T-79.4501
Cryptography and Data Security

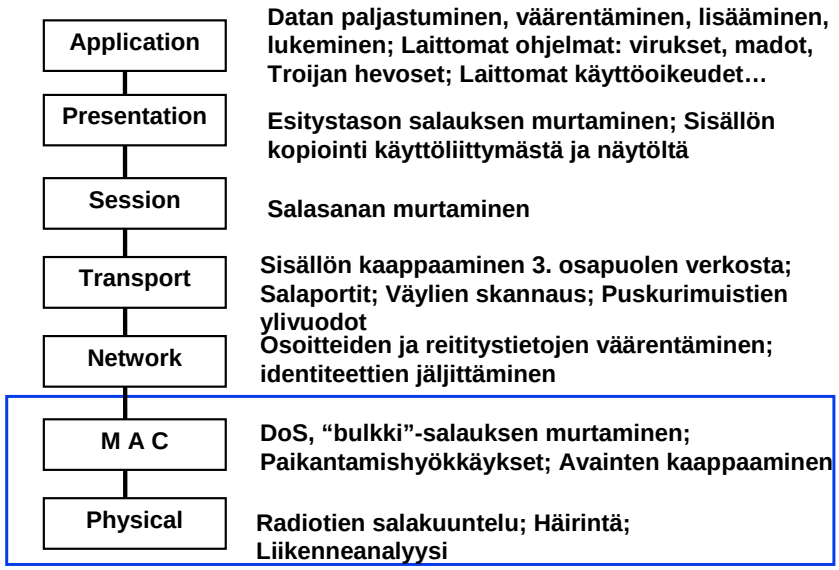
Lecture 11

Bluetooth Security

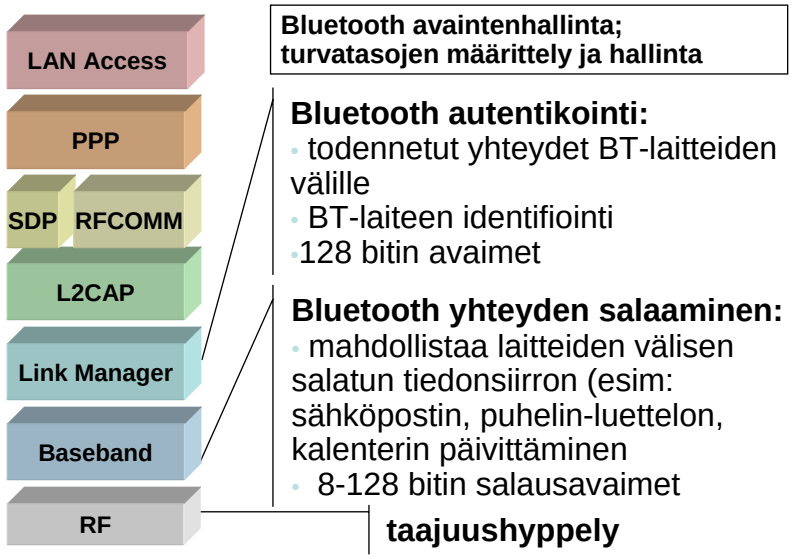
Bluetooth turvallisuus

- Uhkakuvat
- Bluetooth turvallisuuden tavoitteet
- Linkkitason turvamekanismit
  - Pairing menettely
  - Autentikointi ja salausavainten luonti
  - Algoritmit

Kommunikaatioverkkojen turvallisuusuhkia



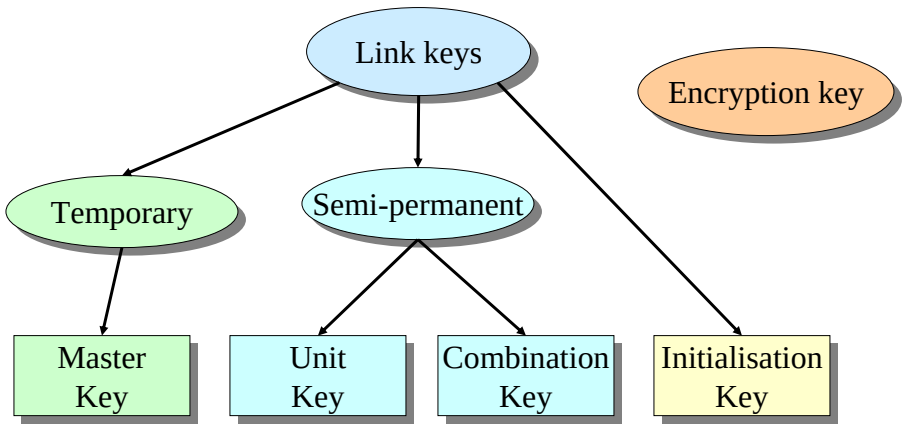
Turvaaminen Bluetoothissa



Turvallisuus
päästä päähän vai linkkikerroksessa?

- Bluetooth tarjoaa linkkikerroksen turvallisuusratkaisut
- Käytännön sovellukset vaativat usein turvaamista päästä päähän
  - dial-up yhteydet palvelimelle (IPSEC)
  - sähköposti (PGP,S/MIME)
  - webbiselain sovellukset (TLS)
- Bluetooth SIG suosittelee myös korkeampien kerrosten turvaratkaisujen käyttämistä

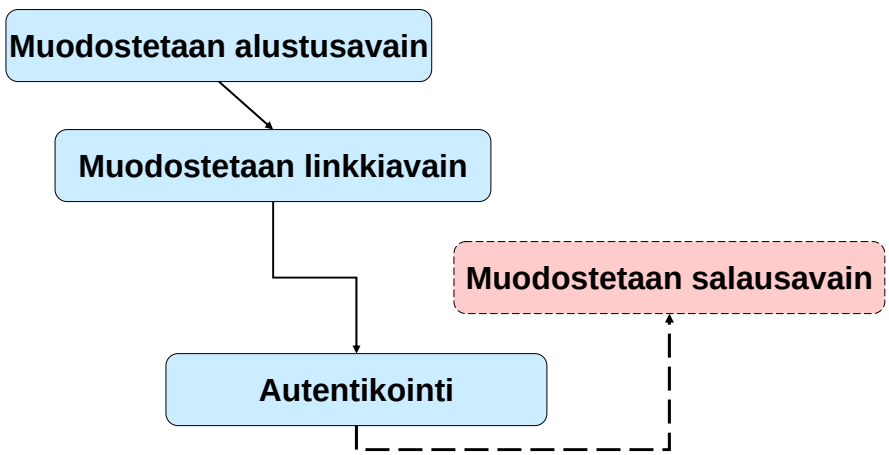
Bluetooth avaimet (I)



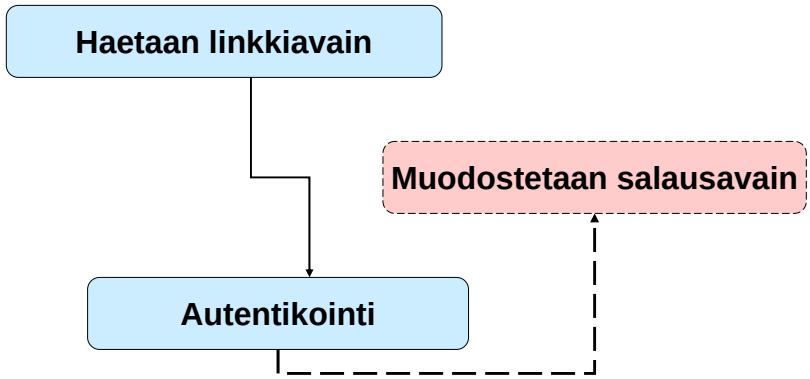
Bluetooth avaimet (II)

- Alustusavain: Initialisation key
  - Johdetaan PIN-luvusta
  - Käytetään kerran linkkiavaimen muodostamiseen
- Linkkiavain: Combination key
  - Kumpikin laite osallistuu sen generointiin
  - Kahden laitteen välinen salainen avain
- Linkkiavain: Unit key
  - Muodostetaan vain toisesa laitteessa
  - Laite käytää sitä kommunikointiin kaikkien muiden laitteiden kanssa
- Salausavain: Encryption key
  - Johdetaan käytössä olevasta linkkiavaimesta
  - Muodostetaan autentikoinnin yhteydessä
  - Pituus konfiguroitavissa (8-128 bit) ja maksimipituus usein rajoitettu HW toteutuksessa

Bluetooth Pairing - menettely
Ensimmäinen autentikointi

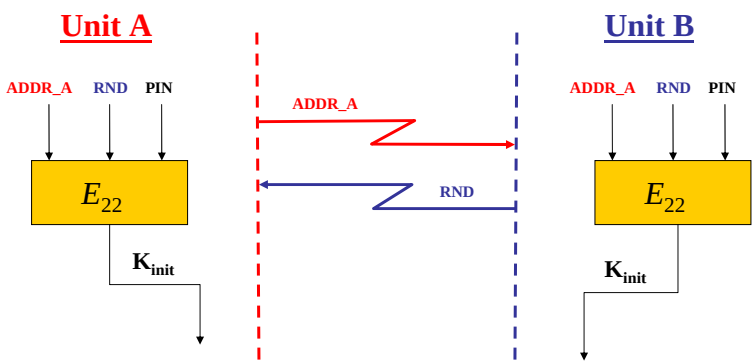


Seuraavat autentikoinnit ja salausavaimen luonti



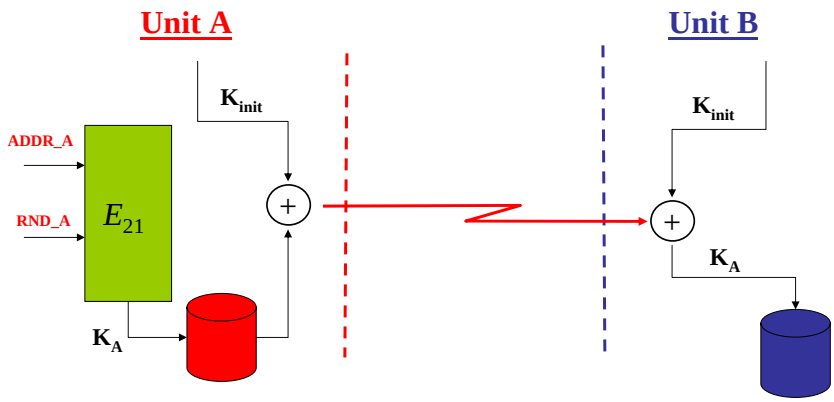
Pairing Procedure

Generate Initialization Key



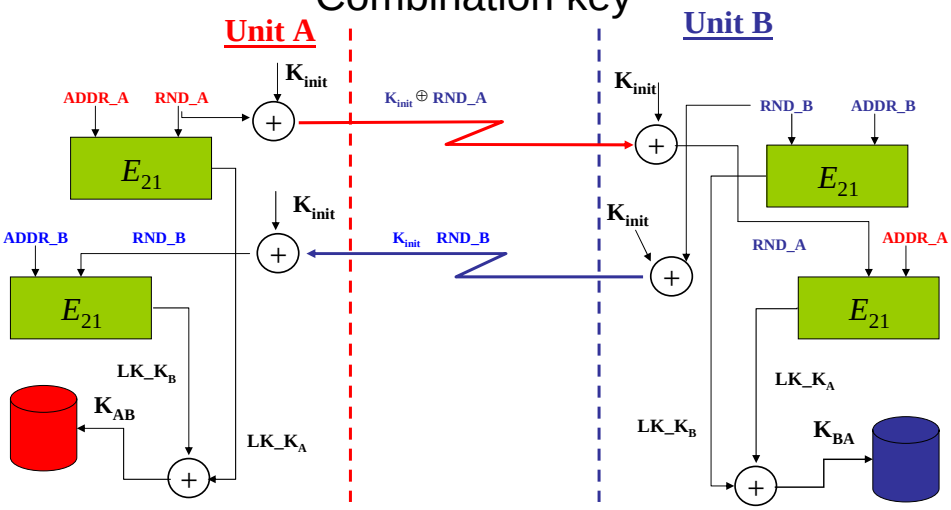
Pairing Procedure

Unit key

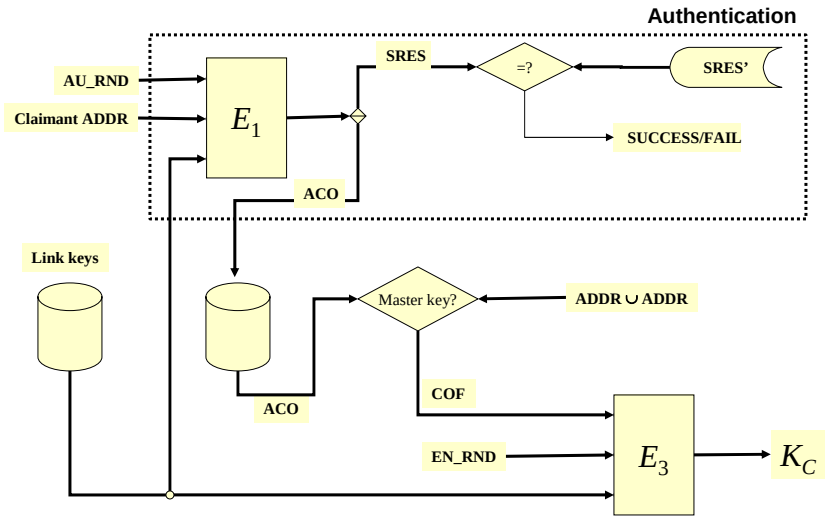


Pairing Procedure

Combination key

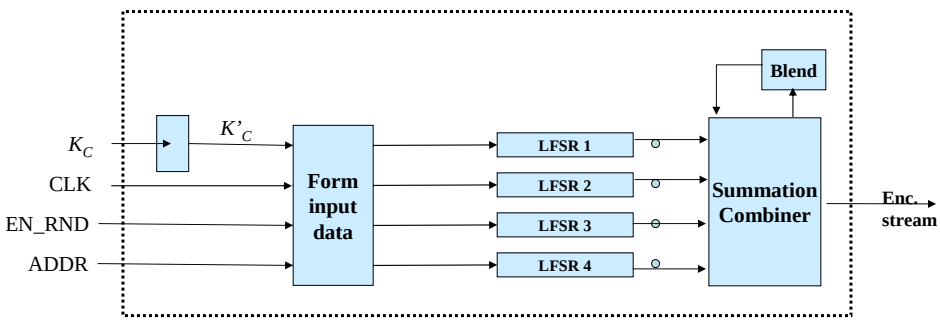


Salausavaimen K_C muodostaminen



The Algorithms

E_0—Salausalgoritmi



Bluetooth Algoritmit

E_0—Salausalgoritmi

- Jonosalausalgoritmi
  - Nopea ja yksinkertainen HW toteutus
- Vahvistetut korrelaatio-ominaisuudet
  - Viivästetty rekistereiden takaisinkytkentä
  - Pyöritetään aluksi tyhjää 240 kertaa
- Usein toistuva alustus
  - LFSR alustetaan jokaista salattavaa data pakettia varten
- Käytetään point-to-point ja point-to-multipoint yhteyksien salaamiseen

Bluetooth Algoritmit

E_1—Autentikointi algoritmi

- Perustuu SAFER+ algoritmiin
- Yhteensä 17 kierrosta
- Takaisinkytkentä, jotta algoritmista saadaan yksisuuntainen

E_2 = {E_{21}, E_{22}} —Linkkiavainten muodostaminen

- Perustuvat myös SAFER+ algoritmiin

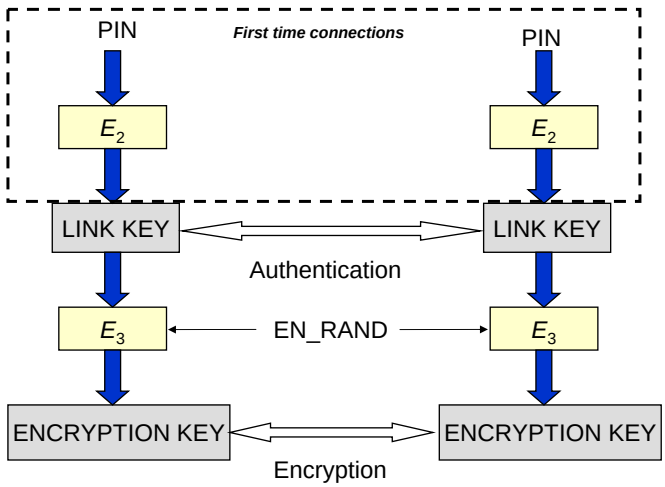
E_{21} (unit keys, combination keys)

- Input: RAND, BD_ADDR (48 bit)
- Output: Key (128 bit)

E_{22} (initialisation and master keys)

- Input: RAND, PIN, Length(PIN)
- Output: Key (128 bit)

Bluetooth avaimet - Yhteenveto



Bluetooth turvallisuus

- Varsin vahvat algoritmit[1]
- Turvallisuus perustuu linkkiavaimen vahvuuteen
- Linkkiavain muodostetaan joko Bluetooth PINin avulla tai syöttämällä suoraan sovelluksesta
- Anonymiteetin turvaaminen on ratkaistava erikseen
- Paikantamismahdollisuus – hyöty vai turvallisuusriski?
- Antaa mahdollisuuden hyvin erilaisten turvallisuusehtojen määrittelemiseen ja toteuttamiseen
- Linkkikerroksen turvamekanismit voidaan aktivoida suoraan tai sovelluksesta

[1] E_0 heikoin, noin DES:n tasoinen