Johnny Cannot Do Anything Right: And Even Knows All About It

February 29, 2012


2. Radios Radios work on the electromagnetic spectrum, running above visible light. We pick a frequency range, which we call a "channel", and listen on both sides of said channel. 2-way radios, used by law enforcement, need to be secured. Previously, security was done via obfuscation, by choosing a channel and not telling others the channel, banking on the fact that the electromagnetic spectrum is very large. Because this is not the most secure, in 1989, security moved from analog to digital, and a move to actual encryption. Backwards compatibility is important. The government has two radio bands reserved for federal use: 11 MHz (VHF) and 14 MHz (UHF), which is about 2000 channels, most unused. An actress named Hedy Lamarr came up with "frequency hopping" in 1942, where the radios jump around different frequencies, making it more difficult for others to find their frequency. This was not officially used until during the Cuban Missile Crisis.

3. Frames Every frame starts with 48 bits of sync bits. This is followed by the network ID (made of 12 bits), the data unit ID (or frame type) which is 4 bits long, and the end is the error correcting code made of 48 bits. The header frame has the talk group ID, the message indicator, and the algorithm ID. The logical link data units is made of an alternating pair. LDU1 has the source Id and the destination ID. LDU2 has the new message indicator, the new algorithm ID, and the new key ID.

The error correction in the LDUs is made for simply voice. It attempts to correctly provide bits to create better voice communication. Because we can’t guarantee bit-perfect packets, we cannot use block cyphers. Instead, we have to use steam cyphers.

4. Modes There are 3 different modes: Simplex, Repeater, and Trunking. The simplex is radio to radio, the repeater is fixed channel amps, and trunking is specialized amplifying router that correctly shifts channels as needed.

5. Problems Encryption problems include accuracy of frames not being guaranteed. We’re unable to use a cryptographic method to guarantee that the sender is the specified sender. Encryption is one way. Metadata problems include data being all in the clear. The device ID is sent "in the clear". There’s a protected flag that needs to be set, thus encrypting the device ID. However, it’s rarely set, and as a result, the device ID is not encrypted. Subsystem problems involve data mode. The data mode has a confirmed mode and an unconfirmed mode. When corrupt data is sent, a retransit request is sent back. Even in encrypted mode, the only thing that’s checked for the data pack is the header. This can be faked by listening for an encrypted packet and stealing its header. Clear tolerance errors stem from clear transmissions always being accepted. A balance must be struck between security and emergency. Keying problems occur from keying updates. Key updates come from a central location and occur over the air. However, if a key needs to be updated, it becomes a problem in the field.

UI has a few problems. First, customizable UIs result in a lack of concise or comprehensive manuals, but
allow for the UI to be molded to specific needs. Second, the encryption switch is on the same knob as the volume switcher and is easily changed by accident (this is on the Motorola XTS-5000). The third problem is that the only noticeable difference between encrypted and unencrypted is the LED, which is not helpful as it’s not specific. The walkie-talkie also uses a small beep to convey encrypted/uncrypted but it’s very ambiguous.

6. Attacks  Attack #1 is jamming. It’s easy to jam a narrow channel if you’re able to find the appropriate band. You simply need a slightly more powerful transmitter to jam the frequency. It is possible to jam frequency hoppers by finding the entire band. However, the only part of the frame you need to jam is the Data Unit ID, which is only 4-bits large. However, DUID has its own error correction. Because a standard voice frame is 1728 bits, and we only want to jam the data unit ID and its error correction, we only have to jam 3.7% of the frame. As a result, we do not need something too terribly powerful to jam it.

We can also selectively jam. We know if a frame is encrypted, that messages in the clear are received with minimum disruption, and that we can’t add new keys in the field. Therefore, we can push all users in the clear by selectively jamming all encrypted frames, errors would be blamed on encryption working incorrectly. We can also target anything with the datatype of "trunked".

7. Experiments  The experimentors used a small, cheap jammer via a pre-teen texting device which cost $15. Using the small device, they jammed just the datatype of frames (the DUID), including the standard models used in the field. Due to legal repercussions, they did not test this in the field.

The experimentors also went out into the field and listened to general use in major metropolitan areas, listening to federal law enforcement bands over several months. Each city had about 110 channels used. After two years of sampling, they saw roughly 20-30 minutes of use per day. They recorded all transmissions in the clear and threw away non-sensitive transmissions. They split apart the in clear transmissions into 3 different categories. First were individual errors (someone made a mistake). Second was group errors where all users are in the clear but someone says something that lead the researchers to believe that the group was encrypted. Third were key errors where all users move to the clear. The researchers noticed that the no attempts were made to disguise their use even when it’s known that they’re in the clear.

8. Conclusion  "Everything is awful!". Real fixes need to be made at the manufacturer level, including a change in the protocol and an addition of defenses to the radio spectrum. Distributors need to make the UI clearer and better default values (like the encryption clear switch doing nothing). Also, re-keying policies need to change.

9. Questions  Joe pointed out that testing encryption is very difficult, as program testing is generally very binary: it either works or it doesn’t. When checking things like encryption keys, that’s not something so easy to fix.

Discussion turned to how "badass" Matt Blaze is for recording two years of law enforcement radio broadcasts.

Reza and Joe began discussion of encryption on cell phones. G2 encryption has been broken, and since all GSM phones are backwards compatible, GSM phones’ communication is insecure. Reza suggested setting aside encryption for each city separately. Reza suggested an application of the cellular network to P2P radio communication. Adam pointed out that it’s not difficult to DDOS a single cell tower.

Joe points out, "why isn’t everything encrypted?" It’s pointed out that rapid communication may run into an issue. If you have someone who is not up to date on the latest key, communication will not happen.