CYBER SCIENCES CORPORATION

Security Vulnerabilities for P25 Public Safety Radio Systems

State of Missouri Interoperable Communications Conference

February 10th, 2011

William J. Brunkhardt
Chief Technology Strategist
Cyber Sciences Corporation, LLC

CYBER SCIENCES CORPORATION

APCO P25 Security Vulnerabilities:

- Due to the inherent nature of RF communications & the P25 protocol, security vulnerabilities need to be considered
  - Vulnerabilities pose a serious threat to law enforcement and first responders & the citizens they protect
- Today we will briefly address these threats on a non-technical level & propose methods aimed at protecting our P25 critical infrastructure

CYBER SCIENCES CORPORATION

APCO P25 Security Vulnerabilities:

- The P25 protocol was developed on a model of "Implicit Trust"
  - Just like the Internet (TCP/IP) was developed with the same implicit trust
    - For example, in the early days of the Internet, if the University of Illinois sent data to Stanford University, Stanford University just assumed the data was indeed from University of Illinois.
  - Unfortunately, in today's environment, and due to the limitations of TCP/IP, it is very easy to "spoof" IP addresses or credentials

CYBER SCIENCES CORPORATION

APCO P25 Security Vulnerabilities:

- Starting Point:
  - A wealth of information can be found on the Internet

Jefferson City, City of

Frequency	Input	License	Type	Tone	Alpha Tag	Description	Mode	Tag
154.86000	158.92500	WPFE756	RBM	192.8 PL	JffC Police1	Police [F-1]	FM	Law Dispatch
156.21000	156.03000	KAA552	RM	192.8 PL	JffC Police3	Police: Dispatch [F-3]	FM	Law Dispatch
155.58000		KAA552	M		Cole Shrf 1	Sheriff: Dispatch	FM	Law Tac
453.27500	458.27500	KUB844	RM		JffC Parking	Parking Division	FM	Other
158.83500		KNDE685	BM		JeffCity EMA	Emergency Management	FM	Multi-Dispatch
154.40000	153.95000	KRF431	RBM	192.8 PL	JffC Fire 1	Fire [F-1]	FM	Fire Dispatch
155.83500	155.04000	WQDI470	RM		JffC FireNew	Fire: Future	FM	Fire Dispatch
153.95000		KRF431	M		JffC FD FG 1	Fire	FM	Fire-Tac
155.11500		WPQG833	M		JffC FD FG 2	Fire	FM	Fire-Tac
458.91250		WPQG833	M		JffC FD RF	Fire (Extender or Remote Link)	FM	Fire-Tac
460.51250	465.51250	KRF431	M		JffC FD RF2	Fire: Remote Links or Mobile Extender	FM	Fire-Tac
153.89000	155.40000	KXL292	RM	88.5 PL	Cole EMS	EMS: Dispatch	FM	EMS Dispatch
154.10000	158.88000	KDL859	RM	192.8 PL	JffC PubWrk1	Public Works	FM	Public Works
153.78500		WPIG986	M		JffC PubWrk2	Public Works	FM	Public Works
460.58750	465.58750	WQCU448	RMF		JffC Prk&Rec	Parks & Recreation	FM	Public Works

Passive System Exploits:

- An adversary could passively “sniff” the over the air network with “common off the shelf” (COTS) components & software

- This data stream could be converted to eavesdrop on the voice traffic & look at the granular “metadata” being passed

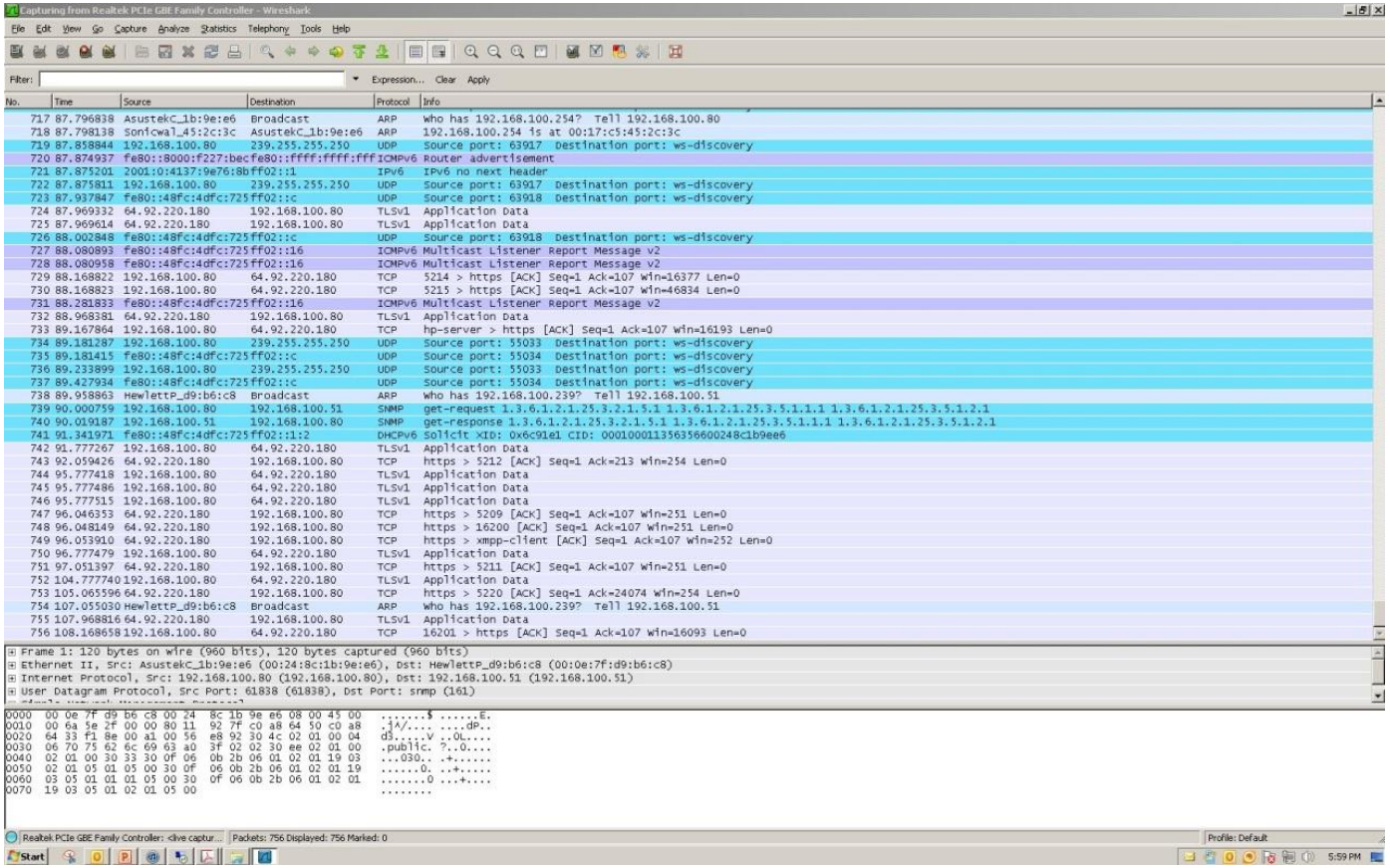
Passive System Exploits:

- Metadata contains intimate details of user IDs, user locations, NAC codes, etc. (Even with system encryption enabled, metadata is sent in the clear)

- Passive sniffing and network surveillance provides valuable information for more sophisticated attacks

Active/Targeted Exploits cont:

CYBER SCIENCES CORPORATION



WireShark Software Application Doing Network Surveillance Over the Air P25 Traffic

Active/Targeted Exploits:

CYBER SCIENCES CORPORATION

- **Injection of false data**
  - Using already captured metadata, false data & voice traffic can be easily injected into the system – regardless of whether or not encryption is enabled
  - This data can be introduced without detection as the system thinks it is an authorized user
    - P25 protocol assumes “Implicit Trust”

Active/Targeted Exploits:

CYBER SCIENCES CORPORATION

This simple setup has the capability to bring a trunked P25 radio system to its knees….

CYBER SCIENCES CORPORATION

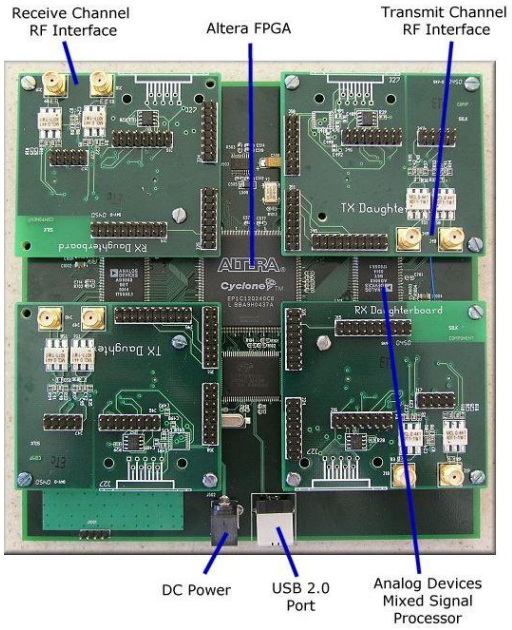
Active/Targeted Exploits cont:

- **Wireless Distributed Denial of Service Attack (WDDoS)**
  - Using inexpensive software-defined radios (SDRs) and/or commercial radios, an adversary can geographically position jamming devices that interfere with the P25 system
  - The adversary does not have to "drown out" the base station signal…only partial data frames have to be corrupted to cause havoc

Active/Targeted Exploits cont:

- **Wireless Distributed Denial of Service Attack (WDDoS)**
  - Using software defined radios connected to a small PC or microcontroller, we can do the following:
    - Send traffic to mobiles or portables that appear to come from dispatch
    - Send traffic to dispatch that appears to be coming from an authenticated mobile/portable
    - Key up mobile/portable requests so quickly, in random order, that it overloads the base station/control channels

Active/Targeted Exploits cont:



Software Defined Radios (SDRs) that can be connected to a simple PC

Active/Targeted Exploits cont:

CYBER SCIENCES CORPORATION

Question:

CYBER SCIENCES CORPORATION

- **Who has been aware of these types of vulnerabilities?**
- **Has anyone had discussions with end users about the threat of jamming?**
  - **Analog/Digital**

Active/Targeted Exploits cont:

CYBER SCIENCES CORPORATION

- **GPS Receiver Vulnerabilities**
  - Most base stations contain a Rubidium Oscillator time reference clock for time synchronization
  - Disrupted GPS signals (even within a few short hours) = reference clock drifts that it could be problematic for the radio network

Active/Targeted Exploits cont:

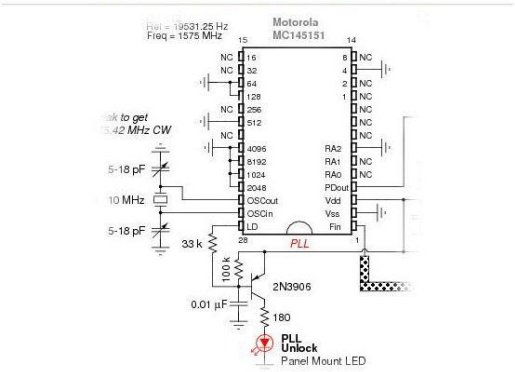
CYBER SCIENCES CORPORATION

- **GPS Receiver Vulnerabilities**
  - Small, inexpensive GPS jammers placed close to the site can be very effective
  - High-power GPS jammers can have much greater coverage (these are can be located by direction-finding equipment much more easily)

Active/Targeted Exploits cont:

CYBER SCIENCES CORPORATION

GPS Receiver Antenna @ A Base Station



Homemade GPS Jammer Schematic Found on Internet

You can buy GPS jammers off the Internet from China for less than $100

GP4000 Portable Mini GPS Jammer, GPS Blocker

Portable mini GPS jammer will block all GPS trackers in radius of 5 meters. Has very compact design and can be hide in pocket.

$ 99.00

MORE INFO

ADD TO CART

GP5000 Car Use GPS Jammer, GPS Blocker, Tracking Jammer

GPS jammer,blocks GPS tracking. GP5000 will disable the GPS link and render the spy device useless

$ 129.00

MORE INFO

ADD TO CART

GPS Jammers For Sale On Internet

Esoteric/Future Possible Threats:

CYBER SCIENCES CORPORATION

- **EMP Burst (Electromagnetic Pulse)**
  - Literally all modern electronic devices rely on sensitive components vulnerable to EMP
  - Although the threat is low, experts agree a small yield nuclear weapon could be used in a terrorist attack for the prime purpose of generating EMP to cripple critical infrastructure
    - Power generation
    - Data centers
    - Telecom facilities

Esoteric/Future Possible Threats:

CYBER SCIENCES CORPORATION

- **EMP Burst (Electromagnetic Pulse)**
  - A very small EMP could render the base station/system controller useless
  - Newer, more esoteric technologies are being considered that could replicate a small nuclear EMP

The Bottom Line: What Can We Do?

CYBER SCIENCES CORPORATION

- **Proposed Solutions**
  - Clearly understand the vulnerabilities of P25 and other radio communications systems
    - RF vulnerabilities
    - Backhaul vulnerabilities
    - Physical vulnerabilities
  - Educate law enforcement & first responders that this threat is REAL – There may be a time they can't rely on their primary communications systems

The Bottom Line: What Can We Do?

CYBER SCIENCES CORPORATION

- **Proposed Solutions**
  - Monitor suspicious activity around base stations & repeater sites
    - Suspicious persons
    - Suspicious electronics, vehicles, antennas

Highly-Directional Yagi Antenna

The Bottom Line: What Can We Do?

CYBER SCIENCES CORPORATION

The Bottom Line: What Can We Do?

CYBER SCIENCES CORPORATION

- **Proposed Solutions**
  - Have LEOs pay attention to equipment in vehicles during traffic stops
    - Look for non-commercially produced electronics (don't falsely accuse the amateur radio operators! ☺)
  - Prepare alternate plans of communications in case the primary P25 system is rendered inoperable
    - Conventional/Analog frequencies
      - MTAC
      - VTAC
      - VLAW

The Bottom Line: What Can We Do?

CYBER SCIENCES CORPORATION

- **Proposed Solutions cont:**
  - Consider Radio Direction Finding (RDF) Equipment & network surveillance equipment to quickly identify location of jammer
  - Monitor P25 system logs and watch for abnormalities
  - Remember, others could be listening

The Bottom Line: What Can We Do?

CYBER SCIENCES CORPORATION

- **Proposed Solutions cont:**
  - Consider “Red-Team” exercises to probe for vulnerabilities
  - Prepare a written “plan of action” to be used in the event of a suspected system attack
  - Educate users of P25 system how to use simplex/talkaround capabilities of the radio should the base station become inoperable

The Bottom Line: What Can We Do?

CYBER SCIENCES CORPORATION

- **Proposed Solutions cont:**
  - Don’t be afraid to reach out to experts and ask questions (vendors, consultants, engineers)

Discussion:

- **Questions/Comments?**

Please feel free to contact me:

William J. Brunkhardt
Chief Technology Strategist
Cyber Sciences Corporation, LLC
Direct: +1.913.951.3005
E-Mail: bill@cybersciencescorp.com