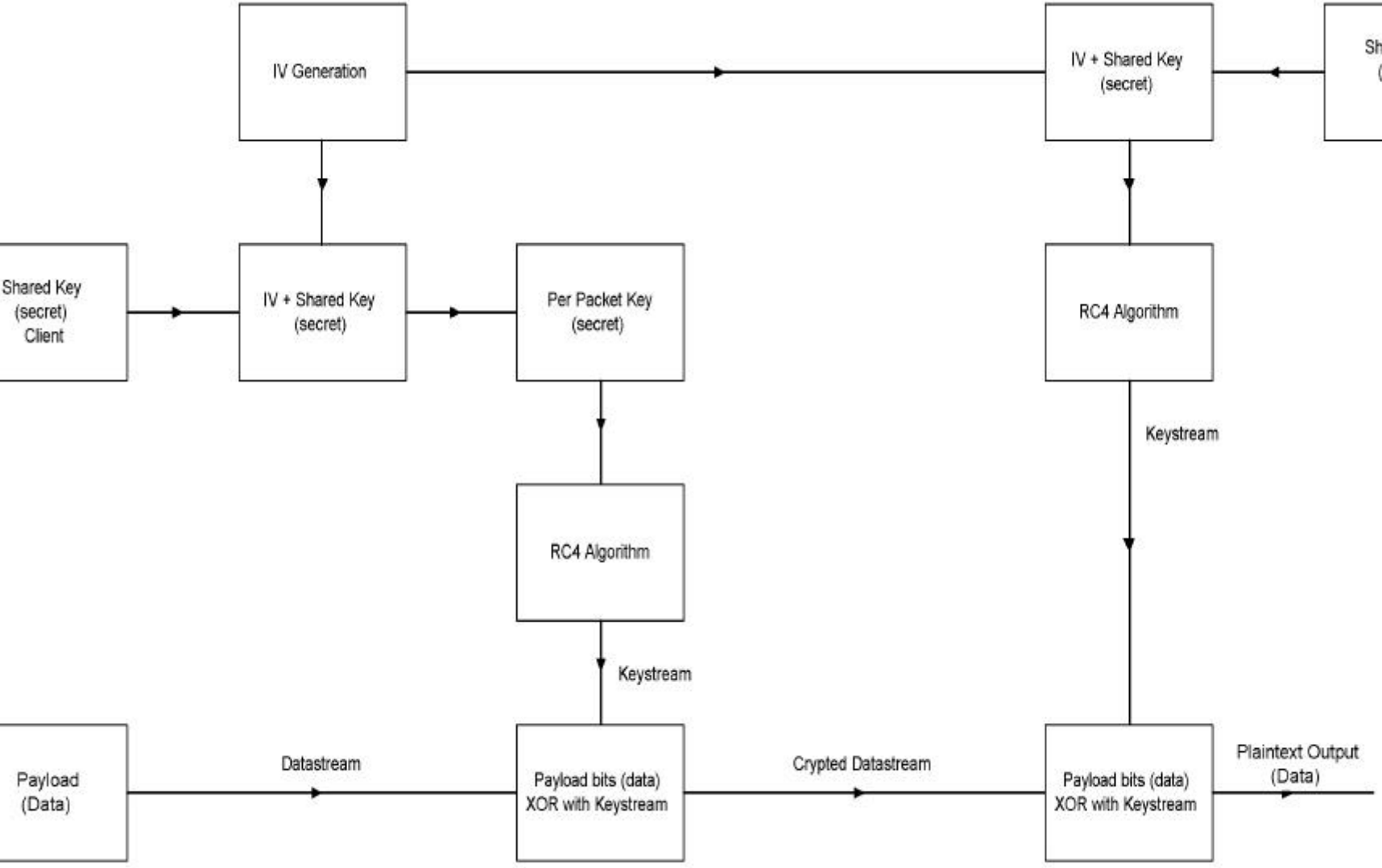
Tekniset rajoitukset 1/2

- Avoin taajuusalue
- Millä tahansa WLAN –kortilla varustetulla koneella voidaan oletusarvoisesti liittyvä verkkoon
- Verkot, enemmän tai vähemmän, julkisesti näkyviä (SSID)
- Vahvan autentikoinnin toteuttaminen standardin puitteissa hankalaa

Tekniset rajoitukset 2/2

- WEP –salaus alun perin 40 bittinen +IV
- WEP –salauksen heikkoudet
  - Salauksen tekninen toteutus heikko
    - Askeltava initialisointivektori
    - Heikot IV:t helpottavat salauksen murtamista (tilastolliset menetelmät)
  - Staattiset salausavaimet hankaloittavat ylläpitoa
- Salauksen toteutuksessa valmistajasta riippuvia ratkaisuja

WEP -salaus


IV Generation
IV + Shared Key (secret)
Shared Key (secret) AP
Shared Key (secret) Client
IV + Shared Key (secret)
Per Packet Key (secret)
RC4 Algorithm
Keystream
RC4 Algorithm
Keystream
Payload (Data)
Datastream
Payload bits (data) XOR with Keystream
Crypted Datastream
Payload bits (data) XOR with Keystream
Plaintext Output (Data)

Tekniset rajoitukset ovat vähenneet

- 40bit => 104bit WEP (+IV)
- Initialisointivektorien valinta kehittynyt
  - askellus => satunnainen => WKA (Weak Key avoidance) eli heikot IV:t ohitetaan
  - Tunnettujen heikkojen avainten määrä kasvanut
- Suljetut verkot (SSID:tä ei yleislähetetä)
- MAC – ja protokollasuodatus yleistyneet

Tekniikassa ilmenneet viat

- WEP –salaus haavoittuvainen hyökkäyksille
  - Etenkin alkuperäinen toteutustapa (40bit WEP yhdistettynä askellus IV:n käyttöön) helppo murtaa
- Suljettu verkko ei todellisuudessa ole suljettu (SSID edelleen selväkielisenä)
- Pääte- ja asiakaslaitteiden tietoturvaominaisuudet usein riittämättömiä

Keskeiset tulokset / WEP

- WEP –salauksen käyttö järkevää ja riittävän turvallista seuraavien reunaehdoin
  - 104bit + IV aidosti satunnaiset salausavaimet
  - Kaikissa verkon päätelaitteissa täysi WKA tuki
  - Tiukka salausavainten hallinta
  - Suljetun verkon ja MAC suodatuslistojen käyttö
  - Verkon toiminta-alueen rajaaminen
  - Verkon käyttäjiä korkeintaan joitakin kymmeniä

Keskeiset tulokset / WPA

- WPA salaa liikenteen riittävän hyvin, mikäli PSK (Pre-Shared Key) aidosti satunnainen
- Ei aidosti standardoitu menetelmä
  - yhteensopivuusongelmat & kompromissit
  - tullaan korvaamaan IEEE 802.11i protokollalla
- WEP:n tavoin toimii ainoastaan WLAN – verkoissa
- Sopii käytettäväksi pienehköissä verkoissa yhtenäisellä laitealustalla

Keskeiset tulokset / IPsec + PKI

- Suojaustaso toteutettavissa tunnetusti vahvoilla algoritmeilla
- Standardoitu ratkaisu
  - Ei sitouduta tietyn valmistajan tuotteisiin
  - Eri ohjelmistojen ja laitteiden ristiin käyttö mahdollista
  - Sekä ohjelmisto- että laitteistopohjaisia ratkaisuja

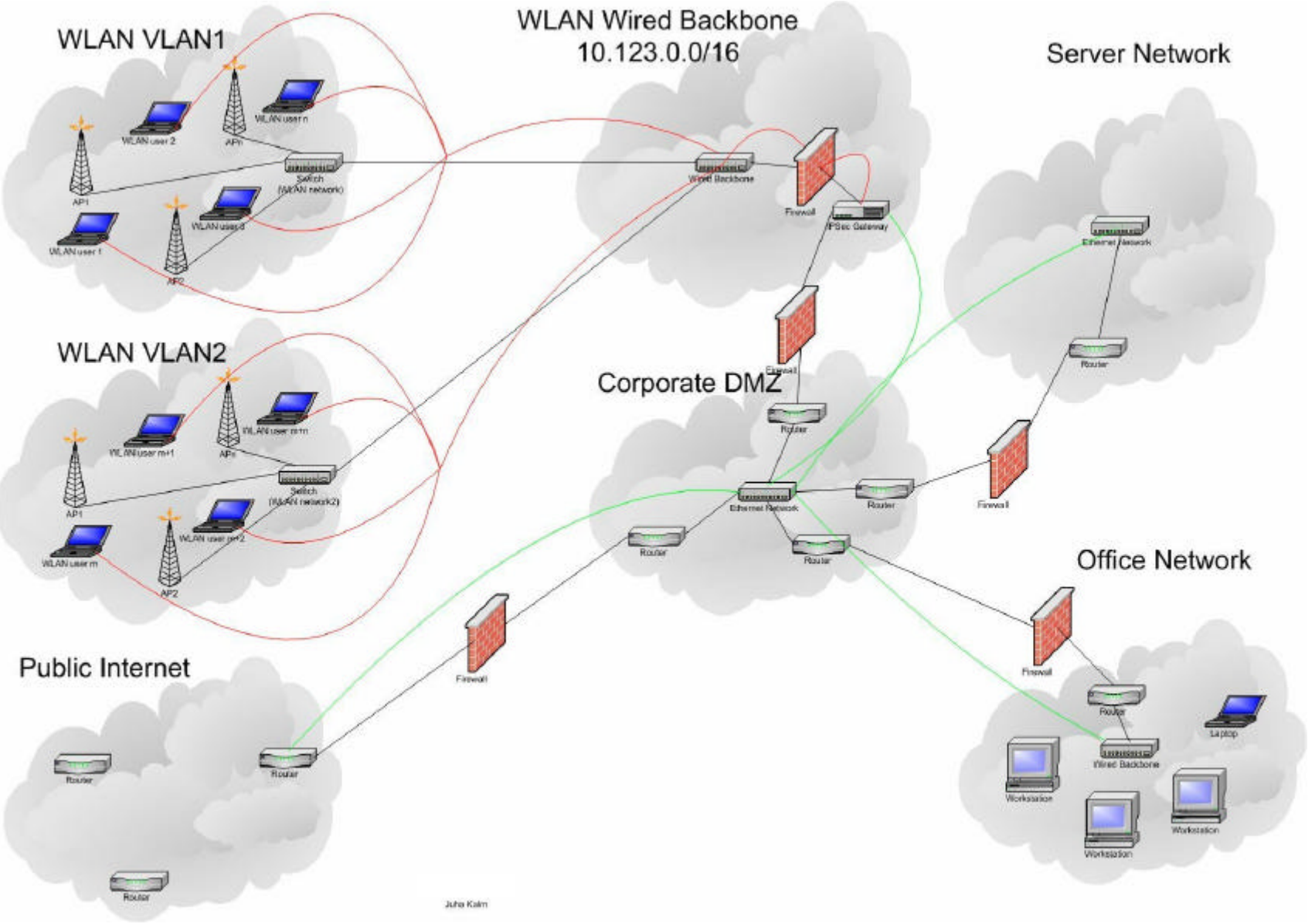
Keskeiset tulokset / IPsec + PKI 2

- Ratkaisu käytännössä täysin riippumaton liityntätekniikasta
  - -Suojaus toteutettu IP –protokollan päälle
  - ⇒Sopii käytettäväksi mm. WLAN, Hiperlan, GPRS ja UMTS –verkoissa
  - ⇒Mahdollistaa myös etätyöyhteydet (esim. ADSL tai ADSL + WLAN)
- Mahdollistaa myös laajojen verkkojen suojaamisen (useita tuhansia käyttäjiä)

Demonstraatiojärjestelmä

- Tavoitteena kehittää toimiva ratkaisu langattomien verkkojen tietoturvan toteuttamiseksi
  - Liityntätekniikasta riippumaton ratkaisu
  - Rakennettavan järjestelmän oltava kaikilta osiltaan riippumaton valmistajasta
  - Yhteensopivuus käytetyn PK –infrastruktuurin kanssa
- Rakentaa demonstraatiojärjestelmä testien pohjaksi
- Raportoida rakennettavan järjestelmän ominaisuudet ja mahdollisuudet

IPsec GW


WLAN VLAN1
WLAN Wired Backbone
10.123.0.0/16
Server Network
WLAN VLAN2
Corporate DMZ
Public Internet
Office Network
Juha Kalm

Oman työn osuus

- Kirjallisuustutkimus
- Testiverkon suunnittelu, rakennus ja raportointi
- IPsec –protokollaan pohjautuvan järjestelmän suunnittelu olemassa olevaa PKI –infrastruktuuria hyödyntämällä
  - Ohjelmistopohjainen ratkaisu (Super FreeS/WAN)
  - Laitteistopohjainen ratkaisu (Cisco)
- Osallistuminen ohjelmistopohjaisen järjestelmän rakentamiseen
- Asiakasohjelmiston asetusten määrittelyn suunnittelu ja toteutus

Johtopäätökset

- Pienimuotoisissa verkoissa joissa tietoturvan taso ei ole kriittinen on WEP ja WPA edelleen käyttökelpoisia tekniikoita kunhan niiden rajoitukset ymmärretään
- Laajemmissa verkoissa IPsec & PKI käyttökelpoisempi ja turvallisempi
  - Parempi tietoturva
  - Laitteistoriippumattomuus tuo joustavuutta
  - Käyttäjien hallinta helpompaa
- Käyttäjä on edelleen heikoin lenkki