Bluetooth

Stephen Carter
March 19, 2002

Quote of the Day

"I don't have to be careful, I've got a gun."
-Homer Simpson
About Bluetooth

- Developed by a group called Bluetooth Special Interest Group (SIG), formed in May 1998
- Founding members were Ericsson, Nokia, Intel, IBM and Toshiba
- Almost all of the biggest companies in the telecommunications business have joined the Bluetooth SIG and the number of the participating companies is now over 1,500

What is Bluetooth?

- A **cable-replacement** technology that can be used to connect almost any device to any other device
- Radio interface enabling electronic devices to communicate wirelessly via short range (10 meters) ad-hoc radio connections
- A standard for a small, low cost (~ $5), low power, radio based chip to be plugged into computers, printers, keyboards, monitors, mobile phones, refrigerators??, PDAs, etc…
Bluetooth details

- Uses the radio range of 2.45 GHz
- Theoretical maximum bandwidth is 1 Mb/s
- Several Bluetooth devices can form an ad hoc network called a “piconet”
  - In a piconet one device acts as a master (sets frequency hopping behavior) and the others as slaves
  - Example: A conference room with many laptops wishing to communicate with each other

Bluetooth v. 802.11?

- **Bluetooth**
  - Designed for quick, seamless short range networks
  - Features low power consumption, small protocol stack, robust data & voice transfer
  - Cheap price
  - Good choice for WPAN (Wireless Personal Area Networks)
- **802.11**
  - Designed for infrequent mobility, IP-based data transmission
  - Medium range and high data rate
  - At least 10x the price of bluetooth
  - Good choice for WLAN (Wireless Local Area Networks)
Bluetooth v. 802.11?

WPAN technologies enable users to establish ad hoc, wireless communications for devices (such as PDAs, cellular phones, or laptops) that are used within a personal operating space (POS). A POS is the space surrounding a person, up to a distance of 10 meters.

No serious competition exists between the Bluetooth & 802.11. They are aimed at different markets and different roles.

Bluetooth v. 802.11?

- IEEE has established the 802.15 working group for WPANs. This working group is developing a WPAN standard, based on the Bluetooth version 1.0 specification. Key goals for this draft standard are **low complexity, low power consumption, interoperability, and coexistence with 802.11 networks.**
Bluetooth Specification Protocol Stack

- Radio
  - defines the requirements for a Bluetooth transceiver operating in the 2.4 GHz ISM band.
- Baseband
  - describes the specification of the Bluetooth Link Controller (LC) which carries out the baseband protocols and other low-level link routines.
- LMP
  - used by the Link Managers (on either side) for link set-up and control.
- HCI
  - provides a command interface to the Baseband Link Controller and Link Manager, and access to hardware status and control registers.
- L2CAP
  - supports higher level protocol multiplexing, packet segmentation and reassembly, and the conveying of quality of service information.
- RFC
  - provides emulation of serial ports over the L2CAP protocol. The protocol is based on the ETSI standard TS 07.10
- SDP
  - The Service Discovery Protocol (SDP) provides a means for applications to discover which services are provided by or available through a Bluetooth device. It also allows applications to determine the characteristics of those available services
Bluetooth Security

• Must consider standard ad hoc network issues
  – Availability
    • DOS attacks easy to perform
    • Routing protocol attacks
    • Battery Exhaustion attacks
  – Authorization & Key Management
  – Confidentiality & Integrity
    • Anyone can sniff messages from the air
    • Radio Interference

Bluetooth Security (cont)

• Every bluetooth device has 4 entities for maintaining security
  – Bluetooth device address
    • 48-bit address that is unique for each Bluetooth device and defined by IEEE
  – Private authentication key
    • 128-bit random number used for authentication purposes
  – Private encryption key
    • 8-128 bits in length that is used for encryption
  – Random number
    • frequently changing 128-bit random or pseudo-random number that is made by the Bluetooth device itself
Bluetooth Security (cont)

- In Bluetooth Generic Access Profile, security is divided into 3 modes
  - non-secure
  - service level enforced security
  - link level enforced security
    - device initiates security procedures before the channel is established
- Device security modes
  - Trusted or untrusted
- Service security modes
  - Authorization and Authentication
  - Authentication only
  - Open to all

Bluetooth Security (cont)

- Security mechanisms more complex than 802.11 due to the “ad-hocness”
- A number of weaknesses and vulnerabilities exist in Bluetooth security
- May be adequate for non-sensitive data and smaller applications, but money transactions or military applications???
- Sound familiar???
Credits

- Palowireless Bluetooth Resource Center
- Microsoft XP Help and Support Center