Dallas Siren Hack: RF Network Vulnerabilities Exposed

By Bob Baxley

Published: 2017-04-14 · Archived: 2026-04-05 21:15:56 UTC

In light of recent events, particularly the Dallas siren hack we'd like to go through a couple of plausible scenarios that might explain this attack and how they relate to the need for more security when designing RF-enabled devices and implementing RF-enabled networks.

For now, let's look at the Dallas incident to examine how some public safety and large-scale RF networks work, how they might be vulnerable to such attacks, and what you should take into account when designing and securing such networks.

Inside the Dallas Siren Hack

The Dallas Office of Emergency Management (OEM) never disclosed exactly how their system was compromised. However, by examining common network designs and transmission methods, we can piece together plausible scenarios that explain how attackers gained access.

At a high level, emergency siren systems often include:

- A **central control node** (usually a computer linked to RF radio equipment and an antenna).
- Multiple **siren nodes** spread across a large geographic area. Each includes a pole-mounted siren, a radio receiver, and a control module.

This wide-area distribution is why RF is often chosen: it allows a single controller to broadcast commands to many devices simultaneously. Unfortunately, that also means a successful compromise can cascade quickly across the network.

How RF-Enabled Emergency Networks Operate

Single-Frequency Networks

One possible scenario for Dallas is that they use a single-frequency network. In this situation, all the sirens and radios operate at either end of a single-frequency network, which is registered with the FCC.

A single-frequency network uses a large single transmitter to cover an entire emergency region. The transmitter might be up high on a tall building or on a hill and uses a very, very large power output to allow the radio waves to propagate over a significant distance and cover the entire array of sirens. Since all of the Dallas sirens appear to have been set off at once, this may indicate some sort of centralized control over all of them, as opposed to individually, visiting each one and setting it off.

So, in the single frequency network attack, the attacker most likely traveled to a high point to achieve a good propagation to all the sirens. The equipment to undertake this sort of attack would have included a powerful transmitter, a power amplifier, and antenna set to the specific frequency used by the Dallas system (or around about those frequencies).

Repeater-Based Networks

In this network there is a centralized instance of a single repeater to cover a large region. The repeater accepts weaker signals on one 'input' frequency and rebroadcasts them at a stronger signal on a different 'output' frequency to cover the larger area.

How does this play out? One hypothetical scenario is that a controller module at headquarters sends out a transmission on the input frequency, which is registered to a particular repeater. The repeater then rebroadcasts the same transmission over the output frequency, but at a much stronger signal. The siren modules will be listening on the output frequency, and anything transmitted on the input would be repeated to the output. That's how you can cover this broad area.

We've briefly covered network configurations, now let's take a look at how commands are sent.

Analog vs. Digital Command Transmissions

How commands are sent is just as important as the network topology.

Analog RF Networks

The simplest and least costly approach to use is an analog technique. A normal analog single-frequency or repeater network, most likely using narrowband FM, is used to send voice data. To listen to these transmissions, all that is needed is a hand-held radio, which is easily purchased from eBay or Amazon for less than $30. You don't really need anything more sophisticated than that.

If it's analog transmission, then you can send a series of tones. One possibility is exactly the same sort of dual-tone multi-frequency (DTMF) tones you hear when you dial the digits on a telephone. What might be the case here is that tones are transmitted from headquarters to a receiver and demodulator at each node, and each node is programmed to listen for a certain sequence of tones. Upon receiving the tones, the node will enact some command, in this case, to activate the sirens.

Now, in either single-frequency or analog case, if there is someone out there that has found the frequency in use, they can simply listen for those tones to be transmitted prior to the monthly test. In some cases, where there's practically no security, those tones are transmitted in the clear, and you're able to replay them to achieve the same effect.

Where might the attacker be? On a single-frequency network, the attacker needs to be up high, with a very powerful transmitter,a power-amplifier, and antenna. With an analog repeater, the attacker simply needs to transmit close to the repeater, perhaps with a directional antenna, on the input frequency, and have those tones in the initial broadcast, rebroadcast by the repeater over the entire network to achieve the same effect.

Digital Repeater Networks

With a digital repeater, emergency headquarters has a radio to send digital data instead of just narrowband FM. Data is rebroadcast by the digital repeaters to ensure full coverage of the emergency area.

There may be one repeater, or in the case of modern public safety networks, it might be established as a simulcast network, which means that multiple synchronised repeaters would cover an even broader, geographic range.

The difference here is, instead of tones such as the DTMF tones, there would be a distinct packet of data. This is received by a radio, decoded and then the received command is put into action, in this case, to activate the siren at each node.

Why Encryption Often Falls Short

Digital networks can include **encryption**, but many do not. Even when implemented, encryption is sometimes flawed:

- **Weak key management**: makes keys easy to guess or reuse.
- **Lack of initialization vectors**: allows replay of “encrypted” packets.
- **Over-the-air rekeying**: if hastily implemented, can still leave gaps.

In Dallas, reports suggested encryption was added after the hack. But given industry trends, it is unlikely the system had strong end-to-end protection.

Trunked Networks and Replay Attacks

Some emergency systems use **trunked networks**, where multiple frequencies are pooled and dynamically assigned.

While efficient, trunked systems share the same vulnerabilities:

- No authentication of transmitters before a call is set up.
- No built-in message authentication.
- No mandatory low-level encryption.

As a result, trunked networks remain **susceptible to replay attacks**, just like simpler analog and digital systems.

Smart Cities and IoT: Expanding the Attack Surface

The risks extend beyond public safety sirens. As **smart cities** adopt RF technologies for traffic lights, streetlights, and building automation, the attack surface widens.

- **IoT devices** often use low-power RF protocols like ZigBee, Z-Wave, or LoRa.
- Many sensors ship with **multiple radios** for “future flexibility.”
- Security is frequently an afterthought as manufacturers rush products to market.

Bastille's own research has revealed RF vulnerabilities in common office devices, from wireless keyboards to HVAC controls. If left unsecured, attackers can exploit these devices to compromise not just **individual endpoints**, but **entire critical infrastructure networks**.

Security by Design: Lessons for RF Devices

The Dallas siren hack demonstrates that **security by obscurity is not security at all**. Simply relying on proprietary protocols or dedicated frequencies is no longer sufficient — modern attackers have cheap, powerful tools to exploit weaknesses.

To secure RF networks, organizations must:

- Implement **strong, properly managed encryption**.
- Require **message authentication** to prevent replay attacks.
- Harden **end nodes** to prevent unauthorized control.
- Treat RF systems with the same rigor as **wired and Wi-Fi networks**.

How Bastille Helps Protect Wireless Infrastructure

Bastille specializes in helping organizations **sense, identify, and locate all RF-enabled devices** in their environment — including the ones they may not know exist.

With a **Wireless Vulnerability Threat Assessment**, Bastille can expose hidden RF risks across public safety, enterprise, and IoT networks, and help you secure them before attackers exploit them.

If you'd like to learn more about what Bastille does request a demo or your own Wireless Vulnerability Threat Assessment.
