Joshua Wright
Senior Security Researcher

ARUBA networks

Introduction

- 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
- Wireless keyboard, GSM, Bluetooth examples

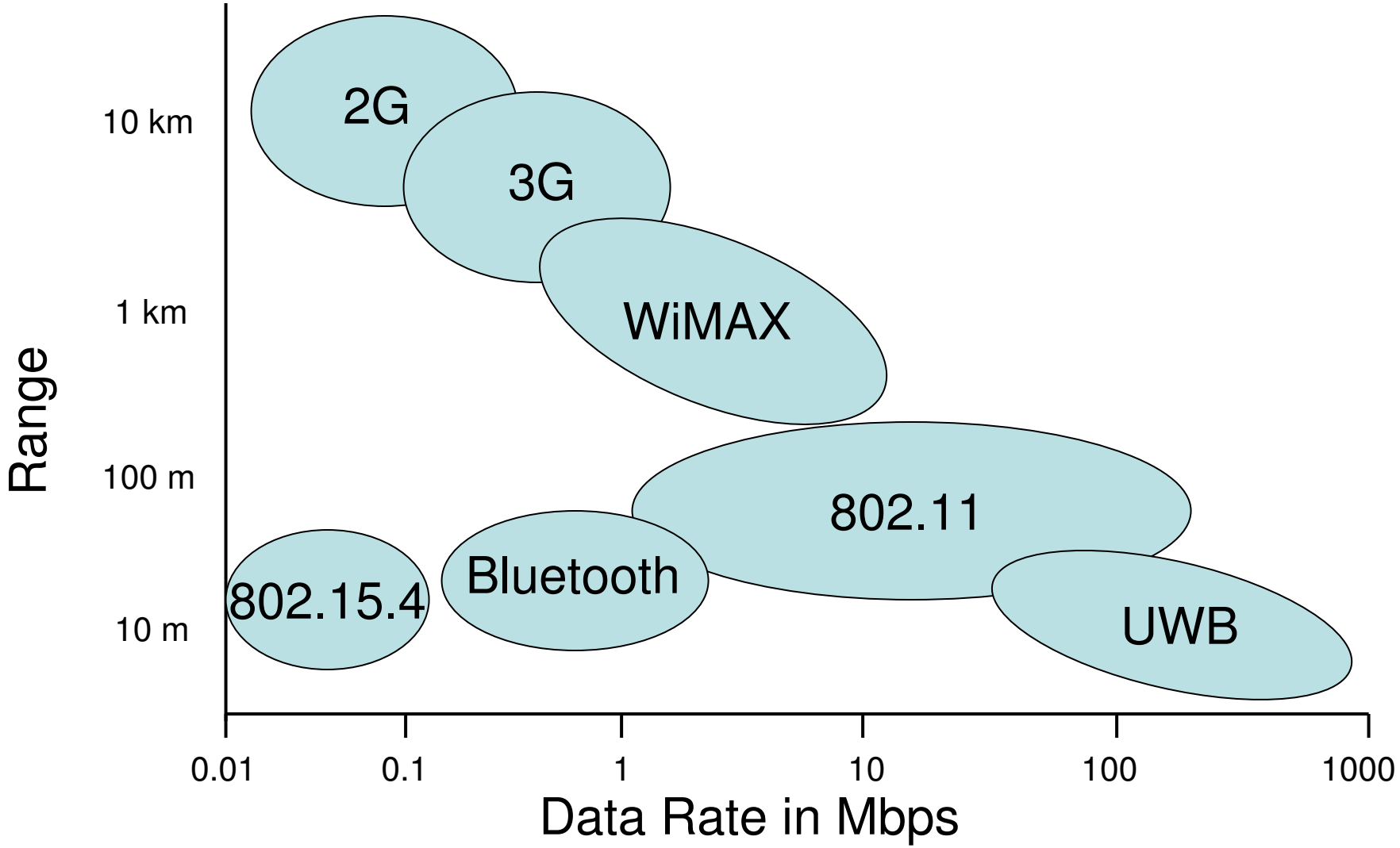
ARUBA networks

Trends in Mobility

- Mobile phones emerging as the next-generation computing platform
- Consumers increasingly adopting short-range wireless to extend features of 3G
- New application opportunities
- Bluetooth peripherals gaining popularity
- WiFi enterprise and consumer deployments gaining universal acceptance

ARUBA networks

Wireless Deployments and Availability

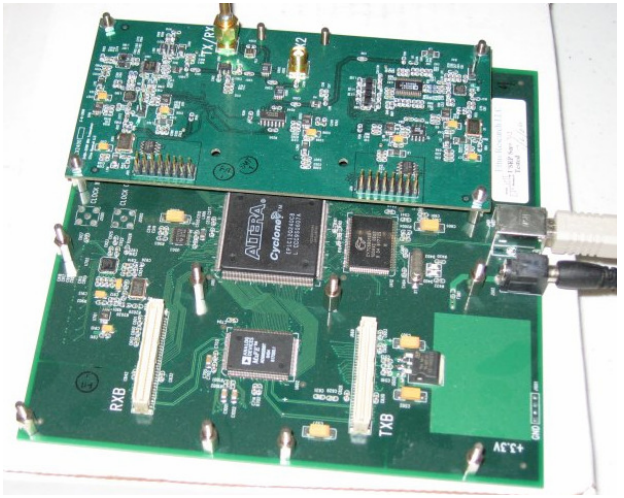


Source: Wireless Communications: The Future, William Webb

ARUBA networks

Software Defined Ratio (SDR)

- Universally accessible, new access to wireless spectrum
- Freedom of software accommodates flexibility, dynamic manipulation of modulation, MAC layers
- SDR easily accessible through USRP/GNURadio project
- New research, experiment opportunities
- Lots of opportunity for disruptive innovation



ARUBA networks

Field Programmable Gate Array (FPGA)

- Speed and form-factor of hardware
- Flexibility of freedom of software
- Falling costs and power requirements make FPGA's increasingly useful in embedded devices

The Evil Side of SDR/FPGA

- SDR and FPGA technology clearly useful for good, also useful for evil
- Well established protocols maintained security through obscurity in limited accessibility
  - 1800 MHz sniffers costly, not easily accessible
  - Proprietary modulation and encoding schemes protect through obscurity
- SDR allows adversary access to previously inaccessible mediums
- FPGAs challenge assumptions on widely-utilized crypto systems

ARUBA networks

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

ARUBA networks

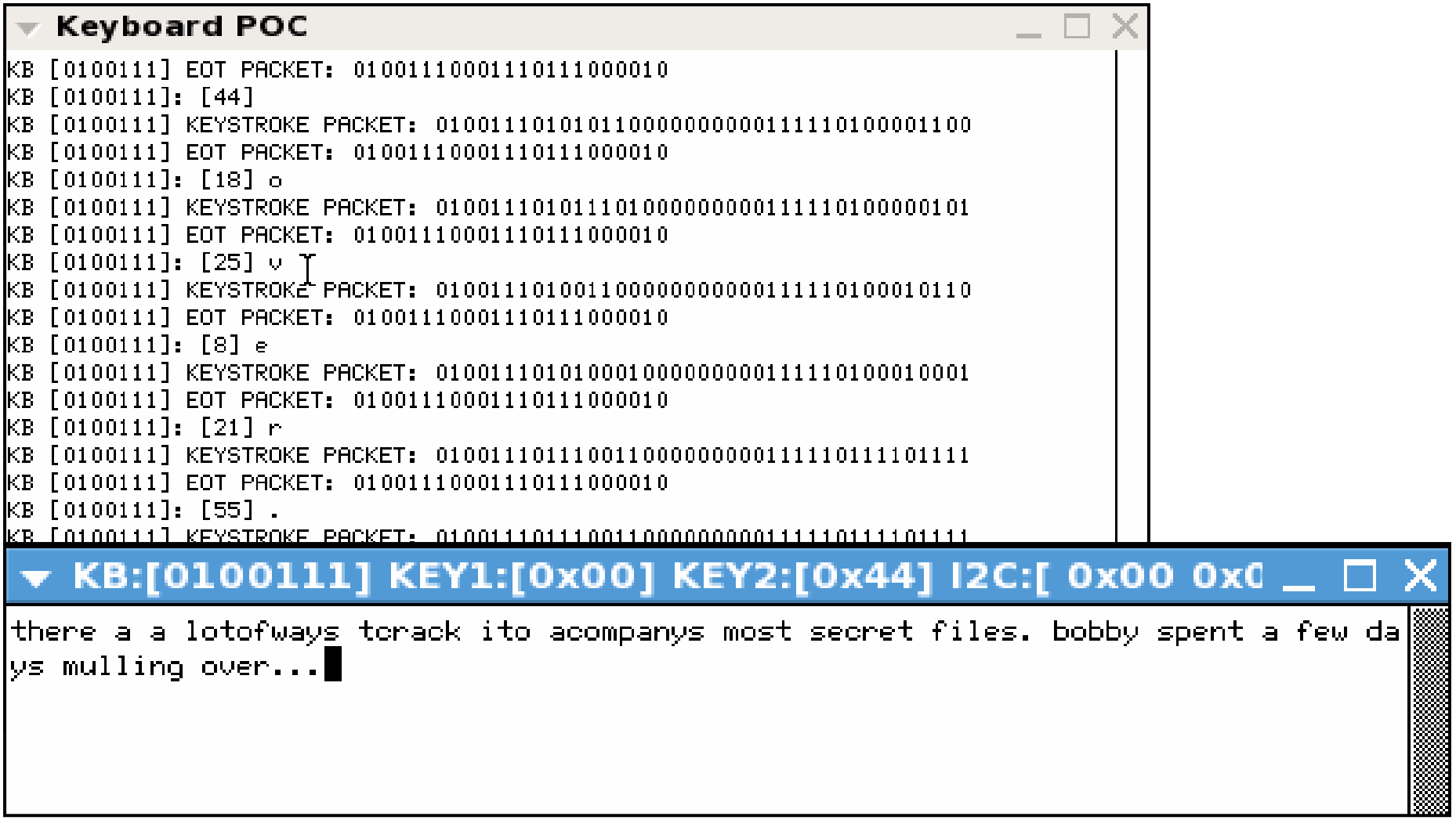
Microsoft Optical Wireless Desktop Analysis

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

Moser's Analysis Indicates ...

- Sync procedure establishes unique identifier and "key" exchange
- Keystrokes obfuscated with 8-bit XOR
- XOR key remains static until re-sync
- Common wordlist used to validate brute-force analysis of keystrokes
  - 20-50 keys reliably returns correct XOR key
- Traffic capture possible from ~10 meters using USRP/GNURadio

27 MHz Keystroke Sniffing



ARUBA networks

Keyboard Sniffing Exposure: "SO WHAT?"

- Short-range exploit, but significant confidentiality impact
  - Effectively a wireless keystroke logger
- Completely passive, little opportunity for post-compromise forensics
- Significant privacy exposure over obscure wireless mechanism

SDR makes this medium easily accessible

ARUBA networks

Group Spatial Mobile (GSM) Interception

- Digital mobile communication protocol
  - 2G technology
  - Over 2 billion users worldwide
- Utilized by AT&T, T-Mobile in US
- Popular throughout the world
- Supports SMS message transport
- THC/Steve, David Hulton

ARUBA networks

Demodulating GSM

- USRP receiver boards available for 800 MHz to 2.4 GHz
- Support in GNURadio for GMSK demod
- Enables adversary to capture and decode GSM traffic
  - Voice calls are encrypted …
  - SMS messages are encrypted …

USRP GSM Traffic Capture Example

```
0: 01 --------1 Extended Address: 1 octet long
0: 01 -------0- C/R: Response
0: 01 ---000-- SAPI: RR, MM and CC
0: 01 -00----- Link Protocol Disciminator: GSM (not C
1: 01 -------01 Supvervisory Frame
1: 01 ----00-- RR Frame (Receive ready)
1: 01 ---0---- Poll/Final bit (P/F)
1: 01 000----- N(R), Retransmission counter: 0
2: 2c --------0 EL, Extended Length: n
2: 2c -------0- M, segmentation: N
2: 2c 001011-- Length: 11
3: 05 0------- Direction: From originating site
3: 05 -000---- 0 TransactionID
3: 05 ----0101 Mobile Management Message (non GPRS)
4: 59 01------ SendSequenceNumber: 1
4: 59 --011001 MMidentityResponse
6: 29 -----001 Type of identity: IMSI
7: 43 -------- ID(7/odd): 234159046549939
```


ARUBA networks

A5/1 Weaknesses

- SMS and voice messages leverage A5/1 cipher
  - Stream cipher, call-setup has 4 frames of known plaintext
- Potential to reverse key by mapping 64-bits of known keystream state
- Multiple datapoints limits attack to 1/64th of keyspace
  - 288,230,376,151,711,744 values

ARUBA networks

Precomputed Attack

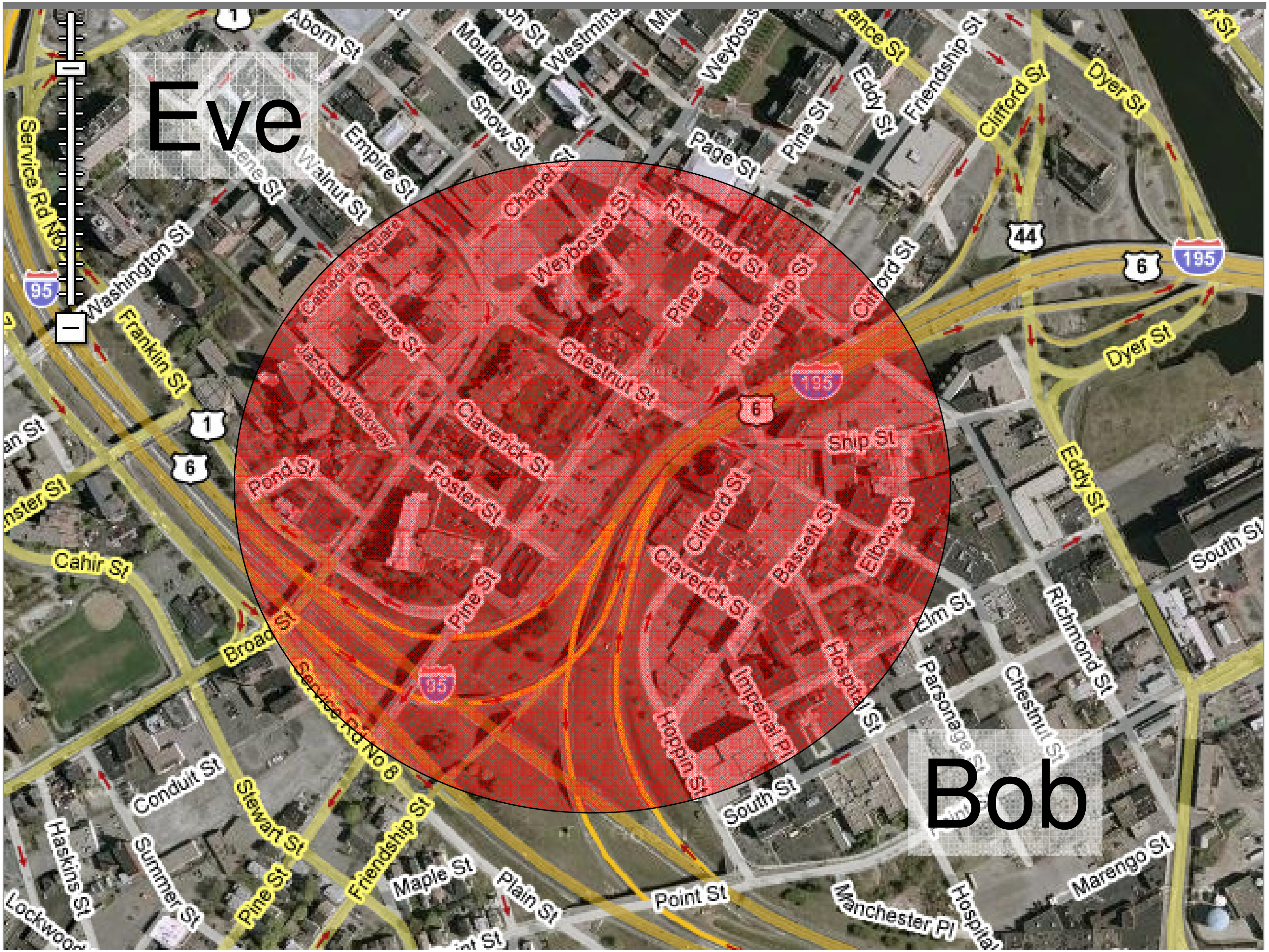
- Possible to precompute all 288 quadrillion keystream states
- 1 PC: 550,000 A5/1's per second
  - 33,235 years
- Using 68 Pico Computing E-16 FPGAs: 72,533,333,333 A5/1's per second
  - 3 months
- Requires 2 TB of storage

This needs to be done only once

ARUBA networks

GSM Sniffing Exposure: "SO WHAT"

- Anonymity threatened through IMSI disclosure in plaintext
  - Location analysis to ¼ mile
- Privacy threatened by weak crypto
  - Captured GSM conversations
  - Captured SMS messages
- Potential for infrastructure attacks against GSM with USRP TX functions

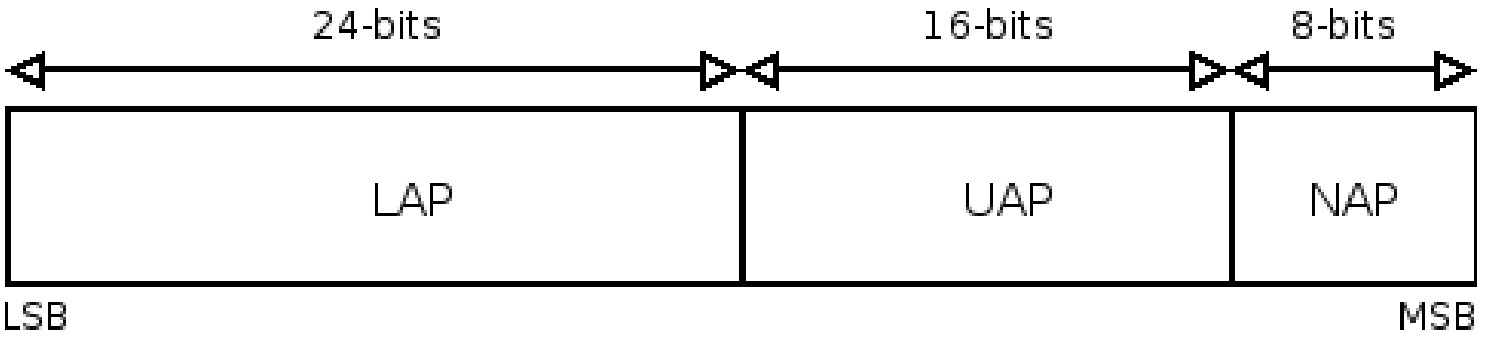

Eve
Bob
Washington St
Franklin St
Cahir St
Broad St
Conduit St
Stewart St
Haskins St
Summer St
Pine St
Friendship St
Maple St
Plain St
Point St
Manchester Pl
Marengo St
South St
Eddy St
Richmond St
Chestnut St
Parsonage St
Elm St
Dyer St
Clifford St
Chapel St
Weybosset St
Richmond St
Pine St
Friendship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

Bluetooth Specification

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

Bluetooth Addressing

- BD_ADDR, 802-compliant 48-bit address for each device
  - Bluetooth Device Address
- Used as a "secret" in Bluetooth
- Three bytes OUI, three bytes from the vendor



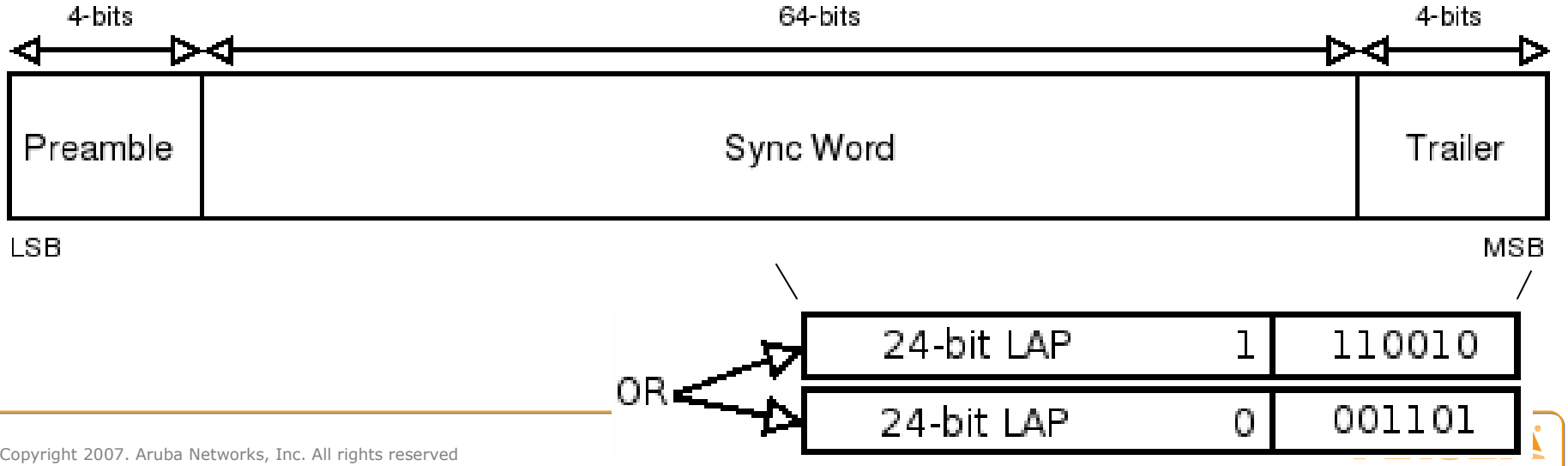
ARUBA networks


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

ARUBA networks

Discovering the Undiscoverable

- Access code data precedes baseband header
  - Includes predictable preamble and trailer data for Barker Sequence
- Sync Word used to uniquely differentiate piconets

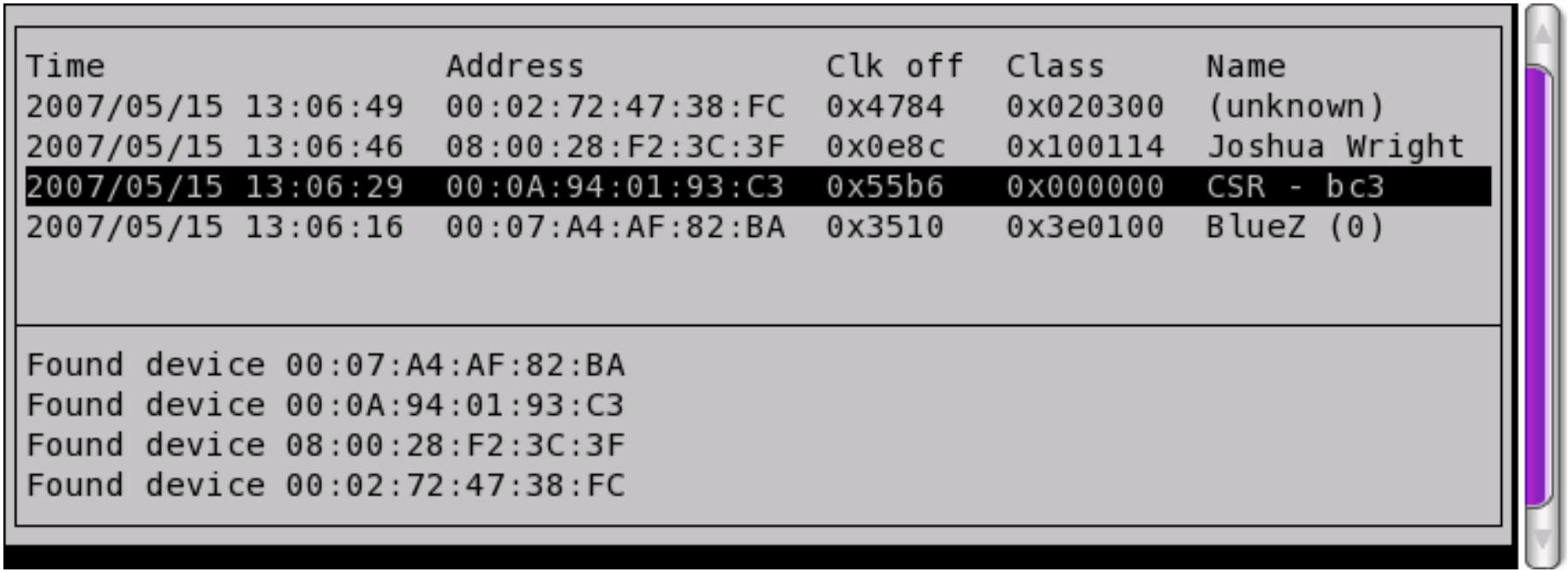


Retrieving the Sync Word

- USRP SDR listens on a single FHSS channel
- As hoppers transmit on channel, adversary captures Sync Word content
- Half of BD_ADDR (LAP) is retrieved
- Remaining NAP and UAP unknown
  - NAP + UAP = OUI (first 3 bytes of MAC)
- Possible to brute-force OUI (16-bits, assuming leading 0x00 in OUI)

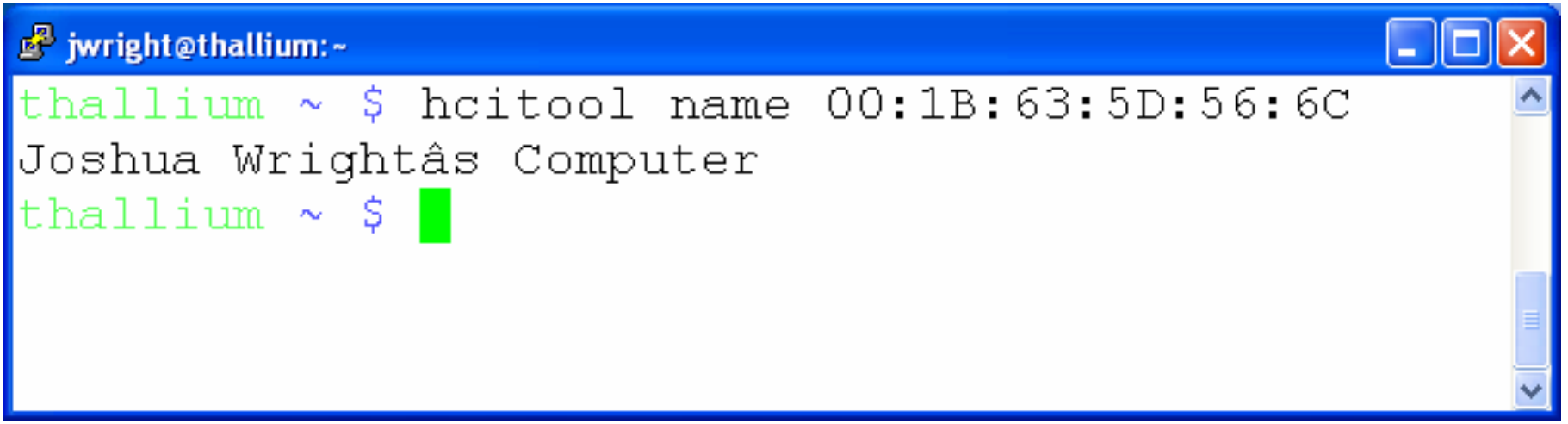
BTScanner - Bluetooth Discovery

- Modified to use BNAP, BNAP database and determined LAP
  - Attempts to connect to each combination



Associating Identity

- Once BD_ADDR is known, HCI name request returns device name
- OSX/iPhone: Automatic user naming
- Eavesdropping on conversations can also reveal this information



ARUBA networks

Headset as a Listening Bug

- Limitation: When link key is not known, unable to decrypt active voice call traffic
  - Instead, target headset when not in a call
- Can leverage the audio mic to record audio
  - Can also inject audio into the headphone
- Headset PIN is (almost) always "0000"
  - Only practical security is non-discoverable mode

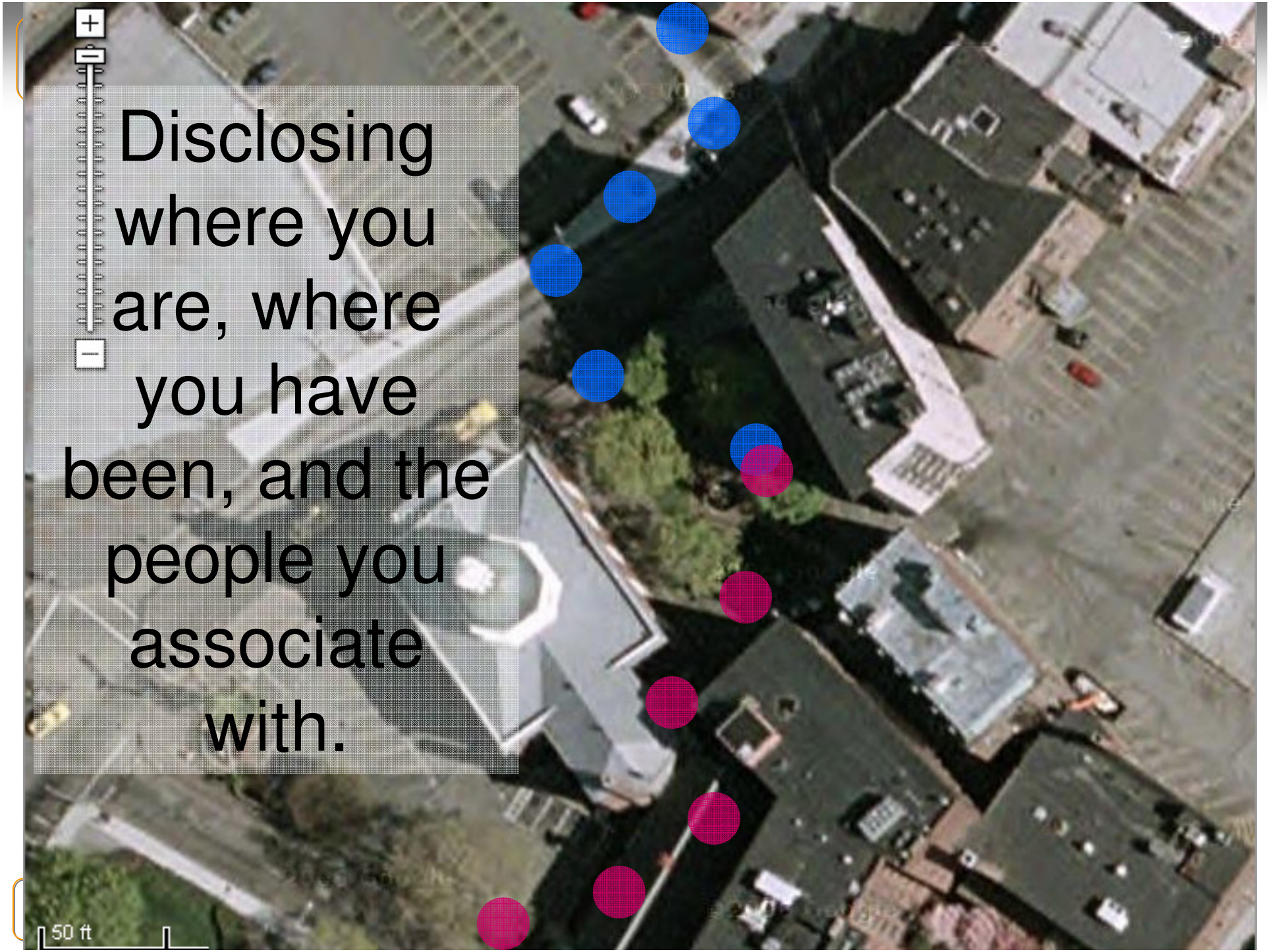
Not an attack against active Bluetooth conversations. Connecting to a device when not in a call to record/inject audio.

ARUBA networks

BT Anonymity Attacks: "SO WHAT"

- 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?

ARUBA networks


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

Future Threats to Mobility

- Licensed spectrum no longer an implicit security mechanism
- Obscure wireless protocols accessible
- SDR and FPGAs challenge existing system deployments
- User location, associations, tracking information accessible
- Technology-specific privacy threats

On Privacy and Anonymity

"… most users will accept the ability to monitor their location [when] the information itself is made available only to responsible parties."

William Webb, Wireless Communications: The Future, pg 56.

- Identity theft has increased consumer desire for privacy
- High-profile privacy and anonymity attacks threaten technology adoption

ARUBA networks

Future Outlook

- GSM eavesdropping becomes trivial
  - Who needs a subpoena?
- Businesses take advantage of location identification for traffic planning
  - Malls, Disney World, Target
- Information collected under the sentiment of anti-terrorism acts
  - Stored for persistence and analysis

Do users value privacy enough to turn down the freedom of mobility? Do you?

ARUBA networks

Conclusion

- SDR and FPGA technology open up new innovation, applications
- Leveraged by attackers to exploit previously inaccessible protocols
  - 27 MHz wireless keyboards
  - GSM networks
  - Bluetooth communication
- Consumer privacy and anonymity threatened by well-established protocols

Questions? Thank you!

- Your Speaker:

Joshua Wright
Senior Security Researcher
Aruba Networks
jwright@arubanetworks.com
Office/Mobile: 401-524-2911
^^^ CDMA Phone

Quis custodiet custodes ipsos?

ARUBA networks

ARUBA networks

USRP SDR and FPGA's

- USRP: www.ettus.com
- GNURadio: gnuradio.org/trac
- Pico Computing FPGAs: www.picocomputing.com

ARUBA networks

27 MHz Keyboard Sniffing

- www.dreamlab.net/download/articles/27_Mhz_keyboard_insecurities.pdf

GSM Attacks

- "Intercepting GSM Traffic", Blackhat Federal 2008 Presentation
- https://www.blackhat.com/presentations/bh-dc-08/Steve-DHulton/Presentation/bh-dc-08-steve-dhulton.pdf
- THC GSM project: http://wiki.thc.org/gsm
- Cracking A5: http://wiki.thc.org/cracking_a5