SWINBURNE UNIVERSITY OF TECHNOLOGY

NSR/AS

Bluetooth Security

Lecture Twenty-Six

Outline of Lecture

- Bluetooth overview
- Bluetooth security

Bluetooth

- Short range cable replacement specification
  - Up to about 10 metres
- A ‘piconet’ technology
- Developed under auspices of IEEE 802.15.1
- Able to support data and voice
  - But at fairly low bit rates
    - 3 Mbps shared

Bluetooth Applications

- Applications include
  - Headsets
  - Connecting computers to peripherals (printer, speakers, scanners etc)
  - Synchronising between PDAs, Mobile Phones, and Workstations
- An ad hoc networking technology
  - Devices can form networks as needed

Bluetooth Specifications

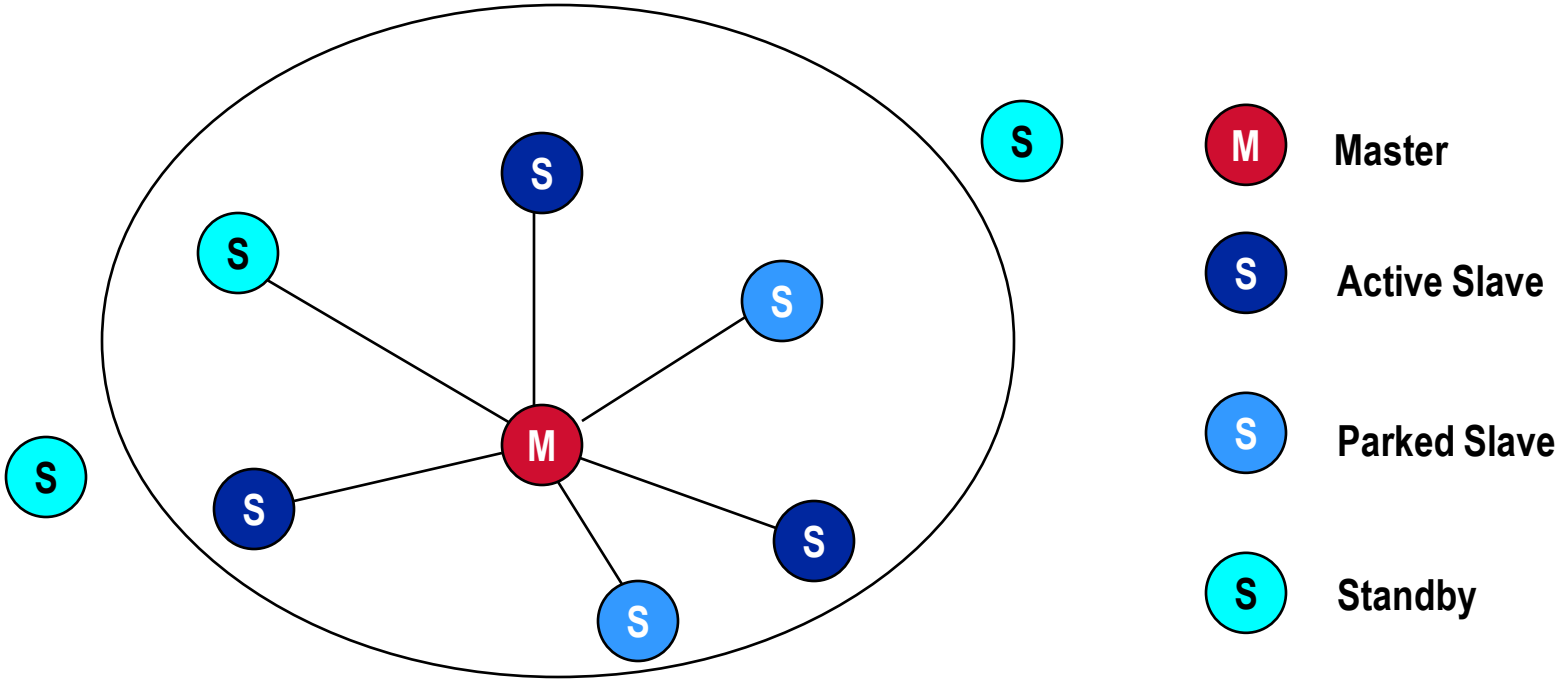
Connection Type	Spread Spectrum (FH)
MAC	FH-CDMA
Spectrum	2.4 GHz (ISM)
Modulation	GMSK
Aggregate Data Rate	3 Mbps
Range	10 metres
Supported stations	8 devices
Voice channels	3
Data security – authentication	128 bit key
Data security – encryption	8 – 128 bits (configurable)

Bluetooth Scenarios

- Cable replacement
  - Keyboards, mouse, microphones, etc
- Ad hoc personal network
  - Networking of several different users at a short range such as in a conference room
- Integrated Access point
  - Use Bluetooth to connect to wide area voice or data services provided by cellular or wired networks

Piconet

- Network consisting of one master and up to seven slaves
- Different piconets use different Frequency Hopping sequences
- Piconet capacity is 3 Mbps (aggregate)



Piconet Station States

- Active (maximum of 8)
  - Transmitting data
  - Connected
- Connecting
  - Inquiring
  - Paging
- Unconnected
  - Standby
- Low Power
  - Parked (maximum of 200)
  - Known to the other stations but not participating in the piconet

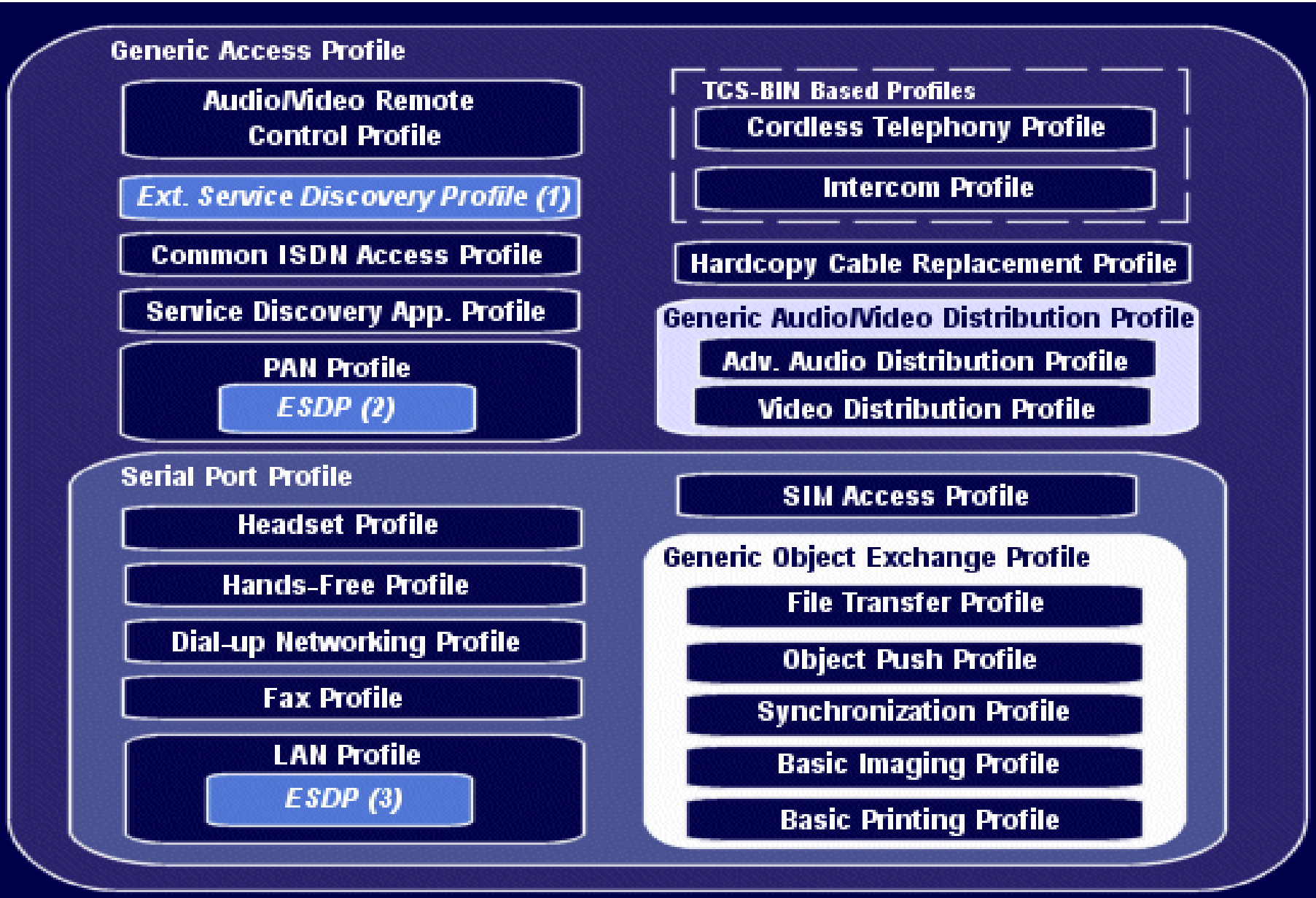
Master / Slave

- Master
  - One device in the piconet is the Master
  - Other devices synchronise their Frequency Hopping sequence and Clocks to this device
  - The Master is responsible for paging slaves in the piconet and Connection Establishment
  - Master/Slave Polling system
- Slaves
  - Other devices
- Any Bluetooth device can be either a master or slave
  - An election process

Application Protocols

- Can be both Bluetooth aware and unaware
- Bluetooth specifies several protocol stacks for different applications
- Makes use of **Profiles**
  - Describe how different applications are implemented

Bluetooth Profiles



Generic Access Profile

- Used by all other profiles
- Describes generic procedures
  - Discovery of Bluetooth devices
  - Connection procedures
  - Security

Serial Port Profile

- Incorporates Generic Access Profile
- Defines requirements for Bluetooth devices necessary for setting up emulated serial cable connections using RFCOMM
- RS232 emulation
- Cable replacement through a virtual serial port
- Includes
  - Headset, Hands free, dial-up, fax, LAN, SIM and Generic objects

Generic Object Exchange

- Defines how Bluetooth devices exchange objects
- Additional profiles specify the exchange of specific objects
  - File transfer
  - Synchronisation
  - Object Push
- Used in ‘Bluejacking’
  - unsolicited transfer of binary objects

Bluetooth security architecture

- Based on symmetric keys for encryption, authentication and symmetric key generation
- Authentication
  - Challenge response protocol
- Link privacy
  - Symmetric key
  - Stream cipher with feedback
- Security modes
  - Mode1: Never demands authentication or encryption on a link
  - Mode2: Security is not initiated at the link level. Higher layers of the profile request authentication and / or encryption
  - Mode3: Security procedures initiated at startup

Pairing

- Procedure by which two devices establish a shared secret key (the link key) that can be used as a basis for later communication
- Manual exchange of key information (PIN number)
- Each device stores a (link key, device address) pair
- Pairing process consists of
  - generating an initialisation key
  - generating a link key
  - link key exchange
  - authentication

Generating an initialisation key

- Based on the PIN code, address and random number
- Address and random number transmitted in clear
- PIN code entered manually
  - ‘secret’ used to generate a shared secret key
  - Can be up to 16 octets in length
  - Default is 4 digits with default value 0000 !!!!
- Once there is a shared initialisation key, a link key is exchanged
  - Initialisation key is short lived and only used to exchange the link key

Generating a link key

- A different key is used for communication between each device pair
- Each device transmits a random number to each other, which is used to generate the link key
- The link keys are encrypted and exchanged using the other device's initialisation key
- Note
  - The link key is never used for direct encryption of data
  - A session key is generated using the link key

Authentication

- Can be either mutual or one-way
  - Depends on the security mode
- Uses a simple challenge-response authentication protocol
  - Verifier issues a random number to the claimant
  - Claimant generates a hash using the random number and the link key
  - Response to random number transmitted to claimant
  - Verifier does the same calculation and if agrees with response from claimant then claimant identity is verified

Encryption

- Link key is used to generate a session key
  - Link key is never used to directly encrypt data
- Session key generation
  - One of the parties transmits a random number encrypted with the link key
  - The random number and the link key are used to generate the session key
  - The session key is used to encrypt data
  - Encryption algorithm is E3 or AES CBC

Encryption

- E3
  - Stream cipher algorithm with feedback
  - encrypts a byte at a time
- Resynchronisation is necessary with feedback algorithms
  - Occurs at the start of every frame

Bluetooth security weaknesses

- Problems with encryption and hashing algorithms
  - Susceptible to brute force attacks
- PIN
  - Security of the keys is based on the security of the PIN
  - Some devices have fixed (unchangeable) PINs (!!!!!!!)
  - Weak PINs (1234, 2222 etc)
  - Default Pin value is usually 0000
  - Default PIN length is 4 digits
    - Very susceptible to brute force attacks

Bluetooth security weaknesses

- Eavesdropping and impersonation
  - If keys compromised or no security implemented
- Key storage
  - Needs to be very secure to prevent hackers
    - Accessing link keys
    - Installing their own link keys
- Location privacy
  - Devices can be in discoverable mode
  - Every device has fixed hardware adress
  - Adresses are sent in clear
  - possible to track devices (and users)

Other weaknesses

- No integrity checks
- No prevention of replay attacks
- Man in the middle attacks
- Lots of bluetooth exploits, mostly involving bluetooth enabled mobile phones

Bluetooth implementation based attacks

- Snarf attack
  - Bluetooth enabled phones
- Phone is enabled
- Attacker connects to the phone
  - Either through a 'bluebug' attack or because security is not set
- Attacker is able to gain access to restricted part of stored data
    - Calendar
    - Business cards
    - IMEI (International Mobile Equipment Identity)
      - Unique identifier for the phone to the mobile network

Bluebug attack

- Name of a bluetooth security loophole on many bluetooth-enabled phones
  - Seems to affect most major manufacturers
- Sets up a covert channel that allows the attacker to issue AT modem control commands without the knowledge of the owner of the phone
  - Undocumented RFCOMM channels supported by Bluetooth chips
- Can do most mobile phone functions without the owner being aware of it
  - initiating phone calls, sending and reading SMS, reading and writing phonebook entries, connecting to Internet…

Bluejacking attack

- Not really an attack, more an unsolicited sending of a binary object
  - object usually a business card or phone directory entry
  - can be an image or other media item
- Could be used for spam
- Mostly irritation value but some potential for serious harm

Quite a lot of bluetooth hacking tools

- Software and systems for doing the bluebug, snarfing and bluejacking
- Bluesniper
  - Long distance attack hardware
  - Modified Bluetooth dongle
  - Range of 1.8 km
- Bloover
  - Carries out bluebug attack
- Bluesmack
  - Denial of service using buffer overflow

General comment on Bluetooth security

- Provided good practices are followed, particularly regarding the PIN, Bluetooth is reasonably secure
  - Still quite a few weaknesses, but probably not too severe given Bluetooth's intended role
- Most of the serious hacks have been at the application level
  - Undocumented channels, Poor default PINs etc

Conclusion

- Bluetooth overview
  - A short range, cable replacement technology
- Bluetooth security
  - Based on symmetric keys
  - Derived from PIN
- Bluetooth security weaknesses
  - PINs
    - Weak PINs, Default PINs of 0000, PINs that can't be changed
  - Undocumented RFCOMM channels
  - Bluetooth devices left in 'discovery' mode