Black Hat Europe - 2013
Meshing Stuff Up:
Ad Hoc Mesh Networks with Android
~ software engineer for the last 12 years

I like to:

- break / embed / repurpose things
- solder things into other things
- stare at asm

Find Me:

- jthomas@accuvant.com
- m0nk.omg.pwnies@gmail.com
- @m0nk_dot
/whoami (stoker)

- <insert infoz here>
- I like to:
  - thing 1
  - thing 2
- Find Me:
  - jrobble@mitre.org
  - mistr.stoker@gmail.com
SPAN is an Open Source research project initially funded by the MITRE Corporation for use in Emergency Preparedness and Response situations

Team:

- Josh Thomas (Accuvant LABS) - Geek with an idea that used to get paid to lead the effort
- Jeff Robble (MITRE) - Lead Developer and currently running the MITRE effort
- Oliver Chong (MITRE) - iOS and Security
- Sheldon Durrent (MITRE) - Security
SPAN is open source and released under the GPLv3

SPAN is a collaborative effort of private, public and independent contributors worldwide.

Associated and leveraged projects

- Serval: http://www.servalproject.org/
- Freifunk: http://start.freifunk.net/
- OpenWRT: https://openwrt.org/
- Commotion: https://code.commotionwireless.net/projects/commotion
- tinc: http://www.tinc-vpn.org/
- pttdroid: http://code.google.com/p/pttdroid/
Will he start already?

- Mesh? / Why do I care about mesh networks?
- What are they and how do they work?
  - Rooting and Routing
- Notes on Android Development at the Hardware level
- Chat, SMS & VoIP
- Securing the Mesh
- Lessons learned and moving forward!
- </end_session>

- TL;DR:
  - www.omg-pwnies.com
  - https://github.com/monk-dot
  - https://github.com/ProjectSPAN
What’s a Mesh Network?

- It’s exactly like graph theory except:
  - Nodes are shiny electronic gadgets that run out of battery and move around a bunch
  - Vertices are unstable and based on arbitrary signal strength
  - The pics are uglier
Ok, but why?
Hurricane Katrina

August 2005

- Over 3,000,000 phone lines went down
- 2000 cell towers knocked out
- Land Mobile Radio (LMR) communications highly degraded
- HAM Radio Operators assisted standard 911 dispatchers
- On scene field reporters exchanged information between victims and authorities
Haiti Earthquake

January 2010

- The 2 main public telephone service providers (Digicel and Comcel) networks went completely down
- Haitian cellular service networks quickly failed with the influx of Red Cross volunteers
- Fiber-Optic and other networks highly degraded
Tohoku Earthquake

March 2011

- Earthquake and the following Tsunami lead to the Fukushima Daiichi Nuclear Power Plant meltdowns
- Degraded and disabled infrastructure across the island
- Forced service providers to limit mobile phone traffic by 90-95%
Recent Worldwide Events

2011 - 2012

- Egyptian Arab Spring Protests
  - President Mubarak cuts off cellular communications during protest
- Hurricane Sandy
  - Twitter proved itself as a viable news and communication outlet when other technologies failed
  - Phones have power when TVs don’t
- Middle East / Israel and Anonymous
  - VoIP & Twitter monitored and manipulated
Solution?
The SPAN Project

- There are too many headaches involved in starting MANET research before you actually get to the hard problems
- Simple framework implementation for MANET - Smart Phone AdHoc Networking
- A transparent proxy so normal applications just work
The Stack

- Blinkie on a Map
- P2P Chat App.
- Other App.

Java Networking Interface
- TCP Socket
- UDP Socket

Reliable Transmission Layer
- Security Manager
- Session Manager

MANET Service
- Network Configuration
- Manual Routing Protocol Selection
- Automated Routing Protocol Selection

Modular MANET Routing Protocol Framework
- Proactive Routing Protocol Manager
  - OLSR
  - BATMAN
  - Protocol 3
- Reactive Routing Protocol Manager
  - DSR
  - Protocol 2
  - Protocol 3

Transparent Proxy
- iptables / netfilter
- Linux Kernel Routing
Easy Problems that are in fact hard

- Getting it running overall
- Per device specialization
  - Hardware diffs
  - AOSP / Kernel customizations
- Network configuration / Ad Hoc joins
Hard Problems that are in fact hard

- Routing
  - Proactive vs. Reactive
  - Sensor based routing
  - Other mesh & routing projects
    - OLSRd
    - SERVAL / BATMAN
    - Byzantium Mesh
    - FreiFunk
- Network Scale / Speed and Power consumption
- Security
Mesh Routing 101 - Proactive vs Reactive
Lesson 1: Proactive Routing
Lesson 2: Reactive Routing
What can we actually do with the Mesh?
Security - It’s never too early / it’s always too late
Lessons Learned and Stories told
Questions? Comments?

Slides and Papers:
https://github.com/monk-dot

Actual Code:
https://github.com/ProjectSPAN

Easy link:
http://www.omg-pwnies.com

• </talk>
The Links

- [http://www.olsrd.org](http://www.olsrd.org)
- [http://www.servalproject.org](http://www.servalproject.org)
- [http://berlin.freifunk.net](http://berlin.freifunk.net)
- [http://project-byzantium.org](http://project-byzantium.org)
Backup Slides
Routing Protocols (Pics or it didn’t happen)

Topology

Definitions

Route to 1-hop neighbor

Route to 2-hop neighbor
Find 1-hop neighbors

Asymmetric Link

Symmetric Link
Multi-Point Relay
What about iOS?
Getting to know your friendly chip vendors!

- Broadcom 4329 - Samsung Galaxy Nexus, Samsung Nexus S 4G, Nokia Lumia 900, older iPhones, Asus Transformer Prime, many more
- Broadcom 4330 - Samsung Galaxy TAB 10.1, Samsung Galaxy S II / Epic Touch 4G, iPhone 4S, many many more
- Broadcom 4334 - iPhone 5, Samsung Galaxy S III
- TI WL1285C - Motorola Razr / MAXX
- Qualcomm - A ton of Android Phones

All behave differently, all are quirky
A Short story in 7 Pictures & 9 Words
Terrorists love Baseball
Hotels hate me
Snipers hate Engineers