

State of Wireless Security

Chris Cox
Anthony Bolan

NEbraskaCERT CSF, June 2015
University of Nebraska at Omaha

Broad Topic

Concentrating on what we find interesting:

- WiFi Security
 - LootBooty, MANA Toolkit
- Identity Snooping w/ Distributed Frameworks
 - Snoopy Framework, CreepyDOL
- Software-Defined Radios (SDR)
 - Commercial Radio Systems, GSM

DISCLAIMER

These views are our own, and not necessarily each others'. They are definitely not our employer's, and probably not any of our instructors', but we'll let them speak for themselves on that.

Without the proper legal agreements in place (written permission, etc.) use of some of these tools may be illegal. We aren't lawyers. Please consult one if you have questions.

WiFi Security

Recent WiFi Security Talks:

- [BYO-Disaster by PuNk1nPo0p, DEFCON 21, 2013](#)
 - Released [LootBooty](#) - allows EAP-GTC downgrade.
 - Obtain 802.1X credentials in cleartext from many mobile phones.
- [Manna from Heaven by SensePost, DEFCON 22, 2014](#)
 - Released the [MANA Toolkit](#) - extensions to Karma, SSLstrip, more.
 - Can allow capture of cookies and login information in some cases.

LootBooty and KarmaBooty

- **EAP-GTC**: Cisco protocol designed for TOTP. Token is transmitted in the clear.
- **Karma**: Rogue AP responds to all probe requests.
- **LootBooty**: A patch to FreeRADIUS, forcing a downgrade to EAP-GTC on vulnerable devices (mostly mobile phones.) 802.1X WiFi passwords then sent in cleartext.
- **KarmaBooty**: An extension to LootBooty by yours truly, adds Karma to LootBooty.

MANA Toolkit

- Developed by [SensePost](#) to update/extend Karma and circumvent newer protections like [certificate pinning](#) and [HSTS](#).
- Mostly modifies Karma and SSLstrip.
- For Karma, MANA does the following:
 - Stores Preferred Network Lists (PNLs) for each device.
 - Creates a hidden access point to circumvent Apple PNL controls.
 - Automatically captures EAP hashes (but doesn't include LootBooty-like downgrade attacks).
 - Can create active APs for each SSID probed for by a device.

WiFi Pineapple

- Mark V - \$99 from [Hak5](#).
 - Wireless AP with custom, enhanceable firmware.
 - Support for USB broadband modems.
 - Many user-written “infusions” allow new capabilities.
 - Pineapple Plug - \$20, connect two Pineapples for more capability/awesomeness.
-
- Compact and useful tool, lots of power in a little package.

Wireless Attacks: How to Stay Secure

- Enable wireless functions only when you need them (WiFi, Bluetooth, NFC).
- Read the messages/warnings your device gives you when you connect to a wireless network!
- Use a non-Android phone. Apple and Windows phones are (better) protected from these attacks.
- Organizations: use a unique credential for PEAP/MSCHAPv2 authorization. Even better: use EAP-TLS! Certificates for everyone!

DEMO DISCLAIMER

In the demos presented in the rest of this talk, tools and technologies will be used which can intercept the WiFi broadcast transmissions of computers, mobile phones and other devices.

If you do not wish to participate in these demos, please turn off the WiFi on your devices now.

Demos: Part I

- MANABooty
- WiFi Pineapple

Snoopy Framework

- [Snoopy Framework](#) from [SensePost](#).
- Created primarily by [Glenn Wilkinson](#).
- Distributed wireless device tracking framework.
- Numerous sensors report back to a central server.
- Main idea: try to identify people and their behaviors by seeing what their mobile devices do.
- Free and open-source! Commercial version in [beta](#).
- SensePost's talks on Snoopy:
 - [Terrorism, Tracking, Privacy and Human Interactions, 44CON, 2012](#)
 - [Practical Aerial Hacking and Surveillance, DEFCON 22, 2014](#)

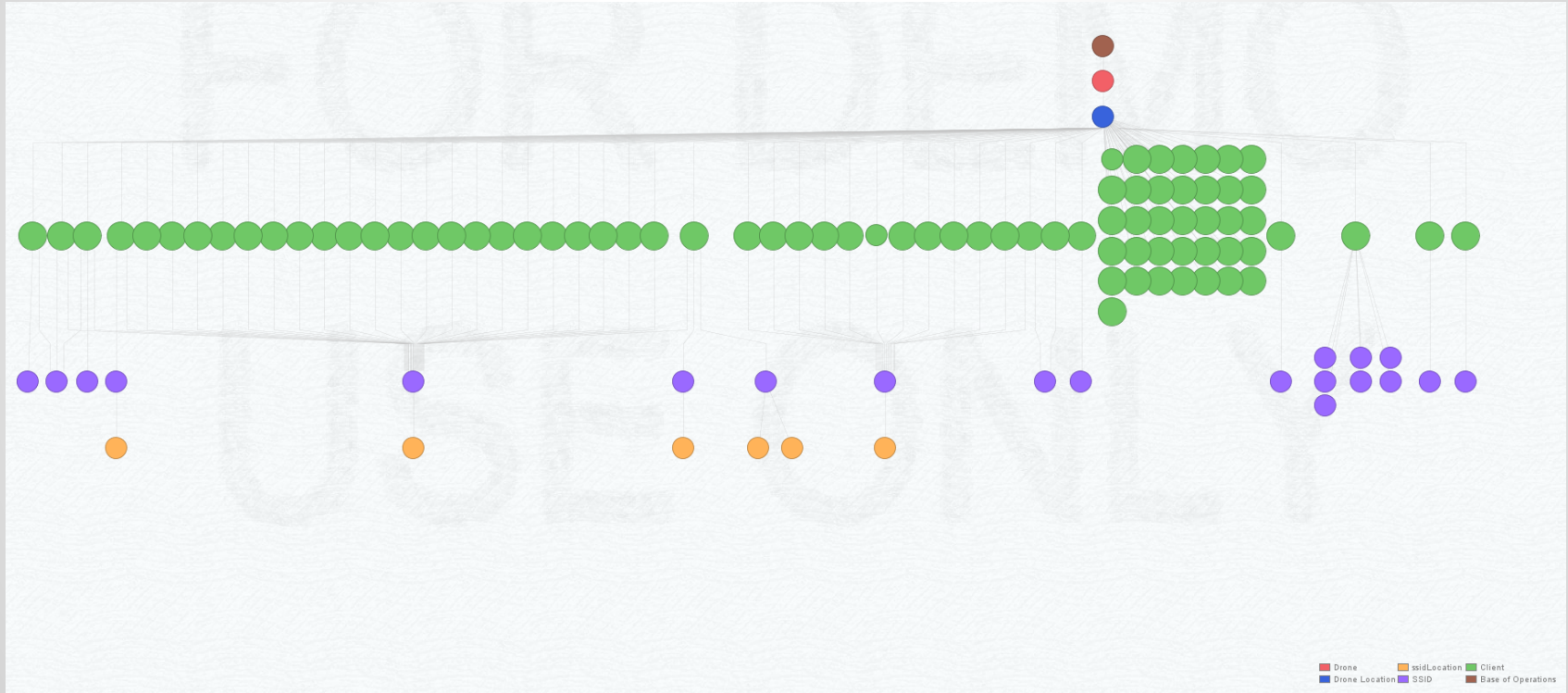
Snoopy Framework II

- Install on Kali Linux with *git clone*, run *./install.sh*.
- Ties into [Wigle](#) for WiFi access point locations.
- Modules for rogue APs, Bluetooth sniffing, WiFi sniffing, GPS location of mobile sensors, etc.
- Extensible! New plugins can be written in Python.
- Can be installed on small, cheap devices.
 - Raspberry Pi - ~~\$35~~ \$25!
 - Beaglebone Black - \$55
 - Chip - \$9 (pre-order)
 - Pretty much any Linux device with a good WiFi chip.

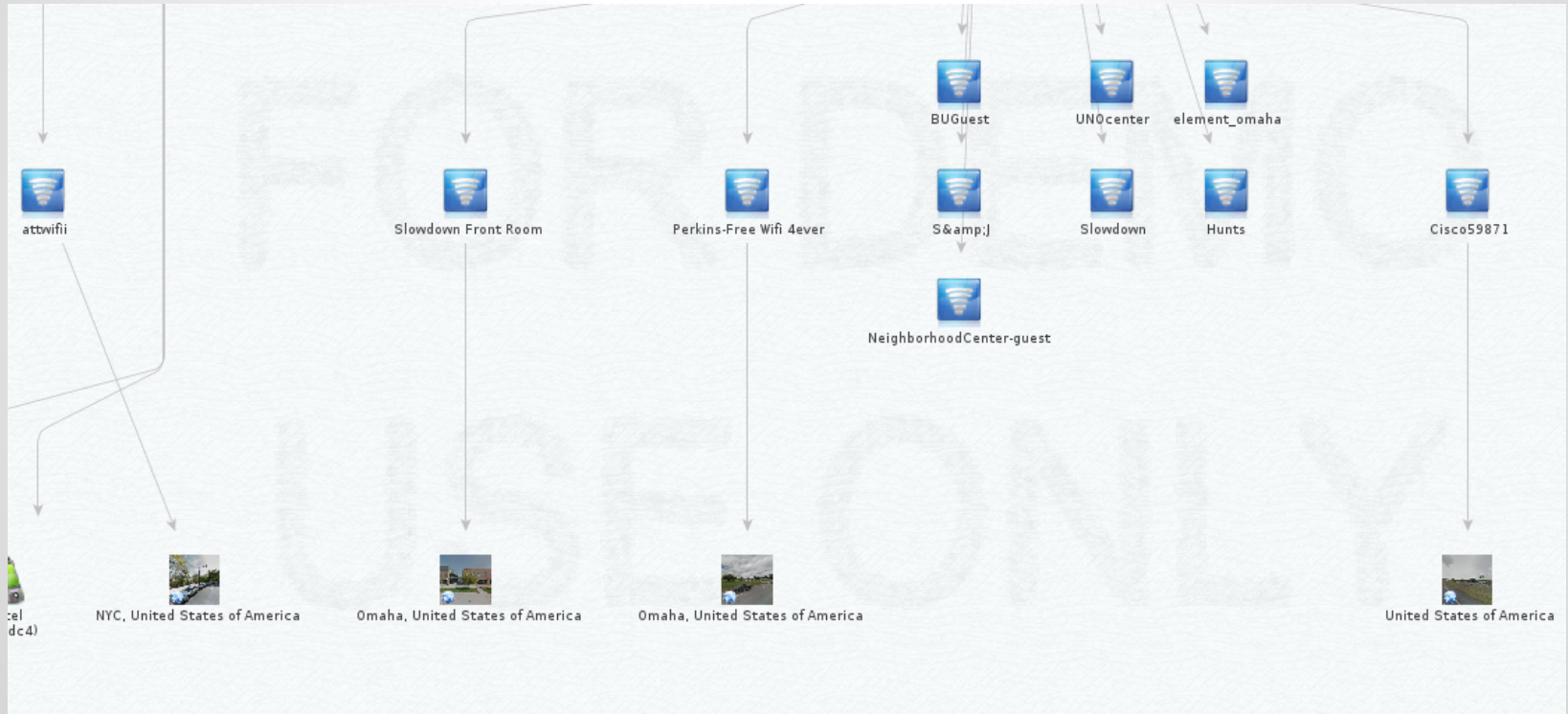
Snoopy Visualization

- Snoopy uses [Maltego](#) (free Community Edition!)
- **Maltego**: OSINT visualization tool by Paterva, can be enhanced with Python-based transform files.
- The *snoopy-ng* package includes transforms for Snoopy.
- Importing these transforms allows visualization of data, including devices, SSIDs, device locations, and data/credentials captured.

Snoopy Visualization II




Snoopy Visualization III




Snoopy Visualization IV

Details

Summary Attachments (0) Notes Properties (16)

 San Diego, United States of America
ssidLocation
[snoopy ssid_location]

Google Me!
Open all URLs
Wikipedia Me!



Notes

Name San Diego, United States of America
City San Diego
Country United States of America
More...

Use the + button to add images

Details

Summary Attachments (0) Notes Properties (16)

Name San Diego, United States of America

City San Diego

Country United States of America

Street Address Pacific Beach Drive, San Diego

Area Pacific Beach

Area Code 92109

Country Code us

Longitude -117.254

Latitude 32.791

Image <http://maps.googleapis.com/maps/api/streetview?size=800x800&sensor=false&location=32.79105377,-117.25390625>

longaddress Church, Pacific Beach Drive, Pacific Beach, San Diego, San Diego County, California, 92109, United States of America

Road Pacific Beach Drive

SSID BlueSeaBeachHotel

State California

Google map <http://maps.google.com/maps?t=h&q=32.79105377,-117.25390625>

Street View <https://maps.google.com/maps?q=&layer=c&cbp=11,0,0,0,0&cbll=32.79105377,-117.25390625>

CreepyDOL

- Creepy Distributed Object Locator
- Created by Brendan O'Connor at [Malice Afterthought](#).
- Talks given at [BlackHat 2013](#) and [DEFCON 21](#).

- Similar to Snoopy, uses a distributed sensor network to locate wireless devices.
- Current project status is unknown. Released code is limited. Custom hardware, called F-BOMBs, is available for sale.

Identity Snooping: Legal Issues?

- IANAL - However, this is 802.11 and we're listening to broadcast traffic. (See: FCC - [Interception and Divulgence of Radio Communications](#)).
- [It's been done for years by retailers](#). Privacy issue? Yes. Legal issue? [Apparently not](#). (But you can opt out now!)
- Stripping SSL or harvesting credentials from unsuspecting victims? [Definitely not legal](#).
- Also: consider [Bluetooth stuff!](#) Many things (cars, IoT devices, etc.) broadcast over Bluetooth.

Commercial Snooping Products

- [Palantir USA](#)
 - Provide identity tracking services to local/state/national government, police forces.
- Many others for commercial retailers. These vendors follow the [Mobile Location Analytics Code of Conduct](#):
 - [Aislelabs](#), [Euclid](#), [EyeQ Insights](#), [Measurence](#), [Mexia Interactive](#), [Path Intelligence](#), [Presence Orb](#), [Purple WiFi](#), [Radius Networks](#), [SOLOMO Technology](#), [Turnstyle Solutions](#)

Positive/Beneficial Snooping?

- Emergency response and rescue.
 - Put environmentally-protected sensors in buildings.
 - Sensors relay number of devices in building, location info.
 - Profit (save lives)!
- Locating potential witnesses.
 - Sensors on traffic lights could indicate witnesses to crimes.
- Graffiti abatement.
- General crime detection/deterrence.
 - Have Snoopy take pictures when devices are found in an area.

Identity Snooping: How to Stay Secure

- Enable wireless functions only when you need them (WiFi, Bluetooth, NFC).
- Use the latest OS version available for your mobile device. (Better probe request functionality, security enhancements).
- Disabling SSID broadcasting of your home network's SSID *might* help, as Wigle won't record hidden networks.
- At retailers, where possible: opt out!

Demos: Part II

- Snoopy Framework

Software-Defined Radio

- Multiple radio receivers/transmitters for purchase.
 - [RTL-SDR](#), [HackRF](#), etc.
- RTL-SDR is very cheap: \$5 - \$15. HackRF is \$328.
- RTL-SDR is a receiver only, 52 - 2200 MHz range.
- Can listen to AM/FM/TV channels, many security radios, public transport, airplane info and more.
- Some radio data is encrypted, but circumvention is possible, though likely illegal.
- Also able to intercept some cell phone ranges. (Also illegal).

SDR: Legal Issues

- Interception of certain types of radio transmissions is illegal, per the Telecommunications Act of 1996.
 - Interception of domestic cellular communications.
 - Interception of a competitor's signals to gain a business advantage.
 - Interception of paid signals, such as cable TV.
 - Selling/publishing telephone recordings.
- Illegal to make/sell scanners with ability to intercept cell phone signals or which provide digital audio decoding.
- Penalties include fines up to \$10,000 and a year in jail, for the first offense.

SDR: How to Stay Secure

- For private security/police radios: use strong encryption where possible. 40-bit DES (I'm looking at you, MotoTRBO) just isn't good enough anymore.
- Spread-spectrum and frequency-hopping technologies makes a hacker's job harder.
- Using a cellular carrier that doesn't use GSM *might* help.
 - Tools to break GSM are readily available online, CDMA and others aren't as common.

Demos: Part III

- Software Defined Radio
 - UNO campus bus system.
 - Airplane tracking.

Final Thoughts

- Turn off your WiFi. You probably don't need it, anyway.
- Be conscious of your devices. Know how and to whom they communicate. This goes for IoT stuff, too!

Thanks

- [SensePost](#)
- [Hak5](#)
- [PuNk1nPo0p](#)
- [Malice Afterthought](#)
- [Paterva/Maltego](#)
- [Great Scott Gadgets](#) (HackRF)

- [NEbraskaCERT](#)
- You!

Questions?

Once again, no WiFis (or cells) were harmed in the making of this presentation.

Questions later?

abolan at unomaha dot edu

ccox at unomaha dot edu