Bluetooth Security: Why Bother?

12 Mar 09

Michael Disabato
Vice President & Service Director
Network & Telecom Strategies
mdisabato@burtongroup.com
www.burtongroup.com
Bluetooth Security: Why Bother?

Thesis

• Phones, cars, laptops, and headsets are just a few of the billions of Bluetooth devices sold each year
• As more devices have Bluetooth embedded, more people are taking advantage of it
• What are the security implications of this increasingly popular technology?
• Where does this fit into an overall enterprise security strategy?
Bluetooth Security: Why Bother?

Agenda

• The Technology
• The Market
• Security Issues
• Recommendations & Conclusions
The Technology

What is Bluetooth

- Cable replacement, not LAN extension
- Designed to eliminate the wire between devices
- A universal connector - eliminates the need for special cables between devices
- Can support streaming audio and medium quality video
- Future releases anticipated to support HDTV in...
The Technology

The Radio

• Operates in the 2.4GHz ISM band on 79 channels each 1 MHz wide

• Uses Frequency Hopping Spread Spectrum (FHSS)

• Raw data rates of 1, 2, and 3 Mbps

• Near Field Communications (NFC) support for Secure Simple Pairing

• Future: Implement ultrawideband
  • 100mbps mandated by standard; 240mbps possible

• Future: 802.11a/b/g support will provide 24Mbps at the radio
The Technology

The Radio

• Three power levels allow for different applications:
  • Class 1 is for long range (300ft/100m) operates at 100mw
  • Class 2 is for ordinary range (30ft/10m) operates at 2.5mw
  • Class 3 is for short range (1ft/30cm) operates at 1mw

• Each radio has a 48-bit device ID (MAC address)

• Bluetooth devices form “piconets” of up to 7 active and/or 200 “parked” devices
The Technology

Adaptive Frequency Hopping (AFH)

- Reduces interference with 802.11b/g networks
- Avoids channels in use
- May be less effective with 802.11n bonded channels
The Technology

Security

- Authentication and encryption protect all transmissions
- Authentication uses the ISO/IEC 9798-2 challenge/response system
- SAFER+ stream cipher with key lengths up to 128 bits used to encrypt data
- Future: Advanced Encryption Standard (AES)
- Provides four security modes:
  - Mode 1: No authentication/encryption
  - Mode 2: Service authentication/encryption
  - Mode 3: Link authentication/encryption
  - Mode 4: Continuous link authentication and encryption (mandated)
- Pairing mechanism creates link keys; authentication creates encryption keys
Profiles

- **Generic Object Exchange**
- **Hands-Free**
- **Headset**
- Basic Imaging
- Common ISDN Access
- General Audio/Video Distribution
- Audio/Video Remote Control
- Advanced Audio Distribution
- Video Distribution
- Personal Area Networking
- **Hard Copy Cable Replacement**

- **Human Interface Device**
- **Basic Printing**
- Cordless Telephony
- **Dial-Up Networking**
- Fax
- **File Transfer**
- Intercom
- **Object Push**
- Service Discovery Application
- Service Port
- **Synchronization**
The Technology

Bluetooth Protocol Stack

Layer 1
- RF
- Baseband
- Link Controller
- Link Manager
- Host Control Interface
- RFCOMM (Serial Port)

Layer 2 & 3
- Layer 4
- Voice
  - Intercom
  - Headset
  - Cordless
  - Group Call
- Telephony Control Protocol
- L2CAP
- OBEX
- vCard
- vCal
- vNote
- vMessage
- Dial-up Networking
- Fax
- Service Discovery Protocol

Layer 4
- Applications
Bluetooth Security: Why Bother?

Agenda

• The Technology

• **The Market**

• Security Issues

• Recommendations & Conclusions
The Market

Current Uses

• Bluetooth-enabled phones, PDAs, and computers continue to drive the market

• “Hands-free” driving laws have increased the use of headsets and other hands-free technology

• Mobile operators are using the cordless telephony profile as a way to increase minutes and differentiate offerings

• Wireless industrial controls and monitoring are displacing cabling due to costs
The Market

Profiles Used
1 - Serial Cable
2 - Synchronization & OBEX
3 - Dial Up Networking
4 - Headset
5 - Hands-free
6 - Printer & Hard Copy Cable
7 - Human Interface Device

Mobile User with Bluetooth

1. Public Internet
2. Hands-free Speakerphone
3. Synchronization
4. Dial-Up Networking
5. Mobile Data Network
6. Printing
7. Human Interface Devices

Bluetooth PAN
Cellular Data Services
802.11 WLAN
Profiles Used
1 - Serial Cable
2 - Audio/Visual Remote Control
3 - Generic Audio/Visual Distribution
4 - Advanced Audio Distribution
5 - Advanced Video Distribution
The Market

Advertising

- Messages on video screens instructed viewers to place phones in discoverable mode to receive video clips, images, and music.
- Content was relevant and free
- UK advertising firm reports 13,000 positive responses out of 87,000 unique, discoverable handsets
- Viacom is rolling out similar ventures in the U.S.
Bluetooth Security: Why Bother?

Agenda

• The Technology
• The Market
• Security Issues
• Recommendations & Conclusions
Security Issues

Bluetooth Risks

• Actual Threat Envelope
  • 10-30 ft/3-10m

• The “Pringles®” effect

• Bluetooth presents less of a risk than 802.11
  • Range is less
  • Association (pairing) mechanism more strict if enabled
  • Good encryption
Security Issues

Discoverable Mode Exploits

• Bluejacking - sending unsolicited messages to mobile device
• Bluesnarfing - surreptitious file downloads from mobile device
• Bluebugging - using the target mobile to make phone calls and modify call handling

Risk Analysis

• Device must be in discoverable mode for attack to work
• If device placed in discoverable mode, turn off as soon as possible
• Newer devices default discoverable mode to “off” - older devices should be updated or replaced
• Do not respond to advertising campaigns
Security Issues

Pin Length and Key Recovery

• A wireless sniffer may be used to retrieve the authentication and encryption keys
• Once encryption keys are recovered, communications traffic can be read

Risk Analysis

• Encryption keys sent during pairing only
• If pairing exchange is missed, keys are missed
• Pairing can be forced, but special equipment is required
• Forced pairing will be visible on the devices - new PINs must be entered
• Re-pair later in a more private location
• Not a problem with 2.1+EDR
Bluetooth Security: Why Bother?

Agenda

- The Technology
- The Market
- Security Issues

*Recommendations & Conclusions*
Recommendations

• Conduct a risk assessment
• Educate your users on their responsibilities
• Verify the version of Bluetooth in each device - new devices should be at least Version 2.1
• If Bluetooth is not needed in a device, turn it off
• Turn off discoverable mode
• Enable Bluetooth security if that is an option
• Do your Bluetooth pairing in private
• Turn off connection sharing and disable ad hoc networking (file shares)
Conclusions

• The security of mobile devices is a continuing concern
• A risk analysis is the first step in determining the level of protection the enterprise requires
• Bluetooth is here, it’s stable, and it’s secure
• Bluetooth has security risks, but they are minimal in real-world situations and can be mitigated with enough care