T-79.4501
Cryptography and Data Security

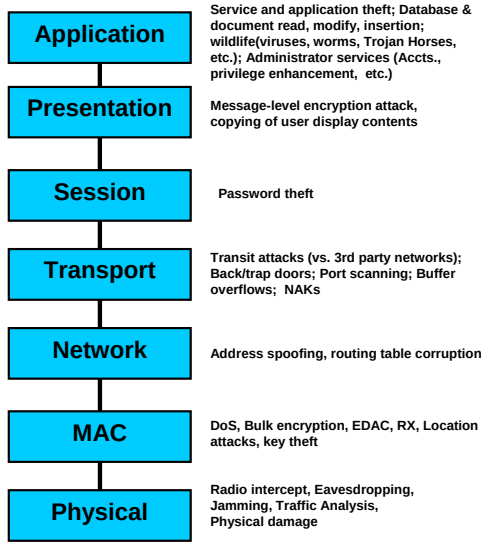
Lecture 11

Bluetooth Security

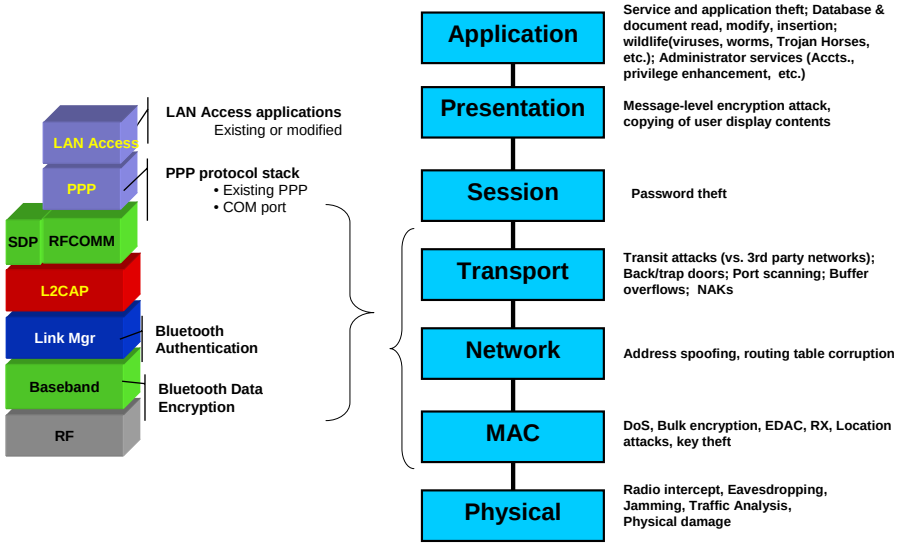
Outline

- Security threats
- Objectives of Bluetooth security
- The Bluetooth Baseband security
  - Pairing procedure
  - Authentication/Encryption key generation
  - Algorithms
- Summary

Threats in communication networks



Protection in bluetooth



End-to-end security vs. link Level security

- Bluetooth provides link level security
- Many applications require end-to-end security
  - dial-up networking for corporate clients (IPSEC)
  - e-mail (PGP,S/MIME)
  - Browser transactions (TLS)
- Bluetooth SIG encourage reuse of existing network, transport, session and application layer security mechanisms

Bluetooth Security Overview

Basic objectives

- Provide means for a secure link layer:
  - Entity authentication
    - Authenticated connections between personal devices
    - “Hardware” identification
    - 128 bits key
  - Link privacy
    - Allow private exchange of data between devices
    - Examples: File transfer, phone book/calendar/task synchronisation
    - 8-128 bits key

Bluetooth Security Overview

What it does not do...

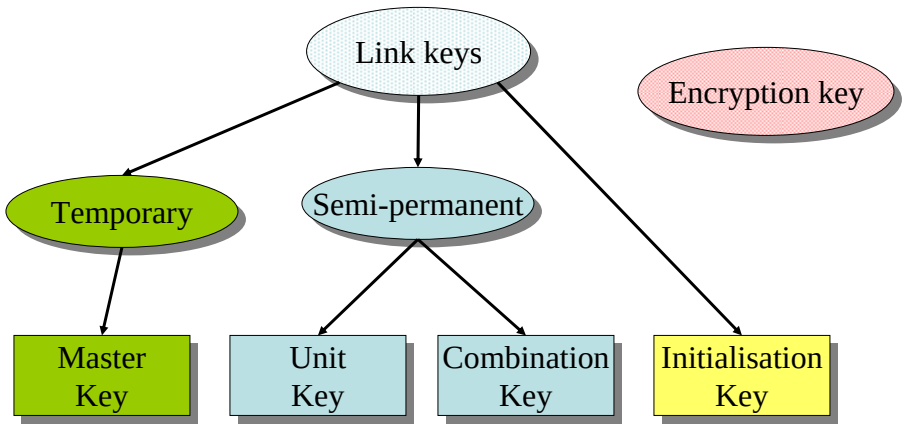
- Message authentication
  - Originating application is not identified
- Secure end-to-end links
  - Plain text in, plain text out...

Bluetooth Security Overview

Basic concept

- Key types
  - Link keys (128 bit)
  - Encryption keys (8-128 bit)
- Pairing
  - Establishing secret keys
- Encryption algorithm
  - Stream cipher

Key Types (I)



Key Types (II)

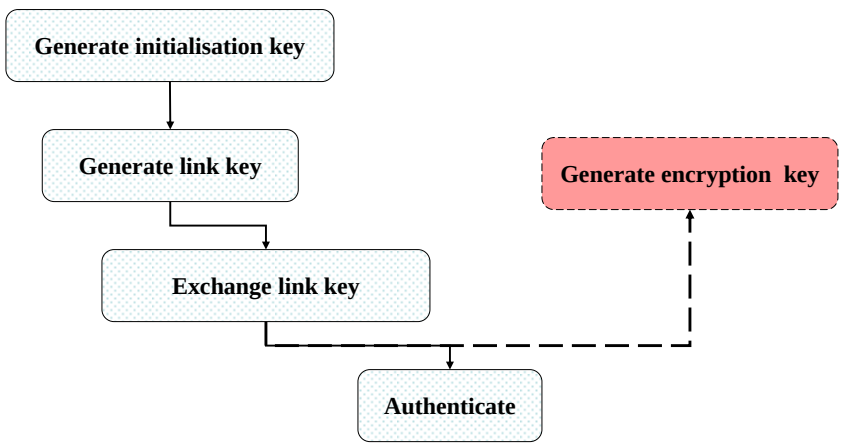
- Initialisation key
  - Derived from supplied number
    - Relatively short PIN—direct user interaction
    - "Super PIN"—key agreement protocol at application layer
  - Used once, then discarded
- Combination key
  - Combination of two contributions
  - Unique for each pair of units

Key Types (III)

- Unit key
  - Generated in one unit
  - Restricted memory resources
- Encryption key
  - Derived from current link key
  - Renewed every session
  - Configurable key length (8-128 bit)
  - Maximal length HW restricted

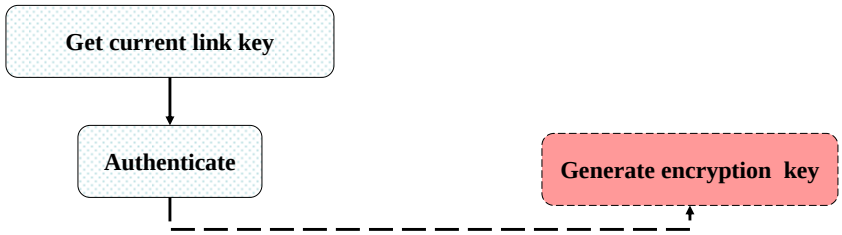
Pairing Procedure

First time connection



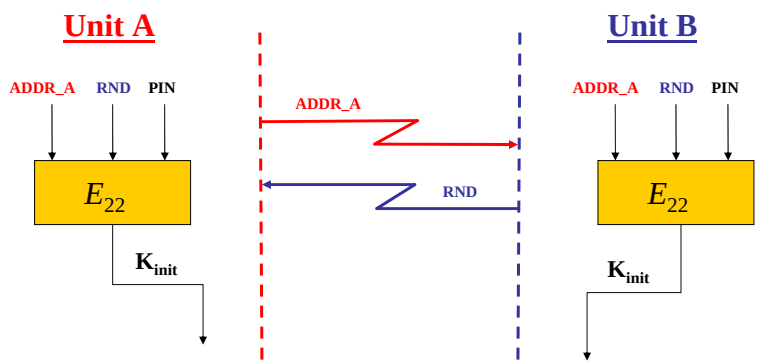
Pairing Procedure

Non-first time connections



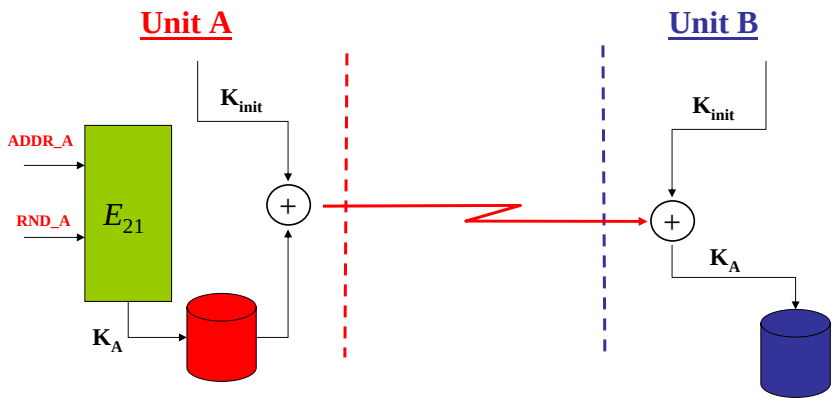
Pairing Procedure

Generate Initialization Key



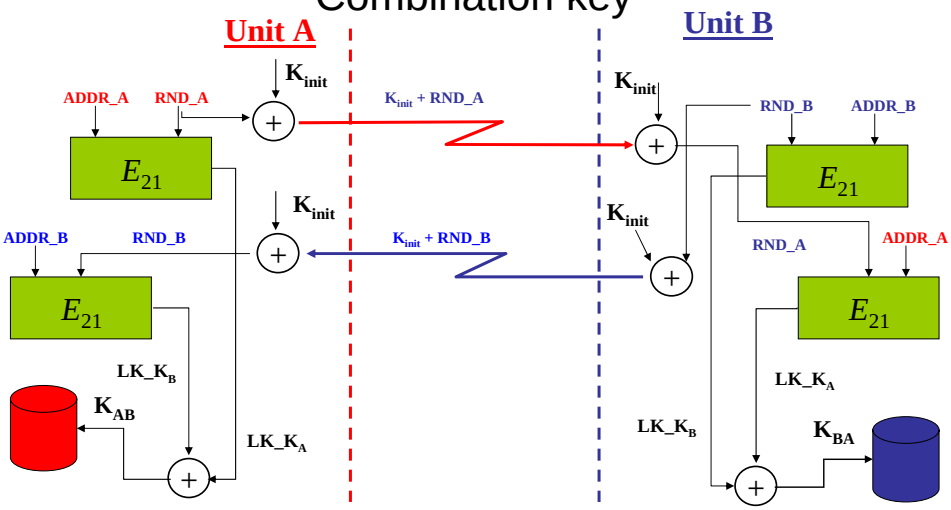
Pairing Procedure

Unit key



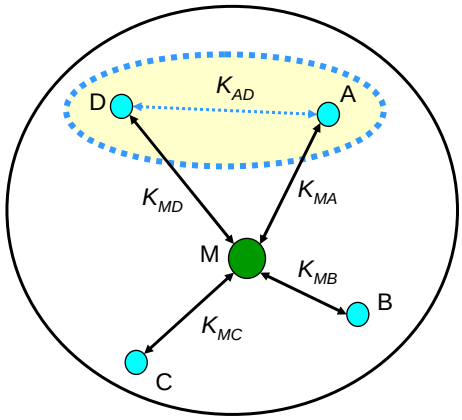
Pairing Procedure

Combination key



Key Usage

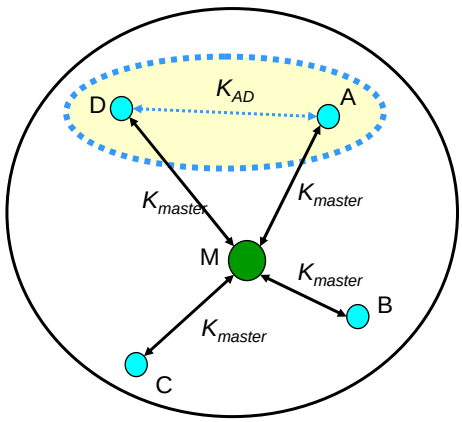
Semi-permanent or temporary link keys?



Point-to-point configuration

Key Usage

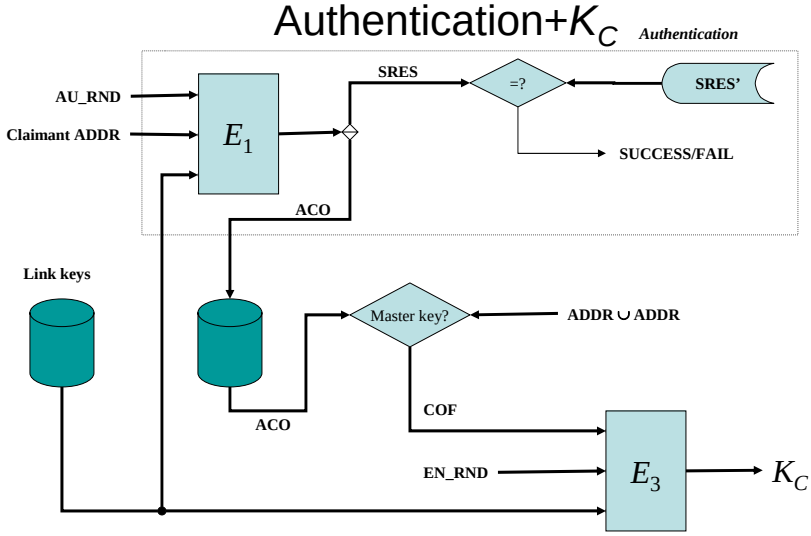
Semi-permanent or temporary link keys?



Point-to-multipoint configuration

Encryption Key Generation (I)

Authentication+K_C

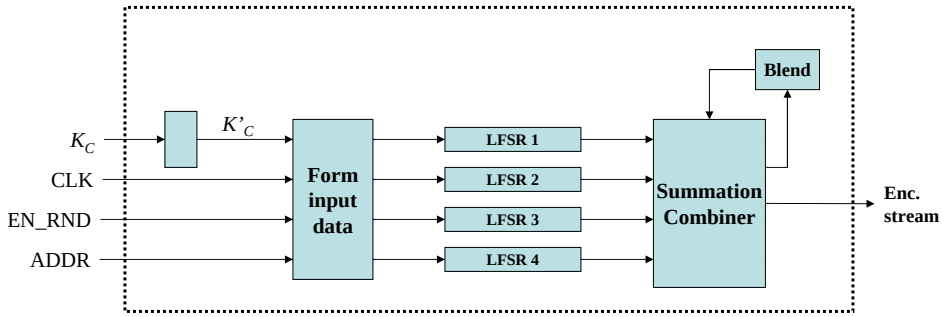


Encryption Key Generation (II)

- Kc is 128 bits
- Governmental attitudes/Export issues
  - Different key lengths needed
- Negotiation necessary (1-16 bytes)
- Generates Kc' in HW of correct length
  - Part of E_0 algorithm
- Initiate the LFSRs of the encryption machine

The Algorithms

E_0—Encryption algorithm



The Algorithms

E_0—Encryption algorithm

- Stream cipher
  - Fast and easy HW implementation
- Improved correlation properties
  - Blend register feedback
  - Initially clocked 240 times
- Frequent re-synchronising
  - LFSR starting state updated for each slot
- Point-to-point or point-to-multipoint

The Algorithms

E_1—Authentication algorithm

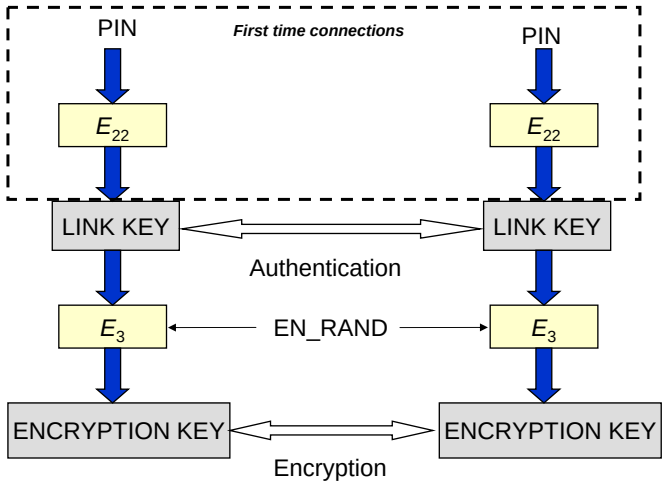
- Computationally secure authentication code
- Based on SAFER+
  - Runs for 17 rounds
  - Modified to be non-invertible

The Algorithms

E_{21}, E_{22}—Link key generation

- E_{21}:
  - Input: RAND, BD_ADDR (48 bit)
  - Output: Key (128 bit)
  - Unit and combination keys
- E_{22}:
  - Input: RAND, PIN, Length(PIN)
  - Output: Key (128 bit)
  - Initialisation and master keys

Key usage summary



Algorithm summary

- E0
  - HW implementation
  - Subject to export regulations
- E1, E21, E22, E3
  - Based on the same block cipher
  - Suitable for SW implementation

Summary

- There exists many security threats in communication networks
- The Bluetooth specification provides authentication protection and link level encryption
- The Bluetooth specification meets security industry level for protection