Privacy Loss in a Pervasive Wireless World

Joshua Wright josh@inguardians.com Check out: www.bradybunchboondoggle.com

Introduction

- Different kind of security discussion
- Pervasive wireless connectivity is a foregone conclusion
- Consumers, enterprises alike rapidly adopting wireless technology
- Highly desirable feature, profitable industry from many perspectives
- Increasingly valuable target to exploit

The Bottom Line ...

Pervasive wireless connectivity threatens consumer privacy, anonymity

- Current security approaches do not adequately address this threat
- Always-on, always-connected devices introduce new security challenges
- Privacy and anonymity not attainable with current well-established technology
- Multiple technology examples (and demos!)

Not a Conspiracy Theorist



Photo credit: Maya Wright (age 7)

Privacy Loss Basics

- Privacy loss comes in convenient and desirable forms
 - TiVo and your freedom to skip commercials
- Privacy loss is (often) asymmetric
 - Patriot Act and FIA exemption
 - ChoicePoint's refusal to turn over data collected on an individual (IPR)
- Privacy is a basic human need

Wireless Privacy Threats

- Wi-Fi anonymity disclosure
- Untraceable keystroke logging
- Proprietary technology threats
- GSM location and call monitoring
- Bluetooth identity disclosure

Wi-Fi Preferred Network List

- List of networks you've previously connected to
- Workstation will frequently probe for network availability

– Discloses past wireless associations

- Not the default in XP SP3 and Vista
 - But often changed to accommodate cloaked SSIDs (and former PCI reqs.)

WiFi Privacy Threat 1

privacy-ssid-disclosure.dump - Wireshark							
<u>File Edit View Go Capture Analyze Statistics H</u> elp							
	7 월 ■ 🗐 €, €, @, 🕾 🕁 🗵 畅 % 💢						
<u>F</u> ilter: wlan.sa == 00:19:7d:1b:03:fa	▼ <u>E</u> xpression <u>C</u> lear <u>A</u> pply						
Destination Protocol Info							
17d:1b:03:fa ff:ff:ff:ff IEEE 802 Probe Request, 77d:1b:03:fa ff:ff:ff:ff IEEE 802 Pro	SN=34, FN=0, Flags=C, SSID = McCarran WiFi" SN=35, FN=0, Flags=C, SSID = "McCarran WiFi" SN=42, FN=0, Flags=C, SSID = "Cox Caesar SLV Rooms" SN=46, FN=0, Flags=C, SSID = "Cox Caesar SLV Rooms" SN=47, FN=0, Flags=C, SSID = "Cox Caesar SLV Rooms" SN=53, FN=0, Flags=C, SSID = "Cox Caesar SLV Rooms" SN=56, FN=0, Flags=C, SSID = "ShadyLadyRanch" SN=63, FN=0, Flags=C, SSID = "ShadyLadyRanch" SN=64, FN=0, Flags=C, SSID = "ShadyLadyRanch" SN=65, FN=0, Flags=C, SSID = "ShadyLadyRanch" SN=66, FN=0, Flags=C, SSID = "ShadyLadyRanch" SN=67, FN=0, Flags=C, SSID = "ShadyLadyRanch" SN=68, FN=0, Flags=C, SSID = "ShadyLadyRanch" SN=68, FN=0, Flags=C, SSID = "Rapid Care Medical Clinic" SN=75, FN=0, Flags=C, SSID = "Rapid Care Medical Clinic"						
<							
Frame 31 (85 bytes on wire, 85 bytes captured) Radiotap Header v0, Length 26 IEEE 802.11 Probe Request, Flags:C IEEE 802.11 wireless LAN management frame "Good" weekend in Vegas?							

WiFi Privacy Threat 2

📶 lawn.dump - Wireshark	
<u>File Edit View Go</u> Capture <u>A</u> nalyze	<u>S</u> tatistics <u>H</u> elp
■■■■■	! ≞ ♀, ҿ ⇔ 彛 ₮ ⊻ ≡ 🗐 ♀, ♀, ◍, ₩ ⊠ № % ໘
Source Destination	Protocol Info
00:13:ce:55:98:ef ff:ff:ff:f	IEEE 802 Probe Rec
00:13:ce:55:98:ef ff:ff:ff:f	IEEE 802 Probe Red Obcorryod during a flight
00:13:ce:55:98:ef ff:ff:ff:ff	
00:13:Ce:55:98:er TT:TT:TT:T	
00:13:ce:55:98:ef ff:ff:ff:f	TEEE 802 Probe Request SN-2185 EN-0 Elags- C SSTD-Broadcast
00:13:ce:55:98:ef ff:ff:ff:f	TEEE 802 Probe Request, SN=2203, FN=0, Flags=C. SSID=Broadcast
00:13:ce:55:98:ef ff:ff:ff:f	IEEE 802 Probe Request, SN=2204, FN=0, Flags=C. SSID=Broadcast
00:13:ce:55:98:ef ff:ff:ff:f	IEEE 802 Probe Request, SN=2205, FN=0, Flags=C, SSID=Broadcast
00:13:02:b3:03:a8 ff:ff:ff:f	IEEE 802 Probe Request, SN=55, FN=0, Flags=C, SSID=Broadcast
00:13:02:b3:03:a8 ff:ff:ff:f	IEEE 802 Probe Request, SN=60, FN=0, Flags=C, SSID=Broadcast
00:13:ce:55:98:ef ff:ff:ff:f	IEEE 802 Probe Request, SN=2228, FN=0, Flags=C, SSID=Broadcast
00:13:ce:55:98:ef ff:ff:ff:f	IEEE 802 Probe Request, SN=2229, FN=0, Flags=C, SSID="stayoffmylawn"
00:13:ce:55:98:ef ff:ff:ff:ff	IEEE 802 Probe Request, SN=2230, FN=0, Flags=C, SSID=Broadcast
00:13:Ce:55:98:er TT:TT:TT:T	TEEE 802 Probe Request, SN=2231, FN=0, FTags=C, SSID= StayOTTMyTawn
00:13:ce:55:98:ef ff.ff.ff.f	TEEE 802 Probe Request SN=2252, FN=0, Flags=C, SSID Broducast
00:13:ce:55:98:ef ff:ff:ff:f	TEEE 802 Probe Request, SN=2268, EN=0, Flags=C. SSID Broadcast
00:13:ce:55:98:ef ff:ff:ff:f	IEEE 802 Probe Request, SN=2269, FN=0, Flags=C. SSID="stavoffmylawn"
00:13:ce:55:98:ef ff:ff:ff:f	IEEE 802 Probe Request, SN=2270, FN=0, Flags=C, SSID=Broadcast
00:13:ce:55:98:ef ff:ff:ff:f	IEEE 802 Probe Request, SN=2271, FN=0, Flags=C, SSID="stayoffmylawn"
00:13:ce:55:98:ef ff:ff:ff:f	IEEE 802 Probe Request, SN=2272, FN=0, Flags=C, SSID=Broadcast
00:1e:4c:75:b7:1f ff:ff:ff:f	IEEE 802 Probe Request, SN=8, FN=0, Flags=C, SSID="McCarran WiFi"
00:1e:4c:75:b7:1f ff:ff:ff:f	TEEE 802 Probe Request, SN=9, FN=0, Flags=C, SSID="McCarran WiFi"
•	4 11
H Frame check sequence: 0x8	A4ersor [connect]
🖃 IEEE 802.11 wireless LAN ma	nagement frame
🗆 Tagged parameters (31 byt	25)
SSID parameter set: "st	ayoffmylawn"
B Supported Rates: 1.0(B)	2.0(B) 5.5 11.0 6.0 9.0 12.0 18.0
🗄 Extended Supported Rate	5: 24.0 36.0 48.0 54.0

www.wigle.net

🥹 WiGLE - Wireless Geographic Logging Engine - Plotting WiFi on Maps - Mozilla Firefox							
ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp							
C × ☆ (http://www.wigle.net/	Q						
Home Download Forums Post File Query Screenshots Stats Uploads Web Maps MapPacks/Trees Wiki Login	Í						
(%) VIGLE.NET	Е						
Wireless Geographic Logging Engine: Making maps of wireless networks since 2001							
16,224,612 points from 957,380,561 unique observations.							
ogin user: password: login login Don't expire auth cookie <u>non-ssl</u> or <u>make a new account</u>							
news: 16mm Mon Jan 12 08:55:03 2009 The WiGLE counters reach another million mark, this time on a nice power of 2. Congratulations to 'nowhereboy' Exception this morning (GMT-6:00).	-						
The next occasion looks to be the billionth observation data point. As							
Add a wireless network to WiGLE [from a stumble file] or [by hand]							
the seven year itch The Sep 9 10:39:40 2008 Add [remarks] to an existing network(must be registered) Done	-						

Search Results

😻 WiGLE - Wireless Geographic Logging Engine - Plotting WiFi on Maps - Mozilla Firefox							- X												
<u>F</u> ile	<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp																		
C X A (http://www.wigle.net/gps/gps/main/confirmquery/ S C · Google								,	ρ										
	Home Download Forums Post File Query Screenshots Stats Uploads Web Maps MapPacks/Trees Wiki Logout																		
Showing stations 1 through 3 of this query.																			
map it	netid	ssid	comment	name	type	freenet	paynet	firsttime	flags	wep	trilat	trilong	dhcp	lastupdt	channel	active	bcninterval	qos	use
<u>Get</u> Map	00:0C:41:AC:8A:89	stayoffmylawn			BSS	?	?	2007-06-14 08:47:04	2001	N	41.77667236	-71.37814441	?	20090217133027	6	Y	100	2	
<u>Get</u> Map	00:13:CE:55:98:EF	stayoffmylawn			BSS	?	?	2008-02-14 21:30:24		N	38.92541885	-77.05648804	?	20090216155333	1	Y		0	
<u>Get</u> Map	00:13:ce:33:ef:b9	stayoffmylawn			infra	?	?	2009-02-04 07:03:29		Y	41.78056335	-71.39854431	?	20090217135602	11	Y		0	
	WiGLE Home																		

Privacy Loss in a Pervasive Wireless World © 2009

ш

Þ

Location Analysis



WiFi Privacy Defense

- Update clients to XP SP3 or Vista
- Disable cloaked or "hidden" SSID on APs
- Prevent clients from disclosing SSID

methingclever Wireless Network properties								
Connection Security								
Name: somethingdev SSID: somethingdev Network Type: Access point Network Availability: All users	ver ver network is in range work in available the bradcasting							
	, produced any							
Configure	somethingclever pr	opert	ies	?×				
	Association Authenticatio	n Con	nection					
Vista	Connect even if this	s networ	k is not broadcasting)				
	This network requires a	ı key for	the following:					
	Network <u>A</u> uthentication	n:	WPA-PSK	~				
	Data encryption:		TKIP	~				
	Network <u>k</u> ey:	•••	•••••					
	Confirm network key:	•••						
	Key inder (12) Ped)	SP	Batically					
	This is a <u>c</u> omputer-to-o access points are not	compute used	r (ad hoc) network; wi	ireless				

Cancel

Wireless Keyboards

- Increasingly deployed item for desktop systems
- Marketed as a freedom tool, allowing consumers to work "as they wish"
- 27 MHz variety, inexpensive, common



Microsoft Optical Wireless Desktop Analysis

- Assessment of popular keyboard from Microsoft (Moser, Schrödel)
- Detailed the observed behavior of unassociated, associated keyboards
 Manual analysis, data taps and bus sniffers
- Described the data framing and packet types, security flaws
- Released video of attack tool
- Presented at Blackhat Federal 2008

27 MHz Keystroke Sniffing

$\overline{}$	Keyboard POC	$-\Box X$	
КΒ	[0100111] EOT PACKET: 01001110001110111000010		
KB	[0100111]: [44]		
KB.	[0100111] KEYSTROKE PACKET: 01001110101010000000000111110100001100		
KB.	[0100111] EOT PACKET: 01001110001110111000010		
KB.	[0100111]: [18] o		
KB	[0100111] KEYSTROKE PACKET: 010011101011101000000000111110100000101		
KB	[0100111] EOT PACKET: 01001110001110111000010		
KВ	[0100111]: [25] ν Υ		
KB	[0100111] KEYSTROKÉ PACKET: 01001110100110000000000111110100010110		
KB	[0100111] EOT PACKET: 01001110001110111000010		
KB	[0100111]: [8] e		
KВ	[0100111] KEYSTROKE PACKET: 01001110101000100000000111110100010001		
KB	[0100111] EOT PACKET: 01001110001110111000010		
KB	[0100111]: [21] r		
KB	[0100111] KEYSTROKE PACKET: 0100111011100110000000001111101111011		
KB	[0100111] EOT PACKET: 01001110001110111000010		
КВ	[0100111]: [55] .		
KR	[0100111] KEYSTROKE PACKET: 0100111011100110000000011111011110111		
	KB:[0100111] KEY1:[0x00] KEY2:[0x44] I2	C:[0x0	0 0x0 _ □ >

there a a lotofways tcrack ito acompanys most secret files. bobby spent a few da ys mulling over...

Untraceable Keystroke Logging

- Short-range exploit, but significant confidentiality impact
- Completely passive, little opportunity for post-compromise forensics
- Significant privacy exposure over obscure wireless mechanism
 - URL's you visit, email you type, passwords, etc.
- Practical attack requires non-practical hardware tools (\$1K/USD, not portable)

Next-Generation Keystroke Logger Prototype



Privacy Loss in a Pervasive Wireless World © 2009

Nike + iPod Sport Kit

- Sneaker insert module and accompanying receiver
- Integrates with iPod Nano
 - Audible distance and speed to runner
 - Records runner statistics
- Sneaker insert is TX only, always-on





• \$29/USD at store.apple.com

U. Washington Analysis

- November 2006 paper "Devices that Tell On You"
 - Analysis of hardware between in-sneaker sensor and receiver
- 1-30M range, 32-bit UID for each sensor
- Always-on sensor, always-on location tracking



Distributed Nike+iPod Monitoring

- Sensors identify Nike+iPod users
- Optional: automated photography of area
- Record 32-bit UID
- Plot on map
- Track movement



SparkFun Nike+iPod Serial Adapter

- Emulate Nano interface on receiver, report over USB/Serial
- \$25/USD
- Sample VB source for custom devel

www.sparkfun.com



Proprietary Technology Privacy Defense

- Awareness of privacy threats in proprietary technology
 - Avoid wireless keyboards
 - Enforce strong physical security practices (stay away from windows)
- Recognize location and tracking disclosure threats
- Consider other wireless devices you use

Oral B Triumph Wireless Toothbrush

GSM Technology

- Digital mobile communication protocol
 Over 2 billion users worldwide
- Utilized by AT&T, T-Mobile in US
- Popular throughout the world
- Supports SMS message transport
- Partially protected by weak encryption
- GSM sniffers can be built for ~\$1200

USRP GSM Traffic Capture Example

	K sms.txt + (~\Desktop) - GVIM1
🔏 sms.txt (~\Desktop) - GVIM1	File Edit Tools Syntax Buffers Window Help Caller Phone #
<u> E</u> ile <u>E</u> dit <u>T</u> ools <u>S</u> yntax <u>B</u> uffers <u>W</u> indow <u>H</u> elp	
addela qix de bababal 4.4.8	Berlin, Germany
	6: 91 -001 International Numer
H Callor IMCT Format Bbis DATA	6: 910001 Numbering plan: ISDN/telephone (E164/E.163)
0 CAIICI IIVIJI 64 30 - 60 02 02 48 32 26 2	7: 73 Number (6): 37068499199
8	13: UU UUUUUUUU Destination Address Length: U
0: 31 001100 Pseudo Length: 12	15: 0400 IP-MII: SMS-DELIVER (->MS)
1: V6 V Virection: From originating site	15: 041 more messages (IP-mms): NO
1: 06 -000 0 TransactionID	15: 040 Status Report Indication (IP-SRI)
1: 060110 Radio Resouce Management	15: U4 -U User Data Header Indicator (IP-UDHI): No
2: 21 00100001 Paging Request Type 1	15: 04 0 Reply Path (TP-RP)
3: 0000 Page Mode: Normal paging	16: UD UUUUIUII Uriginating (TP-UA) Address Length: 11
5: 29OUT Type of identity: IMSI	17: 91 1 Extension
6: 64 1D(7/odd0: 246030620208423	17: 91 -001 International Number
HEX 12_data_out_Bbis:390 Format_Bbis_DATA	17: 910001 Numbering plan: ISDN/telephone (E164/E.163)
000: 49 06 1b 40 5c 42 f6 30 - 00 04 48 07 c8 14 8	18: 73 Number(11): 37067659766
001: 65 00 00 80 00 00 1b	24: 00 00000000 Protocol Identifier: 0x00
0: 49 010010 Pseudo Length: 18	24: 00 0000000 normal
1: 06 O Direction: From originating site	25: 00 0000000 Default Data Codin SMS Message
1: 06 -000 0 TransactionID	26: 70 SMSC Timestamp: 07
1: 060110 Radio Resouce Management	33: 03 00000011 User Data Length (TP-UDL): 3 symbols
2: 1b 00011011 RRsystemInfo3C	37: 00(- Content: abc
3: 40 16476 [0x405c] Cell identity	HEX 12_data_out_B: We Format B DATA
5: 42 246 Mobile Country Code	000: 03 03 49 06 1d 10 00 00 - 00 00 00 01 00 00 00 08 🛛 👱
6: f6 03f Mobile Network Code	2259,45 76%
	1330,1 44%

GSM Sniffing Exposure

 Anonymity threatened through IMSI disclosure in plaintext

– Location analysis to 1/4 mile

- Accommodates wide-spread analysis from multiple receivers
- Currently available to LEA, but straightforward to implement for unauthorized purposes



GSM Privacy Defense

This slide intentionally left blank.

Bluetooth Technology

- Ubiquitous in modern phones
- Range between 1M and 100M
 10M most common
- Each device uses a globally unique 48-bit MAC address (BD_ADDR)
- Device names often associate a person with MAC address
- RSSI analysis reveals location history and associations with other Bluetooth users
- Non-discoverable mode recommended to hide BD_ADDR from eavesdroppers (Bluetooth SIG)

LR3 DESIGNED FOR THE EXTRAORDINARY

5

红

<u>r</u>

76

13

MM

-

CLEAR CHANNEL

MM

E WAY

E

12

State data

17-

SAPPORO

PRENIUM BEER

Conguest

1



Make your Bluetooth[®] handset discoverable and get the whole story now.

NC

STARBUC

THE LF

A Crumby Commercial?



LR3 DESIGNED FOR THE EXTRAORDINARY

5

红

<u></u>

76

13

MM

-

CLEAR CHANNEL

MM

E WAY

E

12

James Jam

17-

SAPPORO

PRENIUM BEER

OMOUNT

1



Make your Bluetooth[®] handset discoverable and get the whole story now.

NC

STARBUC

THE LF





Identifying Non-Discoverable Devices

- Even in non-discoverable mode, possible to identify BD_ADDR
 - Software Defined Radio tools
 - Commercial Cognio Spectrum Analyzer
- Can probe for device presence, or passively analyze spectrum
 - Requesting device name
 - OSX/iPhone name coordination behavior

```
$ hcitool name 00:1b:63:5d:56:6c
```

Joshua Wrightâs iPhone

BT Anonymity Attacks

- Businesses tracking repeat visitors
 - "Welcome back "Josh's Phone", it's been 12 days since you were last here. Here are our new products..."
- Associating individuals, people meeting each other
- Tracking a user's location
- Records turned over to police on subpoena?

Disclosing where you are, where you have been, and the people you associate with.

Bluetooth Privacy Defense

- Disable discoverable mode
 - Marginal improvement, not a comprehensive defense
- Use an impersonal Bluetooth device name
- If not needed, disable Bluetooth altogether

Conclusion

- Privacy is an important right, not to be relinquished lightly
- Wireless technology makes it *easier* to compromise your privacy
 - Pervasive across Wi-Fi, Bluetooth, GSM, proprietary devices
- Lack of privacy retention demand perpetuates weak technology

What catastrophic/life-threatening event is needed to tell designers that privacy is important to us?

Thank You!

Joshua Wright Senior Security Analyst InGuardians, Inc. josh@inguardians.com 401-524-2911



INGUARDIANS^{®M}

DEFENSIVE INTELLIGENCE

Also check out:

www.bradybunchboondoggle.com

Quis custodiet custodes ipsos?