Part 1: Project 25
Background

Part 2: Security Flaws
Part 1

Project 25 Background
Who uses P25 Radio?

- Local Law Enforcement
  - Police and SWAT
- Department of Defense
- Secret Service
- Government Officials
- Fire Stations
Countries that use Project 25

- Angola
- Argentina
- Australia
- Bahamas
- Brazil
- Canada
- Chile
- Colombia
- Costa Rica
- Ecuador
- India
  - Source: Motorola
- Kenya
- Kurdistan
- Kuwait
- Latvia
- Malaysia
- Mexico
- Nigeria
- Russia
- Trinidad y Tobago
- United States
- Venezuela
Why use Project 25 or Digital Radio systems?

- Analog signals degrade more over time than digital signals
- More data and meta data can be stored within a message
- Almost lossless data transmission with digital than analog
- Digital signals can be compressed to reduce air traffic
- More configurability in setting up digital systems
- Multi-Vendor Sourcing
  - Having different equipment from different manufactures working together
- Designed to be a replacement for 2-Way Radios
Why use Project 25 or Digital Radio systems?
Difference in Audio quality with analog and digital transmission

- Original Audio
  - 01 – 09 seconds

- Recovered Analog FM with noise signal
  - 09 – 20 seconds

- Recovered Project 25 Digital audio
  - 20 – 30 seconds

Different Digital Signal System Configurations

Simplex configuration: All group members set transmitters and receiver to receive and broadcast on the same frequency. The range of a simplex system is the area over which each station’s transmissions can be received directly by the other stations, which is limited by terrain, power level, and interference from co-channel users.

Repeater operation: Mobile stations transmit on one frequency to a fixed-location repeater, which in turn retransmits communications on a second frequency received by all the mobiles in a group. Repeater configurations thus use two frequencies per channel. The repeater typically possesses both an advantageous geographical location and access to electrical power. Repeaters extend the effective range of a system by rebroadcasting mobile transmissions at higher power and from a greater height.

Trunking: Mobile stations transmit and receive on a variety of frequencies as orchestrated by a “control channel” supported by a network of base stations. By dynamically allocating transmit and receive frequencies from among a set of allocated channels, scarce radio bandwidth may be effectively time and frequency domain multiplexed among multiple groups of users.

Example of a Project 25 setup
Repeaters
Trunking Configuration
Advantages of Project 25

With different configuration designs for Project 25, these systems can use point-to-point or repeaters, instead of using a centralized communication.

Most manufactured P25 radios are for the most part standardized. Some of this is due to the dominance in the market with Motorola.

Designed to be compatible with analog system since they both use the same RF (Radio Frequency) Spectrum.

Voice frames can be encrypted to safely send sensitive information over the air with OTAR (over-the-air rekeying).

Uses Narrow Band Channels, allowing more channels to be used reducing the bandwidth. Narrowband is used within the ranges for VHF and UHF (not the Weird Al Movie).

P25 is designed to provide forward error correction.
Narrow Band

The FCC mandated years ago that radio users in the 150–174 MHz and 421–470 MHz bands convert to 12.5 MHz “narrowband” channels (and equivalents) for their communications by Jan. 1, 2013.

Phase 1 (12.5 kHz) modulation scheme is designed to co-exist with analog legacy.

Phase 2 (6.25 kHz) is backwards compatible with Phase 1 by using trunking systems.
Project 25 Protocol

- P25 Radio operates at 9600 bps (4800 symbols/second)
  - Note: Symbols equates to 2 bits of data (this unit is used in frequency modulation)
- IMBE (Improved Multi-Band Excitation) vocoder (voice encoder-decoder)
  - Listens to a sample of the audio input and only transmits certain characteristics that represent the sound.
- The IMBE vocoder samples the microphone input every 20 milliseconds and produces 88 bits of encoded speech, or said another way, the vocoder produces speech characteristics at a rate of 4400 bits per second. Error correction adds another 2800 bps, and signaling overhead brings the total rate to 9600 bps. P25 standards specify exactly how that information is structured and transmitted.

Source: http://www.signalharbor.com/00jun/
All P25 voice and data traffic is transported by data-link layer frames which are known as data units (DUs). Data traffic uses variable-length packet data units (PDUs) whereas voice transmissions use a variety of fixed-size frames that occur in a fixed structure. Figure 2 shows the structure of a voice transmission. Each voice transmission begins with a header data unit (HDU), followed by a number of voice superframes which carry the compressed voice traffic. That is followed by a terminator data unit (TDU). Each superframe is composed of alternating logical data unit 1 (LDU1) and logical data unit 2 (LDU2) frames, each of which contains nine IMBE compressed voice codewords and differ only in the meaning attached to the non-voice payload of each frame.
When a Project 25 radio sends a message, it does this through multicasting rather than unicasting since there can be many users listening to the same frequency.

Because this system follows a multicast design, there are no acknowledgements (shortened as ACK’s) or sessions involved with transmission.
Over-The-Air-Re-keying

Over-the-Air Rekeying (OTAR) involves radios that use information scrambling — encryption — to ensure that outsiders cannot overhear a conversation. Encryption relies on “keys” that scramble and unscramble the information. Radios can store many keys, but the ability to change or update keys offers better security. Doing this over the air improves secure key management.
Over The Air Encryption

- Algorithm: AES
- Algorithm Type: Type 3 is interoperable interagency security between U.S. Federal, State and Local agencies
- Key Length: 256 bit
- Key Loading Method: KVL Programmer
- Remarks:
  - FIPS 140-2 Certificate

- Algorithm: DES
- Algorithm Type: Type 3 is interoperable interagency security between U.S. Federal, State and Local agencies
- Key Length: 56 bit
- Key Loading Method: KVL Programmer
- Remarks:
  - No longer has a FIPS certificate
  - DES is now considered to be insecure for many applications. In recent years, the cipher has been superseded by the Advanced Encryption Standard (AES).
Other Encryption

- ADP is a Motorola patented and proprietary encryption standard. It is not a published federally certified encryption that any manufacturer could use. Therefore, it cannot be used to communicate securely with other brand of radios except Motorola. It is designed as a cheap implementation of encryption to prevent casual eavesdropping. ADP software encryption isn’t as secure as DES or AES.

- ADP is loaded by the customer programming software so if a radio is stolen and the thief has the customer programming software they can read the system key. ADP is not supported by the P25 OTAR (Over-The-Air-Rekeying) so if the key does get out, there’s no easy way to "fix" everything. All the radios must be returned to the shop to be rekeyed.

- Algorithm Type: Type 4 is for proprietary solutions
- Algorithm: RC4
- Key Length: 40 bit
- Key Loading Method: CPS (Customer Programming Software)
- Remarks:
  - No FIPS certificate
  - Not supported by OTAR (Over-The-Air-Rekeying)
Other Encryption

<table>
<thead>
<tr>
<th>Encryption Algorithms</th>
<th>Motorola</th>
<th>EF Johnson</th>
<th>Harris</th>
<th>Tait</th>
<th>Kenwood</th>
<th>Thales</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES (Federal government encryption standard)</td>
<td>AES</td>
<td>AES</td>
<td>AES</td>
<td>AES</td>
<td>AES</td>
<td>AES</td>
</tr>
<tr>
<td>DES (Former federal government encryption standard replaced by AES)</td>
<td>DES</td>
<td>DES</td>
<td>DES</td>
<td>DES</td>
<td>DES</td>
<td>DES</td>
</tr>
<tr>
<td>ADP (Motorola proprietary encryption)</td>
<td>ADP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: twoway.net/sites/default/files/documents/p25_encryption_and_interoperability.pdf
Part 2

Security Flaws
With every transmission from a P25 Radio, meta-data with the Unit ID, talkgroup ID and NAC (network access code) since the message is sent via broadcast.

- The Unit ID is a 25 bit code that is more the most part unique to each radio
- P25 Radios tend to respond automatically to any ping that it comes across
- Pinged radios are easy to locate, especially when they are in idle
Traffic Analysis (cont’)

- If someone pinged a P25 radio and the radio responded by ending another ping, or an error message, one can locate the radio with latency. (especially with idle radios)

- However, this requires 2 bases at fixed locations with a phased array directional antenna

- This can become a potential threat in military purposes
Denial of Service

- Project 25 have many error-correction codes in their design where each subfield of transmission are error-corrected separately.
- By knowing this, one can jam a single frame by selecting a single subfield in the transmission.
- An adversary can jam the NID (Network ID) subfield in the voice frames. NID’s are 64 bits, and can render a whole message to be renders unreadable.
Denial of Service (Subframe Jamming)

Texas Instruments CC1110 single-chip digital radio transceiver chip can be used to jam subframes in P25 radios.

The chip behaves similar to P25 radios, to the point that it can recognize P25 frames.

A cheap device that uses this chip is in a girl’s toy called “IM ME”.

However, one would need an expensive outward amplifier to make this work.

Source: http://hackaday.com/2010/03/12/easy-im-me-flashing/
Selective Jamming

- If someone was able to make a jammer for P25 radios, they wouldn’t need to jam every transmission. Some transmissions are purposely broadcast unencrypted (such as Evacuation procedures, or non-sensitive information).

- Every transmission that is made to be encrypted “announces” that the message is encrypted.

- A jammer can “listen” to wait for encrypted P25 message and jam their subframes, and force the user to send the message unencrypted.
Intercepting Project 25 Transmission

- With a 24 MHz RF spectrum and having 12.5 kHz channels, the Federal Government has about 2000 discrete VHF & UHF channels.
- Someone can legally own a P25 radio and intercept signals.
- Most sensitive information would be encrypted. But some times there are problems that would cause those messages to be unencrypted.
  - User transmitting unencrypted with an encrypted team
  - Users in a group thought they were encrypted, but weren’t
  - User of a group didn’t have an encrypted key
- Some agencies can be widely known by the channel they are on.