How vulnerable are trunked radio systems to terrorist hacker attacks?

Posted on November 10th, 2007
by daryl in Public-Safety Radio

Links to supporting information about this topic are purposely omitted in an effort to not aid potential trunked radio system attackers.

It's rarely talked about, but well-known by most engineers who are involved with police and fire radio systems. Trunked radio systems are highly vulnerable to denial of service attacks that could quickly render them useless. In less than an hour of searching the Internet, I found sufficient information to create malicious software that would cripple Motorola SmartNet and MA/COM EDACS trunked radio systems.

Trunked radio systems work by sending computer data between a mobile radio and a central system controller. When a mobile user presses the push-to-talk button, the radio sends a digital message to the system controller requesting a channel assignment. If a channel is available, the system controller sends a message back to the mobile radio with the channel information, and also broadcasts a similar message to other radios in the fleet so that they can tune to the designated channel if necessary. A voice conversation can occur after the channel assignment process is completed.

It would be easy for a technically savvy criminal to intercept or maliciously falsify this digital control message. Software could be crafted to intentionally simulate a situation where the entire radio system appeared to be busy. Legitimate users would not receive a valid channel assignment and could not communicate, resulting in a serious denial of service attack. The protocol used between the mobile radio and system controller is rarely encrypted, even if the voice transmission is scrambled. Trunked systems rarely, if ever, include features to prevent denial of service attacks.

Typically we think of computer and radio hackers as sole operators who do not have an organized agenda. What would happen if a technically sophisticated terrorist organization fabricated devices to intentionally disrupt trunked radio system operations? The devices could be built for less than $1000 each, distributed over a wide area, and remotely controlled. It would be nearly impossible to locate and disable the devices in time to mitigate the problems they would cause.

Conventional (non-trunked) radio systems are not vulnerable to such attacks because they do not rely on computers to control channel assignment.

---

*11/12/2007 Addendum*This article has generated a surprising amount of interest. I have received more than 50 e-mail messages about it in the past two days. No one has disagreed with the issue

that I pointed out, and several government officials have told me that they will incorporate this failure scenario in future disaster training exercises.

Some readers have suggested that all radio systems are vulnerable to jamming and that trunked radio systems are no different. I would like to clarify my position on this point. I believe that trunked systems are more vulnerable by an order of magnitude, or greater.

Traditional jamming usually disrupts only a single radio channel at a time and the source can be found by well-known direction-finding techniques. Maliciously interfering with a trunked system at the software level is different in that the offender could simultaneously disrupt operations on multiple channels at multiple sites by exploiting the purpose for which the system was designed. Service could be denied for multiple talk groups (police, fire, ems etc) over a large geographic area with one or more offending devices that radiate a very low amount of RF energy. Traditional direction finding would be very difficult because the offending transmitter would not have to be transmitting continuously.