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

Chef-style TFH

Pragmatist

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

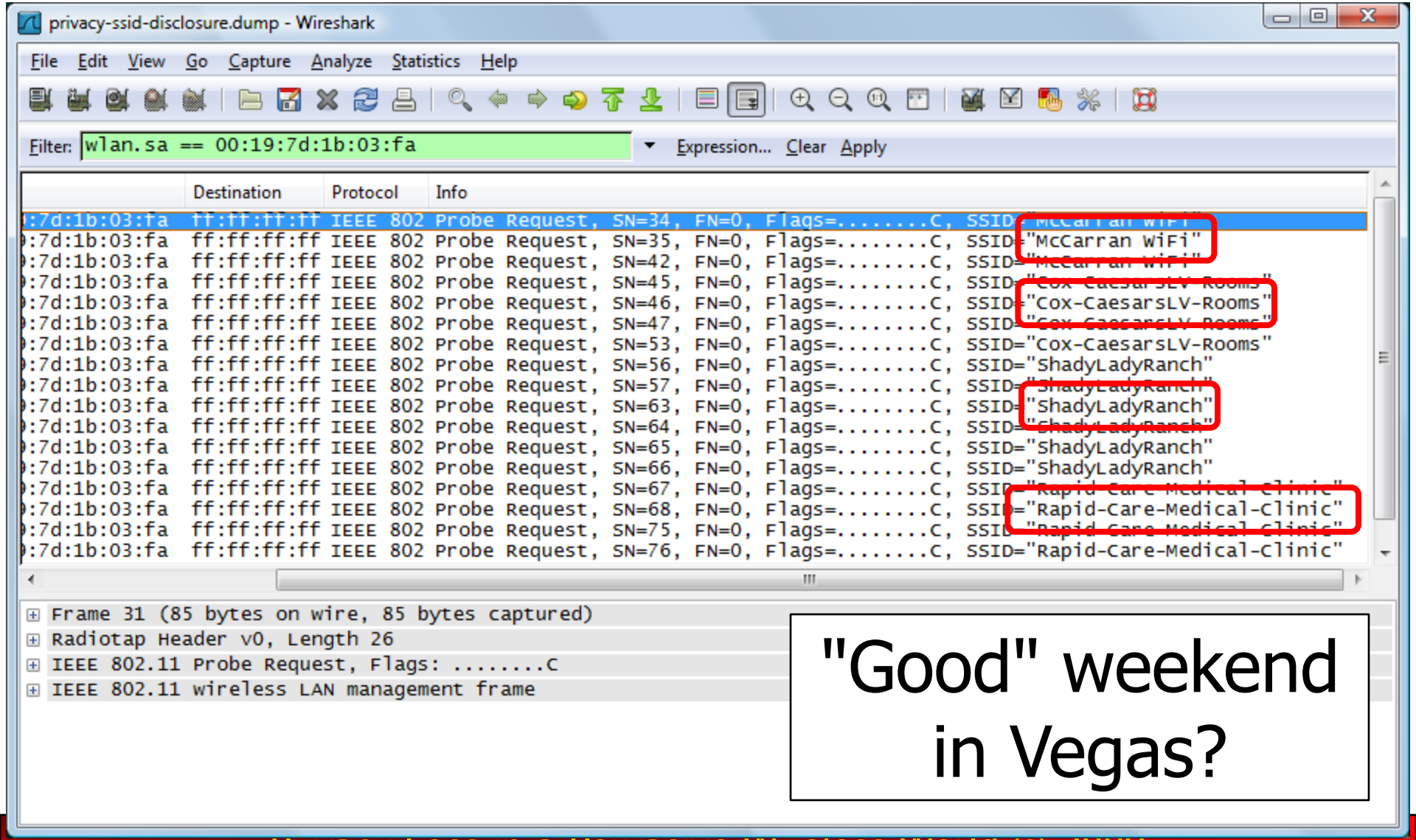
Wireless Privacy Threats

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

Wi-Fi Preferred Network List

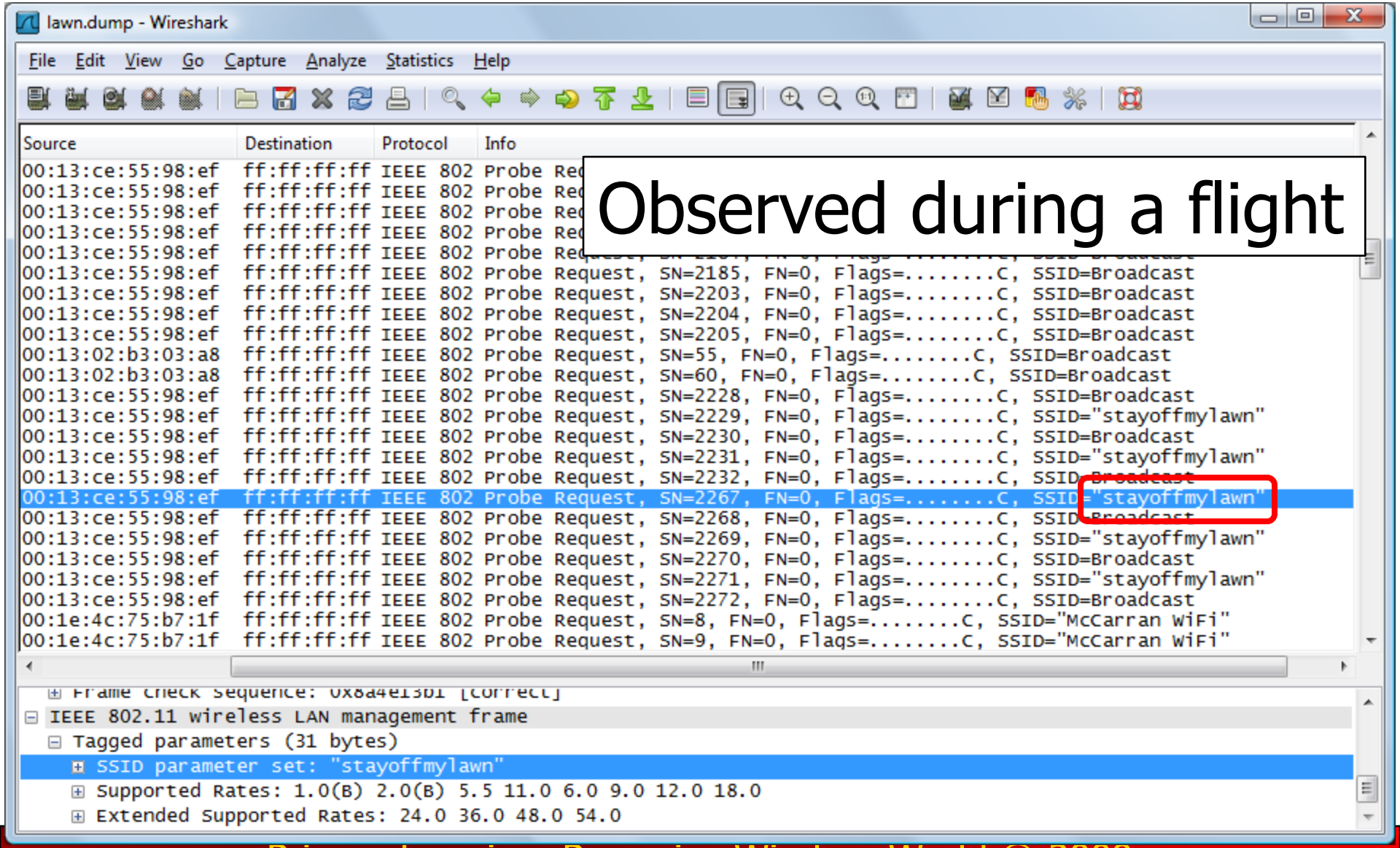
- List of networks you've previously connected to
- Workstation will frequently probe for network availability
  - Discloses past wireless associations
- Not the default in XP SP3 and Vista
  - But often changed to accommodate cloaked SSIDs (and former PCI reqs.)

WiFi Privacy Threat 1



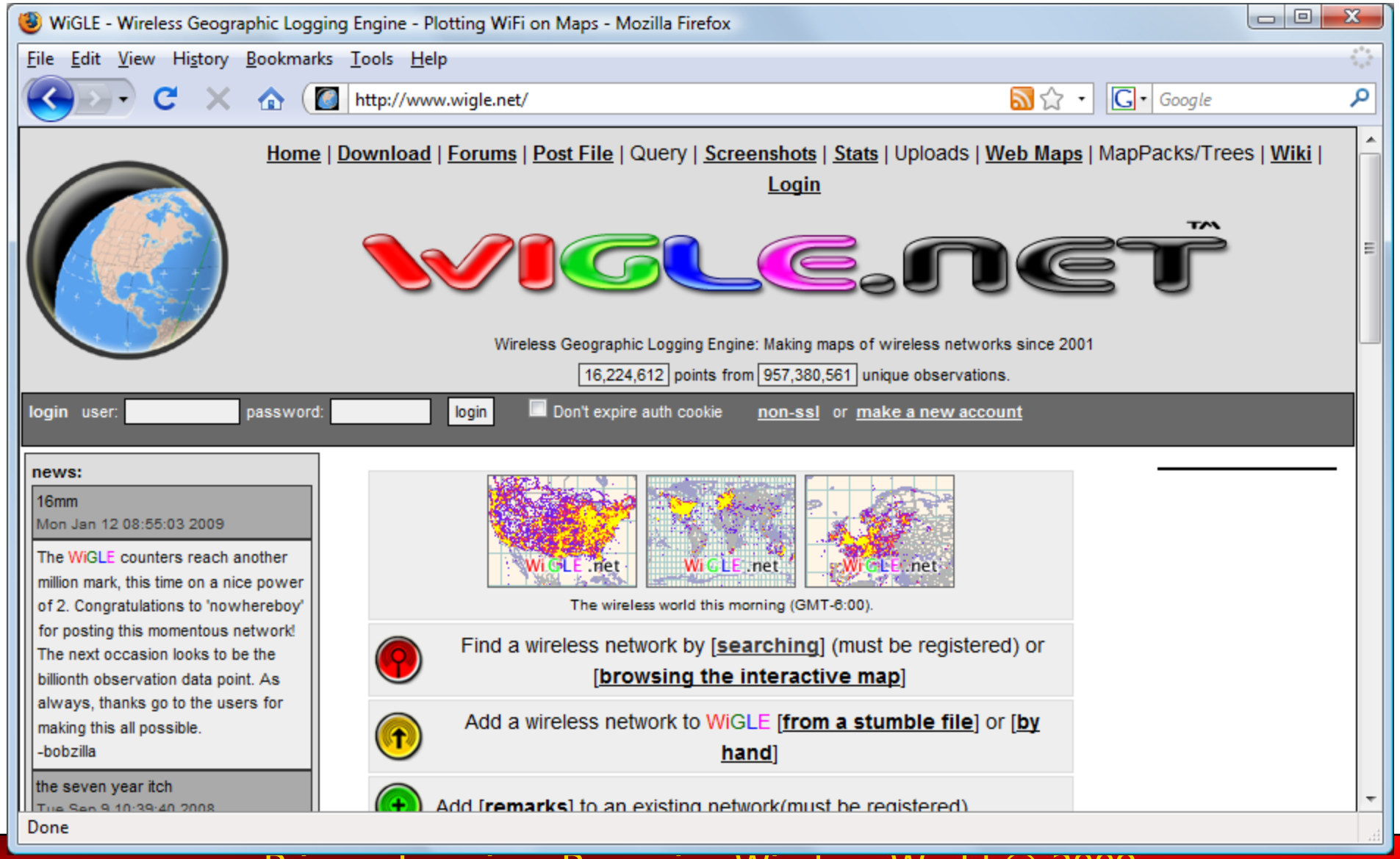
"Good" weekend in Vegas?

WiFi Privacy Threat 2

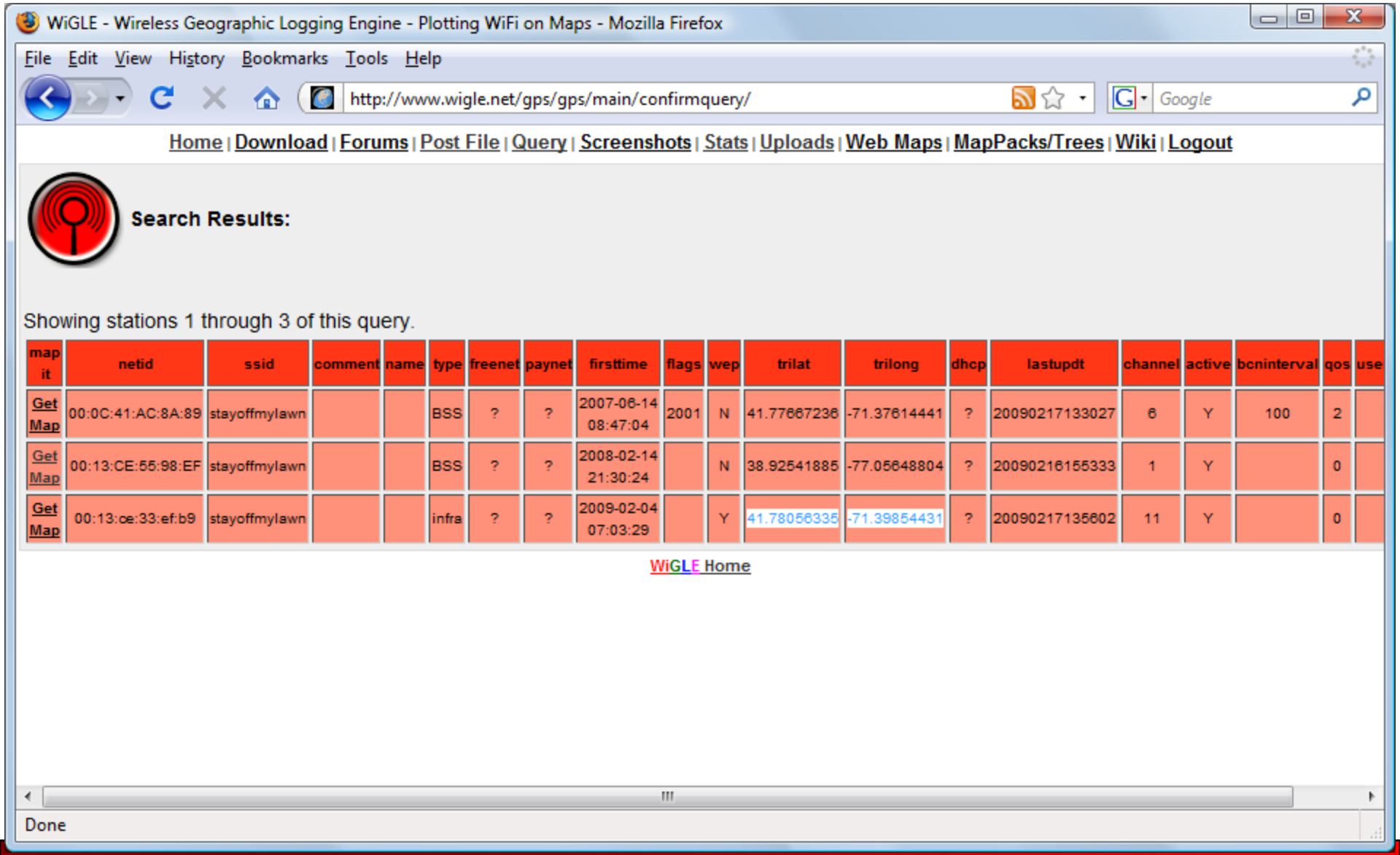


Observed during a flight

www.wigle.net

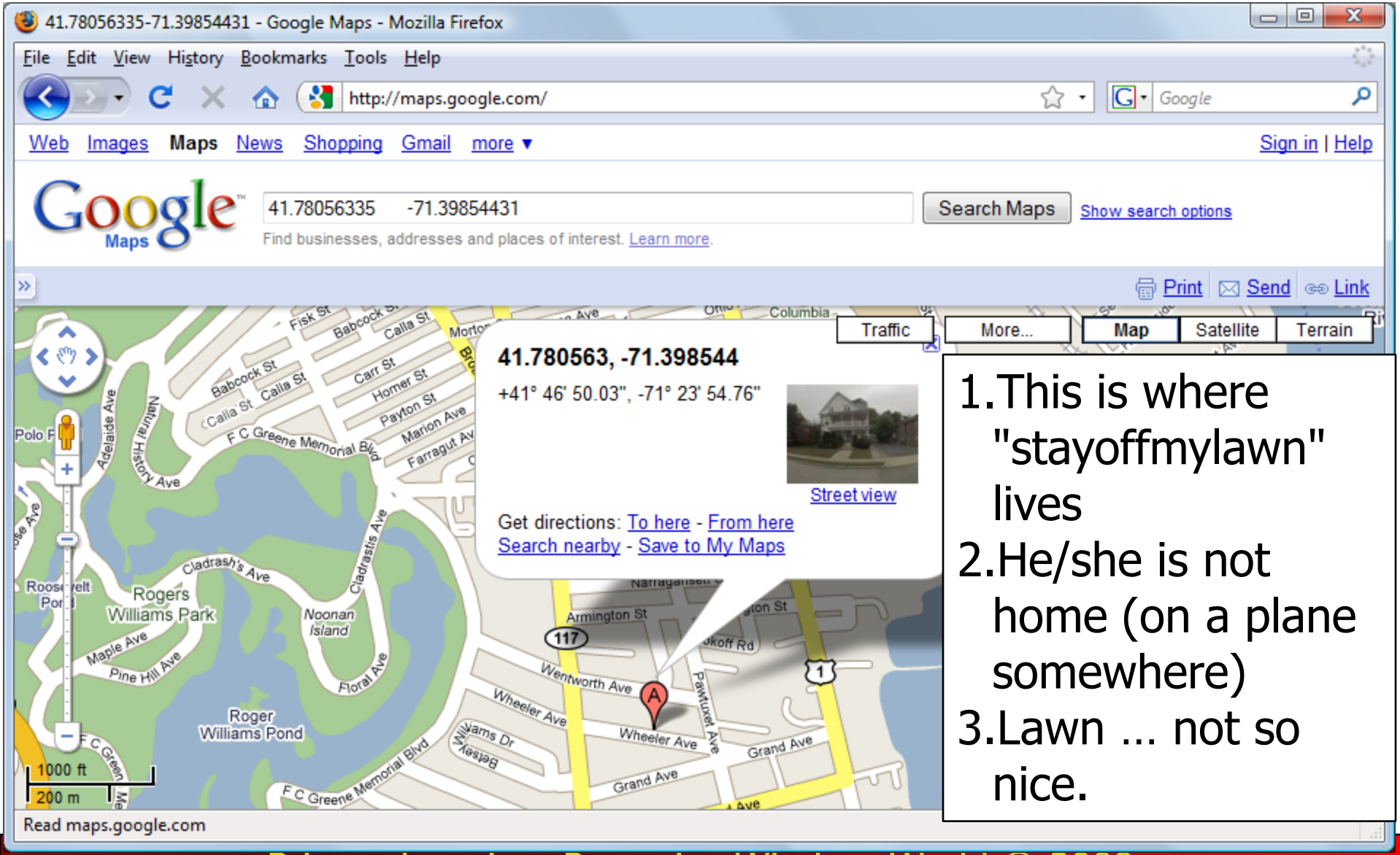


Search Results



map it	netid	ssid	comment	name	type	freenet	paynet	firsttime	flags	wep	trilat	trilong	dhcp	lastupdt	channel	active	bcninterval	qos	use
Get Map	00:0C:41:AC:8A:89	stayoffmylawn			BSS	?	?	2007-06-14 08:47:04	2001	N	41.77667236	-71.37614441	?	20090217133027	6	Y	100	2	
Get Map	00:13:CE:55:98:EF	stayoffmylawn			BSS	?	?	2008-02-14 21:30:24		N	38.92541885	-77.05648804	?	20090216155333	1	Y		0	
Get Map	00:13:ce:33:ef:b9	stayoffmylawn			infra	?	?	2009-02-04 07:03:29		Y	41.78056335	-71.39854431	?	20090217135602	11	Y		0	

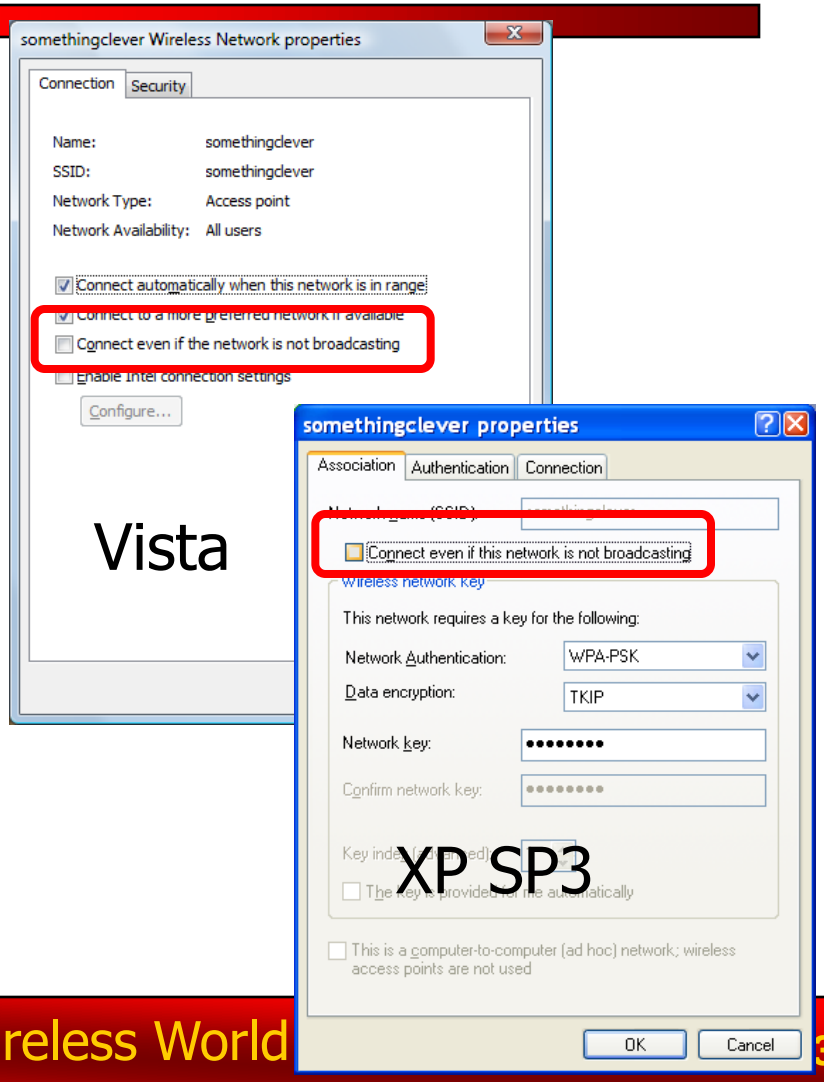
Location Analysis



1. This is where "stayoffmylawn" lives
2. He/she is not home (on a plane somewhere)
3. Lawn … not so nice.

WiFi Privacy Defense

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



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

27 MHz

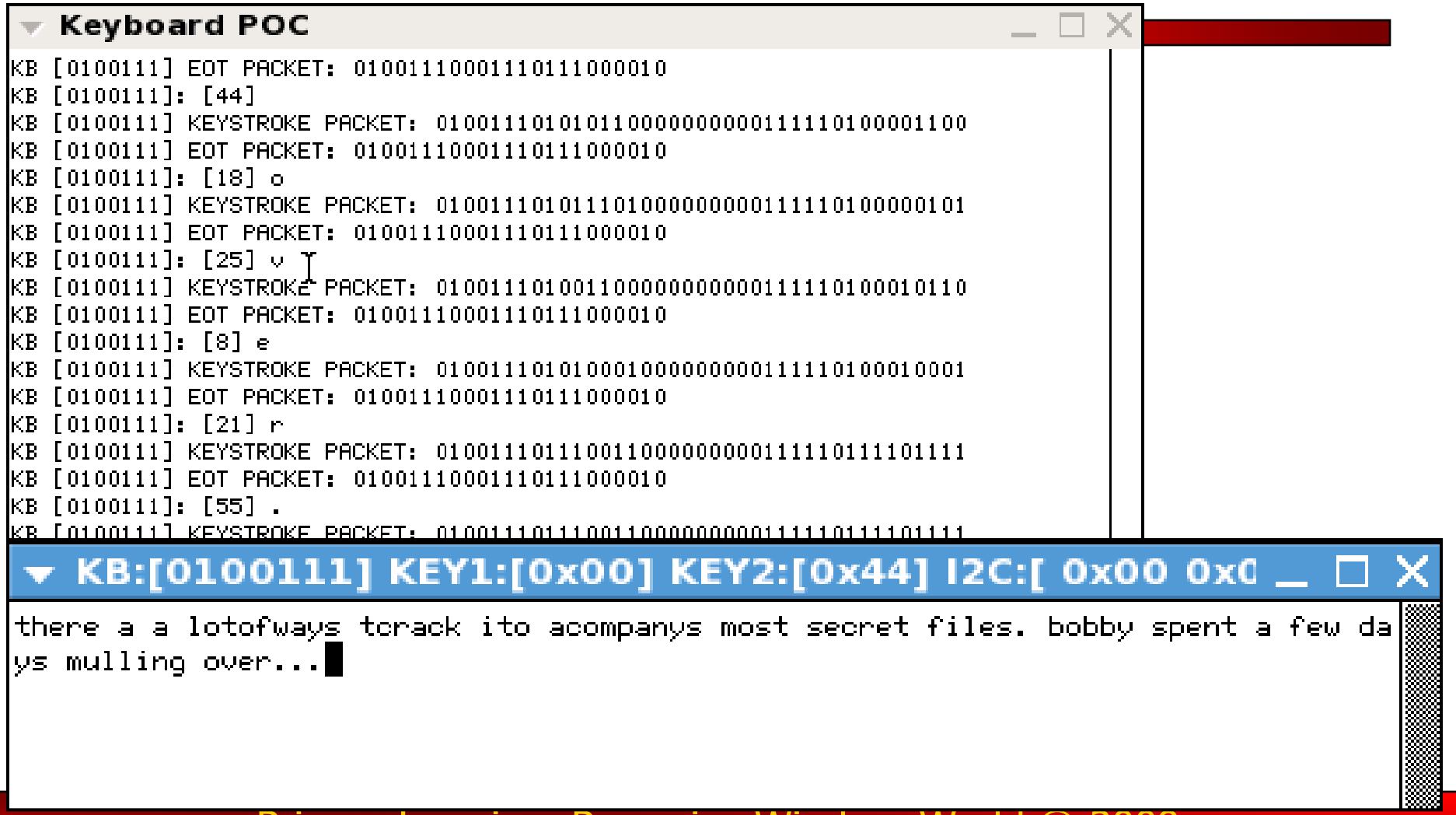
IR

Bluetooth

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

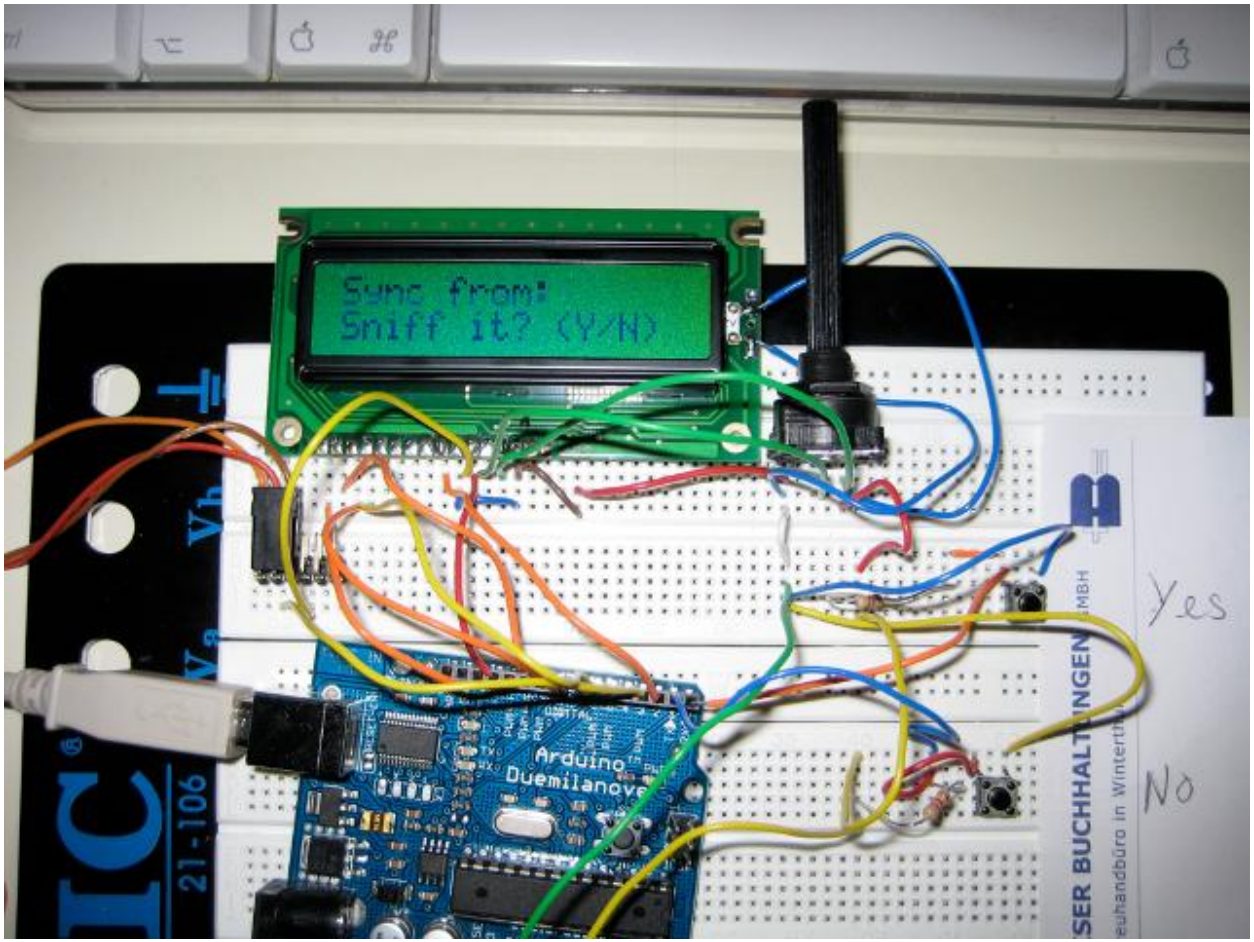
27 MHz Keystroke Sniffing



Untraceable Keystroke Logging

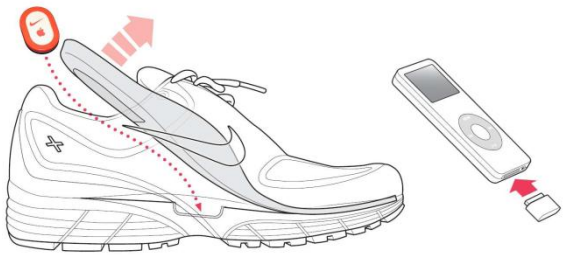
- Short-range exploit, but significant confidentiality impact
- Completely passive, little opportunity for post-compromise forensics
- Significant privacy exposure over obscure wireless mechanism
  - URL's you visit, email you type, passwords, etc.
- Practical attack requires non-practical hardware tools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

Next-Generation Keystroke Logger Prototype



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

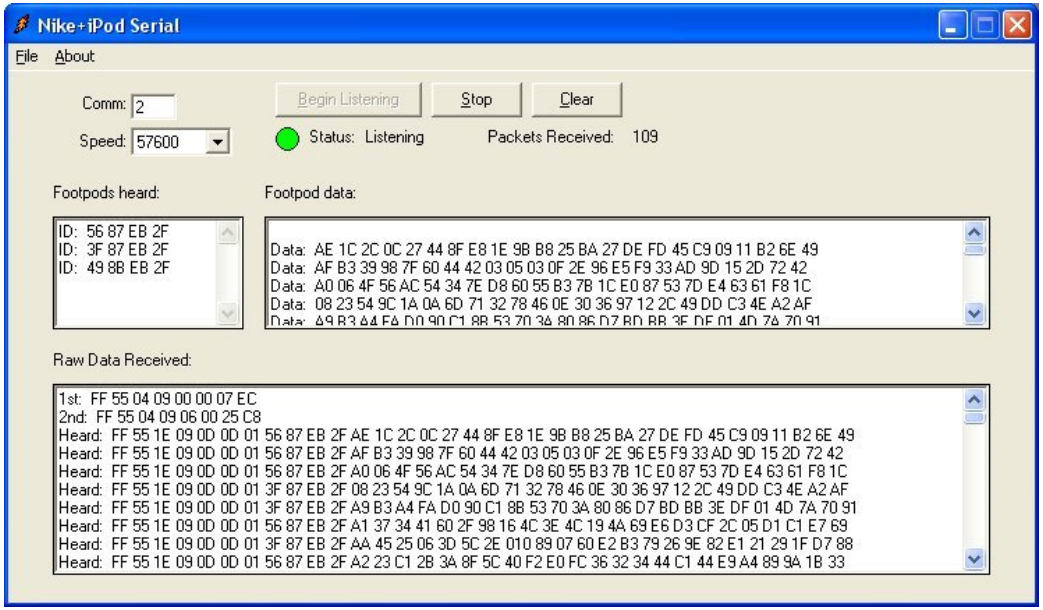
Distributed Nike+iPod Monitoring

- 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

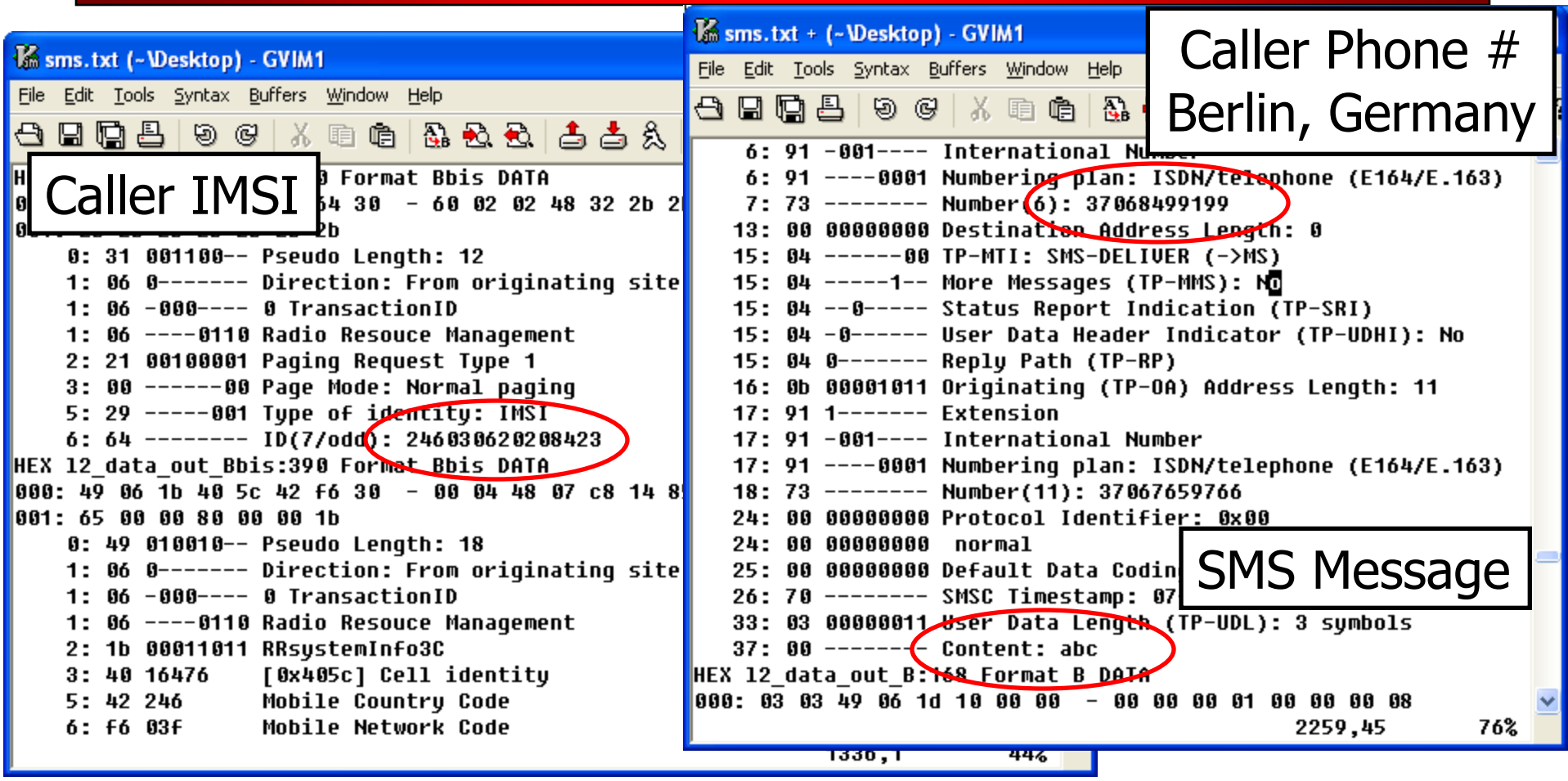
- Awareness of privacy threats in proprietary technology
  - Avoid wireless keyboards
  - Enforce strong physical security practices (stay away from windows)
- Recognize location and tracking disclosure threats
- Consider other wireless devices you use

Oral B Triumph Wireless Toothbrush

GSM Technology

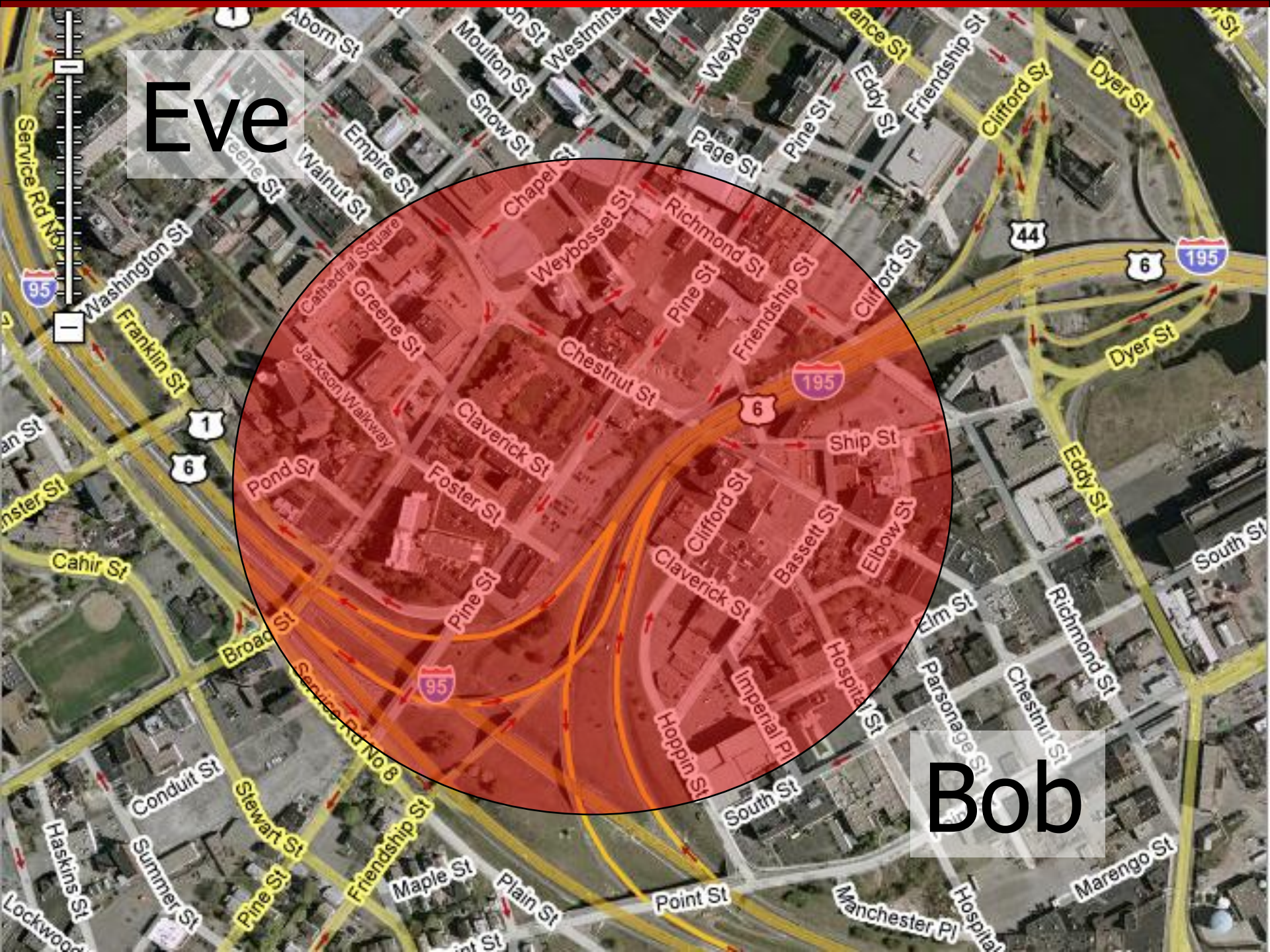
- Digital mobile communication protocol
  - Over 2 billion users worldwide
- Utilized by AT&T, T-Mobile in US
- Popular throughout the world
- Supports SMS message transport
- Partially protected by weak encryption
- GSM sniffers can be built for ~$1200

USRP GSM Traffic Capture Example



GSM Sniffing Exposure

- Anonymity threatened through IMSI disclosure in plaintext
  - Location analysis to ¼ mile
- Accommodates wide-spread analysis from multiple receivers
- Currently available to LEA, but straightforward to implement for unauthorized purposes


Eve
Bob
Service Rd No 1
Washington St
Franklin St
Cahir St
Broad St
Service Rd No 8
Conduit St
Stewart St
Friendship St
Haskins St
Summer St
Pine St
Maple St
Plain St
Point St
Manchester Pl
Marengo St
South St
Elm St
Parsonage St
Chestnut St
Richmond St
Eddy St
Dyer St
Clifford St
Ship St
Hospital St
Imperial Pl
Hoppin St
Bassett St
Elbow St
Claverick St
Foster St
Pond St
Jackson Walkway
Greene St
Cathedral Square
Chapel St
Weybosset St
Richmond St
Pine St
Friendship St
Chestnut St
Empire St
Walnut St
Snow St
Moulton St
Aborn St
Page St
Eddy St
Friendship St
Clifford St
Dyer St
44
6
195
95
1

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)


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.
ClearChannel
SPECTACOLOR
ONE WAY
GNC
STARBUCKS
COFFEE
750

A Crumby Commercial?


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
750
Me


thank
ICE
EXIT
CRAVE CARBS?
Please Alert Cashier to Heavy Items in Cart.
Items can be re-entered for your Convenience.


Bluetooth


BD Address:000CA7041F47

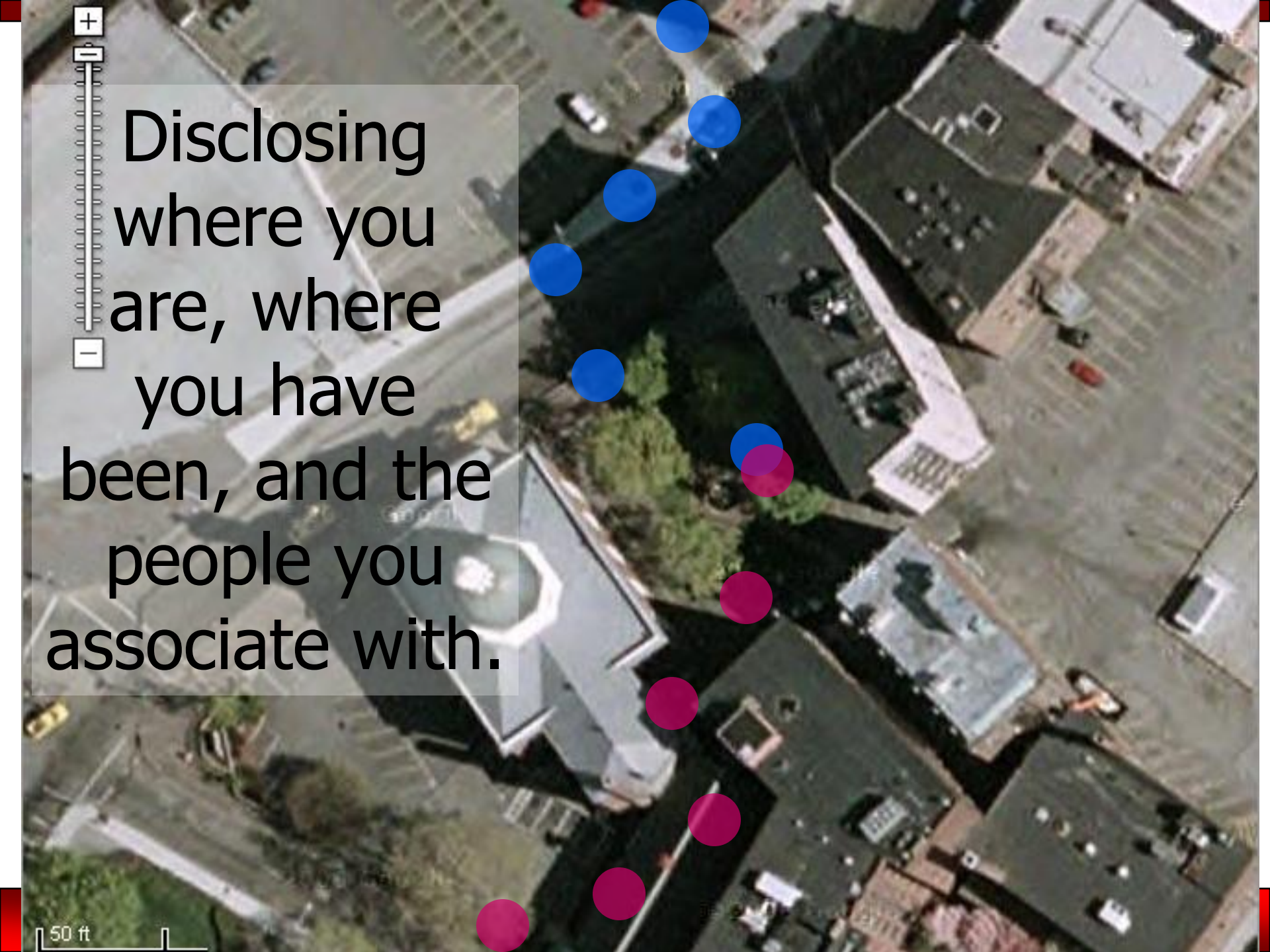
Identifying Non-Discoverable Devices

- 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.
50 ft

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

Also check out:
www.bradybunchboondoggle.com

Quis custodiet custodes ipsos?