



Overview of Bluetooth Security

Security Considerations for a Short-Range Wireless Technology

Wong Ford Long
fordlong@security.org.sg

29 Mar 03

1



Outline of Talk

- Summary of Bluetooth technology (8 slides)
- Bluetooth security architecture (21)
- Vulnerabilities (3)
- Recommendations on use (2)

29 Mar 03

F L Wong, March 2003

2



Bluetooth Jokes

- “I’m having the Bluetooth blues...”
- “A Bluetooth cavity...”
- And other colour and dental jokes...



Description of Technology



Bluetooth Technology



- Peer-to-peer wireless area network
- Small size, low power, short range
- Up to 8 devices in a “piconet”
- Defines lowest 3 OSI layers
- A complex but elegant technology

29 Mar 03

F L Wong, March 2003

5



Ubiquity



- Hundreds of millions to billions of devices eventually forecasted
- In handphones, PDAs, laptops, hands-free etc
- Even mouse, keyboards, in-vehicular etc
- In Windows XP, Linux, etc

29 Mar 03

F L Wong, March 2003

6



Bluetooth Physical Layer

- 2.4GHz ISM band
- 1,600 hops/s over 79 1-MHz frequency channels
- 1 Mbps, actual data throughput ~700kbps
- Piconet consists of 1 master, up to 7 slaves
- GFSK, TDMA
- Uses 3.2kHz clock, 28 bits
- Radio power -30 to 20dBm, range 10-100m



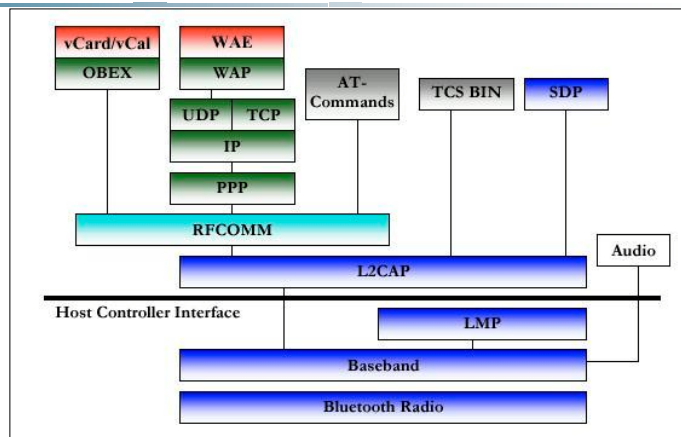
Bluetooth Protocol Stack

- Application Group
- Middleware Protocol Group
- Transport Protocol Group

Transport Protocol Group

- Physical Layer – Radio
- Baseband
- LMP (Link Manager Protocol)
- L2CAP (Logical Link Control and Adaptation Protocol)
- Audio

Protocol Layers



Blue indicates Bluetooth core protocols

Bluetooth Core Protocols

- Baseband
 - Enables the FH radio link, using inquiry and paging procedures to synchronise the frequency and clock of different devices.
- Link Manager Protocol
 - Link set-up and control, control of baseband packet size, security, power modes, duty cycles, and connection states.
- Logical Link Control and Adaptation Protocol
 - Supports protocol multiplexing, packet segmentation and reassembly, and QoS.
- Service Discovery Protocol
 - To query device information, services and their characteristics.

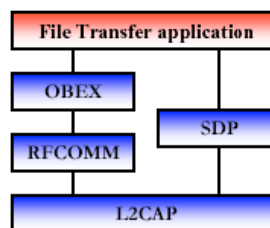
29 Mar 03

F L Wong, March 2003

11

Bluetooth Profiles & Usage Models

- Each Profile - a vertical slice of the Protocol Stack
- A Usage Model accompanies each Profile
- Four general Profiles widely utilized
 - Generic Access Profile
 - Serial Port Profile
 - Service Discovery Application Profile
 - Generic Object Exchange Profile
- Eg Usage Model – File Transfer



29 Mar 03

F L Wong, March 2003

12

Security Architecture

Security - Baseband, LMP & GAP

- Protocol layers - the Baseband and LMP.
- Profiles - mandatory Generic Access Profile plays an important role in security.

- Baseband – defines the random number generation, key management, encryption, authentication, and algorithms for authentication and key-generation.
- LMP – defines the link set-up and control between devices, including the security procedures.
- GAP – defines how devices are to connect to each other and access services for basic interoperability, as well as the security modes and user interface.

Bluetooth Security Architecture

- Supports
 - Authentication
 - Authorization
 - Encryption (therefore Confidentiality)
 - Integrity
- Supports 3 security modes
- Supports different security levels (access control) for
 - Devices
 - Services
- Identifiers – IDs, keys, random numbers

Bluetooth Security Modes

- Mode 1
 - Non-secure
- Mode 2
 - Service-level security
 - Security procedures not initiated before channel establishment at L2CAP level. Allows different and flexible access policies for applications
- Mode 3
 - Link-level security
 - Security procedures initiated before link set-up at the LMP layer is completed

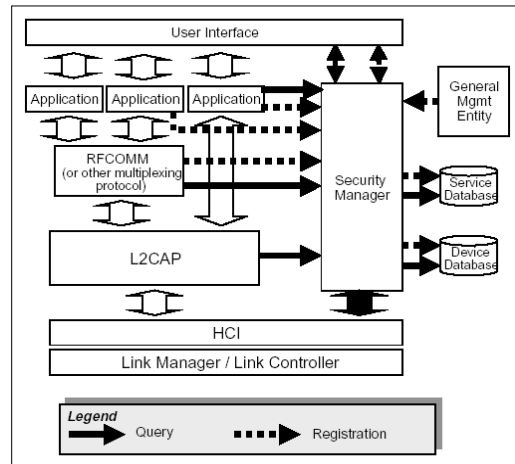
Bluetooth Security Levels

- Devices
 - Trusted
 - Untrusted
- Services
 - Require Authentication and Authorization
 - Require Authentication Only
 - Open to all devices

Bluetooth Identifiers

- Unique IEEE Bluetooth Device Address (BD_ADDR)
 - 48 bits
- Link Key (K_{link}) for authentication (usually pair-wise)
 - 128 bits
- Encryption Key (K_c) (symmetric key) – 8 to 128 bits
- Random numbers (RAND) generated as required – 128 bits

Bluetooth Security Architecture Diagram



What is Bluetooth Link Security?

- Provides means for a secure link layer
- Pairing with use of PIN to establish secret pair-wise link keys
- Challenge-response authentication with knowledge of link key
- Encryption, thus assuring privacy

Key Types

■ Link Keys

- Initialization
 - Initialization Key – derived from PIN, used once, then discarded
- Semi-permanent
 - Unit Key – generated once in unit, used when memory-constrained
 - Combination Key – derived from contributions from two devices
- Temporary
 - Master Key – for point-to-multipoint broadcasts

■ Encryption Key

- Encryption Key – derived from current semi-permanent or temporary key, renewable for every connection, and having configurable key length (8-128 bits)

Algorithms

■ Authentication and Key Generation

(All based on SAFER+ block cipher)

E_1 – Authentication algorithm

E_{21} – Unit and combination keys generation

E_{22} – Initialisation and master keys generation

E_3 – Encryption key generation

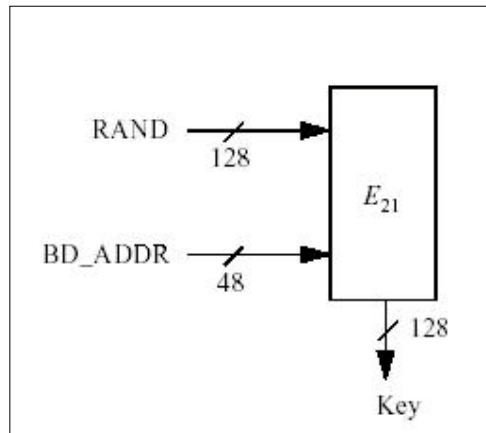
■ Encryption

E_0 – Stream cipher algorithm

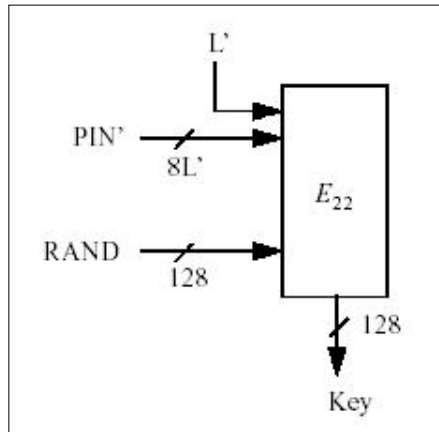
Typical Security Procedures

Device A First Startup Generation of Unit Key (E21)	Device B First Startup Generation of Unit Key (E21)
Device A to Device B First Handshake Generation of Initialization Key (E22) Authentication (E1) Link Key Exchange (E21)	
Device A to Device B Following Handshakes Authentication (E1) Generation of Encryption Key (E3) Encrypted Communications (E0)	

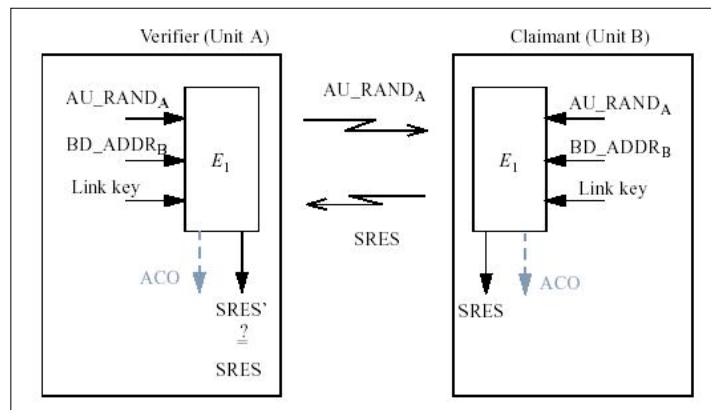
Unit Key generation



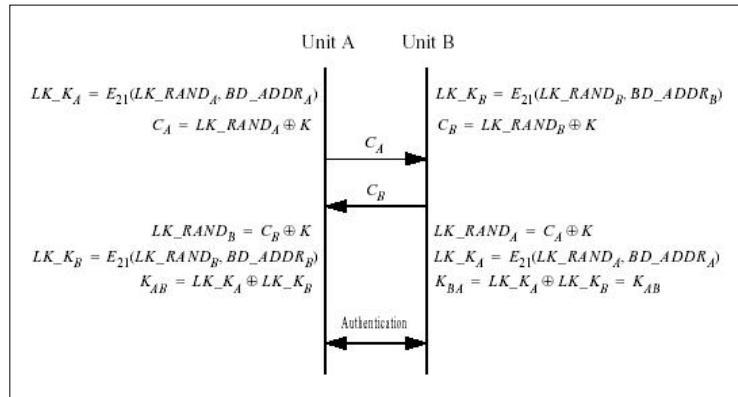
Initialisation Key generation



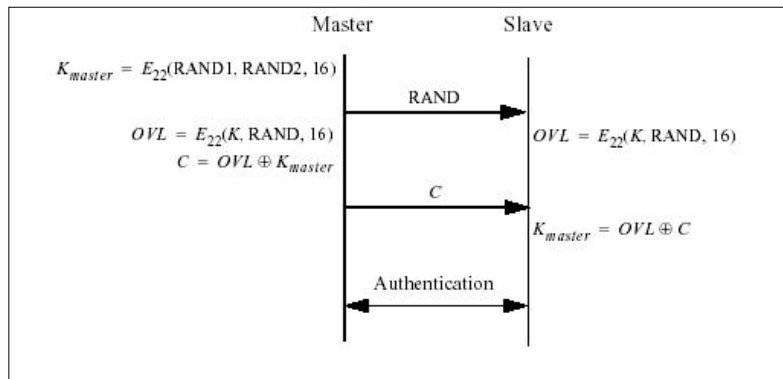
Authentication



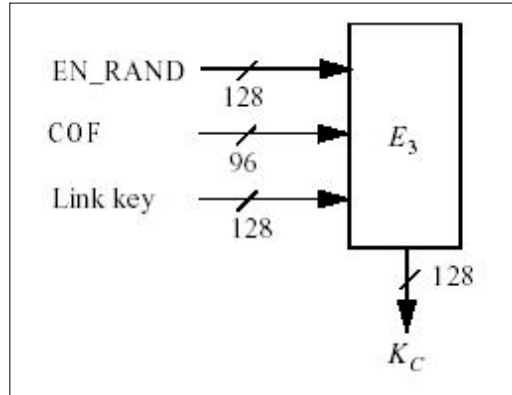
Combination Key generation



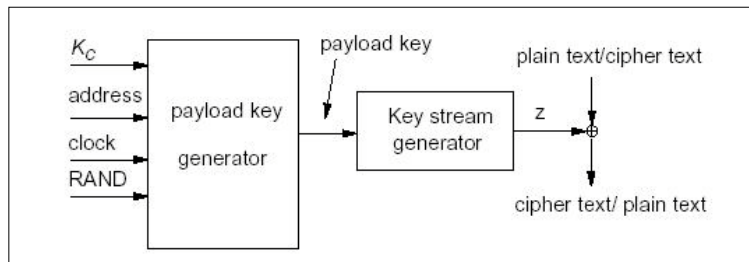
Master Key generation



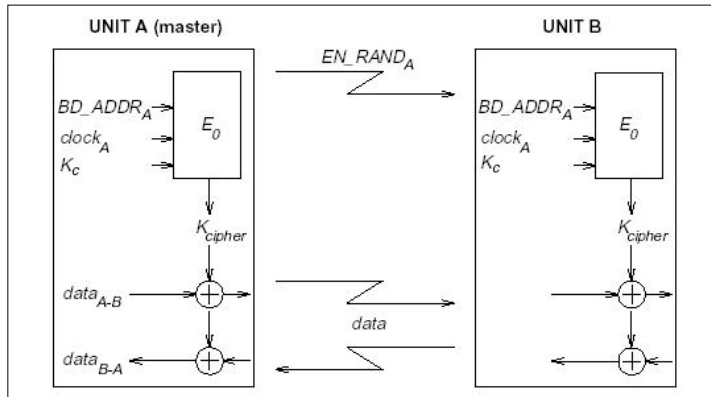
Encryption Key generation



Encryption Process (1)



Encryption Process (2)



29 Mar 03

F L Wong, March 2003

31

State of Bluetooth Security

- Supports confidentiality, integrity, authentication and authorization (access control).
- Shorter range (10m to 100m), so need to get in close.
- No major obvious weaknesses with SAFER+ like the WLAN 802.11b's WEP.

29 Mar 03

F L Wong, March 2003

32

Bluetooth vs 802.11b – Part I

- In 802.11b WEP, a key/Initialisation Vector pair is repeated often enough to make attack possible after capturing ~5 million encrypted packets.
- Key scheduling of RC4 in 802.11b WEP and statistical bias may be exploited to recover key.
- In 802.11b WEP, challenge/response forms a plaintext/ciphertext pair, and use of XOR is weak. In Bluetooth, the E1 algo is not reversible.
- Same key used for authentication and encryption in 802.11b WEP, not so for Bluetooth where the link key is used to generate a ciphering key.

Bluetooth vs 802.11b – Part II

- No known practical attack against Bluetooth's E0 stream cipher, though there have been suggestions of 2^{100} and 2^{66} attacks.
- But use of PIN in Bluetooth need to be carefully monitored.

Vulnerabilities

Known Weaknesses

- Wireless is easier to intercept, than wired is to wiretap.
- If the unit key is used as a link key for authentication, a device can be spoofed.
- If PIN length used is short, brute-forcing can succeed.
- A discoverable device replies to inquiry scans and announces its ID, so tracking is possible.
- SAFER+ supposedly has minor weaknesses.

Other Possible Weaknesses

- Use of well-defined and crowded 2.4GHz makes DoS possible.
- Integration of Bluetooth with various pre-existing protocols will
 - Inherit the other protocols' problems (such as IPv4)
 - Give rise to integration-related problems especially with vulnerable applications

What the Design Can't Take Care of

- Sysadmins
 - Unsuitable security policies
 - Misconfiguration
 - Untrusted drivers and devices
 - O/S and application vulnerabilities
- Users
 - Running Trojans and other malicious code
- Developers
 - Unsecure software engineering
 - Lack of buffer checks etc
 - No proper software verification process

Recommendations on Use

Recommendations on Use (1)

- Determine suitable, enforceable security policies
- Use only signed drivers and devices from trusted sources
- Configure Bluetooth security strongly
 - Use security mode 2 for fine-grained control, or security mode 3 for across-the-board control
 - Turn on authentication and encryption (up to 128 bits)
 - Turn on authorization function for more secure services
- Have access control list to filter by device IDs
- Use strong PINs
- Perform device pairings in safe areas



Recommendations on Use (2)



- Deny use of Bluetooth in sensitive areas
- Don't rely just on Bluetooth in-built security, but also use higher-layer network security mechanisms like
 - Layer 3 – IPSec, VPN etc
 - Firewalls (including personal firewalls)
 - Certificates and PKI for strong authentication
 - Other strong authentication like Kerberos and RADIUS
 - Etc

29 Mar 03

F L Wong, March 2003

41



Thank You.
Questions?

29 Mar 03

F L Wong, March 2003

42