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
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
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.
APPENDIX II

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

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Input</th>
<th>License</th>
<th>Type</th>
<th>Tone</th>
<th>Alpha Tag</th>
<th>Description</th>
<th>Mode</th>
<th>Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>154.6000</td>
<td>158.92500</td>
<td>WPFE755</td>
<td>REM</td>
<td>192.8 PL</td>
<td>JHFC Police 1</td>
<td>Police [F-1]</td>
<td>FM</td>
<td>Law Dispatch</td>
</tr>
<tr>
<td>156.21000</td>
<td>156.03000</td>
<td>KAA552</td>
<td>RM</td>
<td>192.8 PL</td>
<td>JHFC Police 2</td>
<td>Police: Dispatch [F-3]</td>
<td>FM</td>
<td>Law Dispatch</td>
</tr>
<tr>
<td>155.68000</td>
<td></td>
<td>KAA662</td>
<td>M</td>
<td></td>
<td>Cole Sheriff 1</td>
<td>Sheriff: Dispatch</td>
<td>FM</td>
<td>Low Tac</td>
</tr>
<tr>
<td>463.27500</td>
<td>458.27500</td>
<td>KUB644</td>
<td>RM</td>
<td></td>
<td>JHFC Parking</td>
<td>Parking Division</td>
<td>FM</td>
<td>Other</td>
</tr>
<tr>
<td>158.83500</td>
<td></td>
<td>KNDE685</td>
<td>BM</td>
<td></td>
<td>JHFC EMA</td>
<td>Emergency Management</td>
<td>FM</td>
<td>Multi-Dispatch</td>
</tr>
<tr>
<td>154.40000</td>
<td>153.95000</td>
<td>KRF431</td>
<td>REM</td>
<td>192.8 PL</td>
<td>JHFC Fire 1</td>
<td>Fire [F-1]</td>
<td>FM</td>
<td>Fire Dispatch</td>
</tr>
<tr>
<td>155.83500</td>
<td>155.04000</td>
<td>WGD470</td>
<td>RM</td>
<td></td>
<td>JHFC Fire New</td>
<td>Fire: Future</td>
<td>FM</td>
<td>Fire Dispatch</td>
</tr>
<tr>
<td>153.95000</td>
<td></td>
<td>KRF431</td>
<td>M</td>
<td></td>
<td>JHFC FD FG 1</td>
<td>Fire</td>
<td>FM</td>
<td>Fire-Tac</td>
</tr>
<tr>
<td>155.11500</td>
<td></td>
<td>WPG0333</td>
<td>M</td>
<td></td>
<td>JHFC FD FG 2</td>
<td>Fire</td>
<td>FM</td>
<td>Fire-Tac</td>
</tr>
<tr>
<td>460.91250</td>
<td></td>
<td>WPG0333</td>
<td>M</td>
<td></td>
<td>JHFC FD RT</td>
<td>Fire (Extender or Remote Link)</td>
<td>FM</td>
<td>Fire-Tac</td>
</tr>
<tr>
<td>460.51250</td>
<td>465.51250</td>
<td>KRF431</td>
<td>M</td>
<td></td>
<td>JHFC FD RT</td>
<td>Fire: Remote Links or Mobile Extender</td>
<td>FM</td>
<td>Fire-Tac</td>
</tr>
<tr>
<td>153.89000</td>
<td>155.40000</td>
<td>KXL292</td>
<td>RM</td>
<td>88.5 PL</td>
<td>Cole EMS</td>
<td>EMS: Dispatch</td>
<td>FM</td>
<td>EMS Dispatch</td>
</tr>
<tr>
<td>154.10000</td>
<td>158.88000</td>
<td>KDL659</td>
<td>RM</td>
<td>192.8 PL</td>
<td>JHFC Public Works 1</td>
<td>Public Works</td>
<td>FM</td>
<td>Public Works</td>
</tr>
<tr>
<td>153.78500</td>
<td></td>
<td>WPG0988</td>
<td>M</td>
<td></td>
<td>JHFC Public Works 2</td>
<td>Public Works</td>
<td>FM</td>
<td>Public Works</td>
</tr>
<tr>
<td>460.58750</td>
<td>465.58750</td>
<td>WVCU448</td>
<td>RMF</td>
<td></td>
<td>JHFC Park &amp; Rec</td>
<td>Parks &amp; Recreation</td>
<td>FM</td>
<td>Public Works</td>
</tr>
</tbody>
</table>

---Confidential & Proprietary---
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:

WireShark Software Application Doing Network Surveillance Over the Air P25 Traffic

---Confidential & Proprietary---
Active/Targeted Exploits:

- 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:

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

- Jamming Device
- Public Safety Radio Base-Station
- LEO w/Radio
- LEO w/Radio
- Terrorist Activity
Question:

- Who has been aware of these types of vulnerabilities?

- Has anyone had discussions with end users about the threat of jamming?
  - Analog/Digital
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
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:

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

**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

GPS Receiver Antenna @ A Base Station

Homemade GPS Jammer Schematic Found on Internet

GPS Jammers For Sale On Internet
Esoteric/Future Possible Threats:

- 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:

- **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?

- 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?

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?
The Bottom Line: What Can We Do?

- **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
      - VLA W
The Bottom Line: What Can We Do?

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?

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?

- 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