Why (Special Agent) Johnny (Still) Can’t Encrypt: *A Security Analysis of the APCO Project 25 Two-Way Radio System*

Sandy Clark | Travis Goodspeed | Perry Metzger
Zachary Wasserman | Kevin Xu | Matt Blaze

Usenix 2011

P25

- Modulates voice and textual signals into radio packets
    - Current versions transmit at 9600 baud
    - Frame-based protocol
        - Frame begins with 48-bit synchronization pattern
        - 12-bit network identifier, frame type, error correction bits
        - 16-bit header - specifies talk group frame belongs to
        - 96 bits - crypto IV, algorithm ID, key ID
        - Header frame is followed by 1728-bit data frames, then eventually a terminator
            - Data frames are split - first half contains transmitter source ID, and either a destination receiver ID or a talk group ID
            - Second half contains cryptographic information
    - Headers are never encrypted!
- Supports encryption through AES, 3DES, and DES
- Replaces cleartext FM broadcast

Radio Operation Models

- Simplex Operation
  - Communication goes from one transceiver to another.
- Repeater Operation
  - All communications are relayed through a central transceiver that broadcasts them out with higher power.
  - Digital repeaters allow linked communication between distant precincts.
- Trunking Operation
  - Spread-Spectrum communications
  - Central controller dynamically allocates bandwidth on a set of channels to allow for multiplexing.
  - Allows for virtual channels, where users can have more separate conversations simultaneously than there are available frequencies.

P25 Encryption

- Pre-shared symmetric key algorithms are used for all encryption.
  - Keys can be entered manually with special hardware, or over the air via a secure protocol
  - There’s no method for quickly entering or creating new keys.
- Since users cannot rely on bit-for-bit fidelity when communicating via radio in real-world environments, standard cipher modes (like CBC) cannot be used.
- Converts block ciphers like AES and DES to stream ciphers via output feedback mode
  - Shared key is used to encrypt output from a seeded PRNG, then XOR’ed with the plaintext
  - Stream ciphers are vulnerable to known-plaintext attacks when used without message authentication, which radio precludes

Metadata Leakage

- While P25 provides the capability to encrypt metadata, it’s rarely (never) used.
- Individual unit ID numbers are transmitted in cleartext with every header frame.
- While tracking a unit’s physical location requires an RDF setup, this information still allows an attacker to gain privileged knowledge
  - Traffic Analysis
  - Proximity detection

User Tracking

- When the receiver receives a frame that was meant for it, it will silently throw an error and transmit a re-transmit request.
- No warning is ever shown to the user about frame decoding failure, or about retransmitting a request.
- Fairly trivial for an attacker to repeatedly transmit a beacon, then triangulate the responses.
- Active detection is easier for this attack because of the high duty cycle on the attacker’s transmitter.

Userland Issues

- A lack of standardized interfaces across devices makes it difficult to configure security options consistently.
- All handheld devices the researchers examined failed to provide a clear indication as to whether the device was transmitting in encrypted mode.
  - Visual cues on the screen are rarely looked at
  - The physical switch can be accidentally turned
  - Audio cues are ambiguous
- Devices operating in encrypted mode will still receive cleartext transmissions, leaving no indication that data is leaking.

Jamming Techniques

- For narrowband FM broadcast, transmissions can only be jammed by delivering a 2-4x stronger signal to the receiver
  - Very loud and obvious - the radio equivalent of a DDOS attack
- Spread spectrum communication can help prevent the signal from being consistently overpowered
- Digital modulation requires more fidelity, so it can be jammed by a signal 1x as strong as the desired signal
- P25 filters out frames by examining the talkgroup ID in the header, meaning that an attacker can cause frames to be dropped simply by jamming the bits associated with the talkgroup ID

Jamming In-Practice

- Once an attacker synchronizes with the P25 data stream, they need only transmit during the talkgroup ID bits, which last for about 1/100th of a second.
    - At such a low duty cycle, it's very difficult to accurately triangulate a signal's origin
- An attacker could watch for the encryption header and only jam encrypted frames, forcing users back to cleartext communications
- Using a modified children's toy, the authors were able to jam encrypted communications between a nearby receiver and base station

Active Listening

- The authors spent two years recording unencrypted transmissions from local authorities.
- They intercepted, on average, 23 minutes of cleartext audio per day on channels that were meant to be encrypted.
- This audio contained communications by major (federal) government agencies, and sensitive details about police operations that could have compromised certain situations.
- Often, user interface failings led users to believe that they were talking behind encryption when they were not.
- The sensitivity of the conversation material did not seem to change even when users knew they were in cleartext.

Outreach

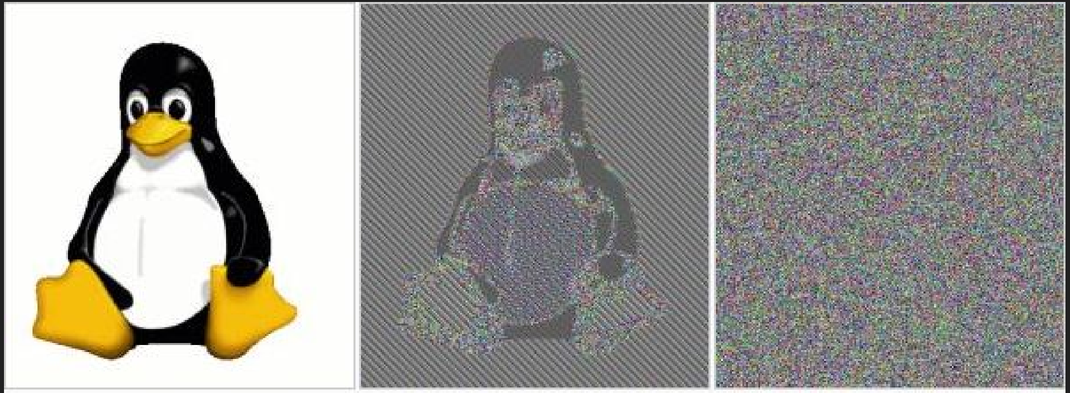
- The authors contacted agencies identified by their P25 listening and advised them on means to improve their security practices.
- Encryption could be locked on or off for any given channel in the user interface, preventing accidental cleartext transmission.
- Frequent key rotation likely causes more trouble than it prevents
  - Issues with rotation train P25 users to simply expect encrypted communications to malfunction.

Mitigations

- Symmetric key cryptography exacerbates the logistics issues.
  - Anything that requires bit-for-bit precision isn’t going to work well over raw radio waves
- Proper use of spread-spectrum technology could minimize jamming.
  - This is what spread spectrum was originally designed for
  - It’s available for P25 radios, just not widely used as a jamming prevention technique
    - Certainly used to exploit available radio bandwidth.
- Metadata should be encrypted by default whenever voice encryption is enabled.
- Protocol should be restructured to prevent jamming by blocking just a few bits
  - Receiver ID could rotate within data portion

Issues with over-the-air cryptography

- Encryption attempts to increase entropy of a message to make it indistinguishable from random noise
- Robust radio protocols attempt to make it as easy as possible to distinguish a signal from the background noise.



Original image

Encrypted using ECB mode

Modes other than ECB result in pseudo-randomness

- Recoverable patterns in encrypted data have been used to eavesdrop on VOIP communications[1].

[1] - Spot me if you can: Uncovering spoken phrases in encrypted VoIP conversations (Usenix 2008)

Discussion

- Is it reasonable for law enforcement agencies to be concerned about these attacks?
- What steps can be taken to mitigate the attacks described by this paper?
- Is it the responsibility of developers to prevent users from accidentally compromising themselves?
- Did the authors take sufficient steps to responsibly disclose the flaws found?
- Is it even possible to build a secure, high-bandwidth communication system without relying on bit-level integrity?