

The Shmoo



Bluesniff - The Next Wardriving Frontier

Bruce Potter <gdead@shmoo.com>

Brian Caswell <bmc@shmoo.com>



Bluetooth Basics

- NOT 802.11! NOT a relative of 802.11!
- Cable replacement technology
 - Low power for embedded devices
- More BT radios than 802.11 radios in existence
 - Phones, headsets, laptops, mice, keyboards
- Master / Slave architecture



Bluetooth Protocol

- Uses 2.4 GHz ISM band, same as 802.11b/g
- Generally low power
 - Class 3 (1mW) for most devices
 - Some Class 1(100mW) devices exist
- Frequency Hopping Spread Spectrum
 - Uses a pre-defined hopping pattern
 - Back in the day, FHSS was a “security” mechanism
 - Resists interference
 - 1MHz wide, hopping every 625 microseconds



Bluetooth Protocol

- A real disaster of a protocol stack
 - Heck, the core spec is 1024 pages.. Good reading!
- Specifies from Layer 1 to Layer 7
- High points
 - RF-level sync
 - Inquiry/request
 - Service discovery
 - Low power modes



Bluetooth Security

- Pairing
 - Using a shared secret (PIN), exchange random number to form key
 - Key used to derive session key for future comms
 - Used for Trusted <-> Trusted comms



Bluetooth Security

- Authentication / Authorization
 - Per connection AA
 - Per service AA
- Encryption
 - Ditto
- It's all OPTIONAL!
 - Left to the developer/user to decide
 - This ends well... :(



Bluetooth Profiles

- Profiles exist to ease interoperability
 - *wink* *wink*
- Keyboard, file transfer, handsfree (and headset), etc...



Bluetooth vs. 802.11b

- More at stake
 - Compromise 802.11 security = Access to network
 - Compromise BT Security = Gateway directly to App level functionality
- More personalized information
 - Phone conversations, calendar info, etc
 - Less interesting for Joe 12-pack, more interesting for executives



Discovery of 802.11

- Direct Sequence Spread spectrum
- Transmitters always in the same “place” in a channel
 - DSSS pretty easy to find
 - Granted, transmitters may be on different channels
 - Cisco - hardware channel switching RF Monitor
 - Prism 2 - firmware channel switching RF Monitor
 - Orinoco - need external channel hopper



Discovery of 802.11

- Beacons
 - “I’m here” every 100ms
 - Can be turned off for “cloaking”
 - Fools Netstumbler
 - Doesn’t fool Kismet or Airsnort
- Regular traffic
 - Windows boxen are noisy
 - Regardless of OS, generally frequent traffic



Discovery of Bluetooth

- FHSS harder to “find”
 - Must align with hopping pattern
 - BT uses 1/2 the normal hop time to Jump Around
 - Still averages 2.5 to 10 secs to find known device
- Devices can be Discoverable
 - Respond to inquiry requests



Discovery of Bluetooth

- Devices can also be non-discoverable
 - Must be directly probed by MAC addr
- Little to no traffic for extended periods of time (esp in low power mode)
 - Cannot easily be listened to b/c receiver cannot sync on hopping pattern
- Sophisticated RF gear can find and intercept traffic
 - Currently no one can make a standard card do this



Bluetooth Attacks

- Interception of traffic during pairing
 - Brute force guess the PIN to recover key
 - Know the PIN b/c it's imbedded
- More likely poorly developed software
 - In BT, security is “optional”
- Or simply bad defaults
 - File sharing with no AA/E in discoverable mode was the DEFAULT for my BT driver on my PDA
 - Just like the early days of 802.11b



Bluetooth Tracking

- Even Class 3 devices can be intercepted at a distance
- If your phone/PDA/earpiece is BT enabled, attacker can follow you using commodity gear
 - Like your own RFID tag



Bluetooth Wardriving

- Used to walk around hitting “scan” button on BT driver UI
- Does not find non-discoverable devices
- Needs new tools to catch on
- Same voyeuristic appeal of 802.11 wardriving
- As it becomes popular, BT developers and users will get a swift kick in the butt to make things more secure



Redfang

- Released by @Stake, Spring 2003
- Looks for devices that do not want to be discovered
 - Brute forces through MAC addresses attempting to find devices
 - First 3 octets fixed, rotates through last three
 - Can take a long time, since FHSS sync can take ~10 seconds per MAC
 - The only way so far...



Bluesniff

- <http://bluesniff.shmoo.com/>
- Our tool (heh.. he said tool...)
- Focused on providing a UI
 - Front-end for Redfang
 - Also finds devices in discoverable mode
 - Yes, people leave things to be discovered
- Making BT wardrivers easier and more efficient will raise awareness of BT security issues



Bluetooth Scanner 0.1

Mon Jul 14 15:49:14 2003

File Record Scan

Devices

HW Address

[Empty list box]

Last Seen

[Empty input field]

First Seen

[Empty input field]

Device Name

[Empty input field]

Version

[Empty input field]

Manufacturer

[Empty input field]

Class

[Empty input field]

Features

[Empty input field]

Signal Strength

[Empty input field]

Link Quality

[Empty input field]

<ESC> to cancel the drop-down menu
<TAB> to move among the widgets
<ENTER> to view details of the device
Use arrows for scrolling



Bluetooth Scanner 0.1

Mon Jul 14 15:49:50 2003

File Record Scan

Devices

Normal Scan

n

First Seen

HW Address

Brute Force Scan

Device Name

Version

Manufacturer

Class

Features

Signal Strength

Link Quality

<ESC> to cancel the drop-down menu
<TAB> to move among the widgets
<ENTER> to view details of the device
Use arrows for scrolling



Bluetooth Scanner 0.1 Mon Jul 14 15:50:11 2003

File Record Scan

Devices Normal Scan n First Seen

HW Address Brute Force Scan

Device Name

Version Manufacturer

Scanning
Starting scanning (normal mode)

Cl

Si lity

OK

<ESC> to cancel the drop-down menu
<TAB> to move among the widgets
<ENTER> to view details of the device
Use arrows for scrolling



Bluetooth Scanner 0.1

(Scanning) Mon Jul 14 15:50:34 2003

File Record Scan

Devices

HW Address

00:80:98:00:1E:41

00:80:98:02:1E:41

Last Seen

2006-09-13 07:29:31

First Seen

2003-07-13 21:42:51

Device Name

lame device

Version

1.1

Manufacturer

cisco

Class

phone

Features

none

Signal Strength

#####80%#####

Link Quality

33%

<ESC> to cancel the drop-down menu
<TAB> to move among the widgets
<ENTER> to view details of the device
Use arrows for scrolling



Future work

- Integration with WiFi scanning tools (namely Airsnort)
- New scanning methods