Agenda

Four main sections:
• Bluetooth vulnerabilities, the facts and the fiction.
• What attacks are really possible.
• Some solutions.
• Prove it.
Bluetooth vulnerabilities

• Fiction: Lots of vulnerabilities exist within Bluetooth

• Virtually no real Bluetooth vulnerabilities.

• Vulnerabilities generally exist in the service layer

• Analogy: Blaming TCP/IP for an IIS vulnerability
Discoverable modes

- Fiction: Devices in non-discoverable or hidden modes are not vulnerable.
- Does not remove the vulnerabilities.
- Removes “low hanging fruit”.
- Some devices more vulnerable in non-discoverable/hidden.
- Tools already available to find devices
Pairing

- Fiction: pairing is required to exploit vulnerabilities
- Pairing not needed
- Services intentionally open to add functionality
- Some devices do not pair, rely on MAC permissions
Availability 1

- Fiction: vulnerabilities are not well known.
- June 2003.
  - Ollie Whitehouse releases Redfang
- October 2003
  - Bruce Potter talks on Bluetooth vulnerabilities at Defcon
- October 2003
  - Grimm, Holtmann and Vedral discuss Bluetooth OBEX vulnerabilities, later known as Bluesnarfing
  - Pentest release btscanner
Availability 2

- November 2003
  - 'Bluejacking' comes to public attention
  - AL Digital authors advisory on mobile phone “Bluetooth” vulnerabilities. Coined “Bluesnarfing”
  - Pentest releases followup advisory
- February 2004
  - Pentest release Nokia DoS advisory
  - Multiple “Bluetooth vulnerability” articles
Availability 3

- March 2004
  - Integralis release Nokia and Ericsson Serial profile advisory
  - Martin Herfurt scans for Bluesnarfing vulnerabilities at CeBIT
Availability 4

- Multiple tools available to exploit known vulnerabilities
  - btscanner
  - btxml
  - Gnokki
  - OpenOBEX
  - Redfang
  - Many others
Non serious nature

- Fiction: vulnerabilities are not serious in nature.
- Theft or alteration of personal information
- Mobile phone IMEI number availability
- Privacy, tracking
- Complete control of certain devices
- Denial of Service (DoS)
- Airborne viruses and worms
Affected devices

• Fiction: Only a small number of devices are affected.
• High number of devices tested were vulnerable
• Most popular mobile equipment affected
• Not limited to phone handsets.
• Common Bluetooth implementations, BlueZ, Widcomm, Microsoft, Symbian, Nokia etc.
Short range

- Fiction: vulnerabilities are not significant as they are range limited
- Standard dongles are low power and omnidirectional
- 70M line of sight range for a Nokia 6310i
- 450M for two unmodified class 1 devices
- WLAN aerials and amplifiers also work in the ISM band
- Good enough for a large train station
Definitions

- **OBEX – Object Exchange**
  - Binary HTTP
  - Simple GET/PUT or information objects
  - Multiple transports. Bluetooth, IrDA, TCP/IP

- **IrMC – Infrared Mobile Communications**
  - Standard filesystem of objects
  - Access permissions

- Both maintained by http://www.irda.org/
OBEX vulnerabilities

• Attack OBEX/IrMC functionality
  – GET/PUT personal information
  – GET device information: capabilities, IMEI
• OBEX object permissions not followed.
• Same service level abilities on all OBEX profiles
AT/Serial port profiles

- Unprotected serial port profiles
- Used for headset/handsfree profiles
- Issue arbitrary AT commands
  - Talk to the SIM.
  - Make calls (data and voice), GPRS.
  - Send SMS messages.
  - Basically complete control.
AT/OBEX service attacks

- Exploit vulnerabilities in the OBEX or AT parsers
  - Device resets
  - DoS
  - Remote code execution
  - Airborne viruses or worms

- Exploits service implementations, not functions
Solutions

• Preventative solutions
  - Only enable Bluetooth when required
  - Use hidden/non-discoverable modes

• Technical solutions
  - Separate OBEX services
  - Privilege separation
  - Unnecessary channels
Prove It

• TURN OFF BLUETOOTH!
• Demos
  – OBEX/IrMC exploit
  – AT command exploit
  – OBEX implementation exploit