URGENT COMMUNICATIONS
Formerly MRT: Mobile Radio Technology

Subscribe About Us Advertise Logout RSS

Advanced Search | Enter Keywords SEARCH

MOBILE VOICE | MOBILE DATA | NETWORKS & SYSTEMS | TEST & MEASUREMENT | POLICY & LAW

urgentcomm » Magazine Articles » Oil and water

MY YAHOO! newsgator Bloglines ShareThis

OIL AND WATER

Jul 1, 2008 12:00 PM, By Doug Mohney

Public-safety agencies are finding that encryption and interoperability don't always mix

First-responder communications interoperability has numerous challenges ranging from agencies operating on disparate radio frequencies and using different waveforms to the verbal shorthand such organizations use in their daily operations. Encryption of radio traffic adds another layer of complexity to achieving coordination between agencies — even if everyone is using Project 25 radios.

“For systems that connect agencies using different digital systems that utilize encryption, [encryption translation] is an issue, and can create either delays or serious communication problems for agencies that require end-to-end encryption,” said Luke Klein-Berndt, chief technology program manager for the DHS Science & Technology Directorate's Office for Interoperability and Compatibility.

Klein-Berndt added that agencies often resort to the use of analog signals as a lowest common denominator, but in doing so they sacrifice the modern features offered by digital systems and the encryption of privileged information.?“This is precisely what the proliferation of Project 25 is hoped to mitigate,” he said.

Support for encryption is built into the standard, so a P25 radio theoretically should be able to talk to another P25 radio, regardless of the manufacturer or agency. “It's a pretty common request to be able to interoperate when agencies ask for a P25 radio,” said John Oblak, vice president of standards and regulatory affairs for EFJohnson Technologies. “The [National Guard] military base has to interface with the state highway patrol and a couple of local authorities.”

But agencies using P25 first have to agree to use encryption, and therein lies the rub. Some agencies say they don't need it for daily operations, while others prefer to have the option to purchase encryption capabilities through a software upgrade at a future date rather than spending the money up front. When an incident occurs that involves multiple agencies, those using encryption have to turn it off to communicate, maintain a cache of encrypted radios to distribute to other agencies, or rely on a gateway solution between networks, which can be unwieldy and time-consuming to set up.

Should consensus to use encryption be reached among disparate agencies, the next step is get them to agree on which type of encryption they should use. Under the P25 specifications, multiple methods are supported, with the most common being the federal government's DES and AES standards. “Many manufacturers have implemented both [types],” Oblak said. “It shouldn't be much of an issue.”

But older radios that haven't been updated may only support DES because the P25 standard predates the federal government's policy to replace DES with AES. However, that's not a big problem, according to Klein-Berndt.

“Falling back to DES is, indeed, what agencies use when both do not have AES compatibility. … P25 specifically accommodates DES for the backwards compatibility that you describe,” he said.

Even when the type of encryption has been agreed on, there are other logistical hurdles to clear. For instance, to access an encrypted channel, every radio involved has to have the same mathematical keys, so a central party has to keep track of the keys and have a mechanism to distribute them.

“The biggest issue is going to be key management,” Oblak said. “That boils down to more logistics than technology.” However, an agency's standard operating procedures (SOPs) will identify those responsible for managing the keys during a response, Klein-Berndt said, with the designated individual the communications unit leader.

Rekeying can be done through two methods. “One is a mechanical or physical key loader,” Oblak said. “For manual key loading, you … take the key loader device to each radio.”

The other option is over-the-air-rekeying (OTAR), which does not require the manual effort necessary to physically connect a device to each radio in a fleet to upload a new key. Consequently, it is a far more preferable method to change and update keys as needed.

Hot Spots

Project 25
Interoperability
Rebanding
PSAP

Essential Reading

A corner turned
Let the buyer beware
When measurements aren't feasible
Verizon, AT&T both plan 2010 launch for LTE networks
Motorola shuffles the deck

Most Popular Articles

TV white spaces could be a boon to rural areas
Contemplating the seemingly unthinkable
Sprint Nextel's rebanding price tag continues to increase
Sprint Nextel: iPCS situation will not harm iDEN customers
NATE revises tower climber fall protection training standard

"The time and effort it would take to rekey varies with the quantity and type of system, and whether over-the-air-rekeying is available," Klein-Berndt said. "[The manual] effort — which can involve the return of hundreds of radios to a single technician — is part of what is slowing the adoption of encryption, especially in an incident. However, the availability of newer systems and wider availability of OTAR is helping."

P25 specifications spelling out encryption methods and OTAR eventually are expected to move first-responder agencies away from relying on dedicated radio caches for secure communications. Klein-Berndt expects compatibility problems stemming from incompatible equipment implementations to be "greatly reduced — if not eliminated" as the P25 Compliance Assessment Program rolls out and more equipment is tested in a consistent, industry-wide manner.

Nevertheless, Klein-Berndt stressed that P25 equipment "is not a silver-bullet solution," noting that interoperable, encrypted communications isn't achievable without effective governance, SOPs, training and exercises.

"For many agencies, regional training and exercises should provide an opportunity to program neighbor jurisdiction's keys/numbers into their radios," he said.

For agencies not using P25 radio systems, introducing encryption to interoperable communications is even more vexing, as interoperability often is accomplished through the use of network patches and Internet protocol (IP) gateways.

Gateways present their own challenges. Smaller agencies are unlikely to have the budget to purchase and install a gateway, while larger municipalities may require multiple gateways to move communications between organizations. There's also a mindset challenge: many public-safety agencies are reluctant or unwilling to establish secure communications with other public — and most especially private and commercial — organizations. For instance, while a law-enforcement agency has no conceptual problems trusting fire and safety groups since it works with them on a daily basis, establishing a secure channel with the American Red Cross, a public utility and/or a Fortune 500 corporation involved in an incident is a significantly different ballgame.

"In the end, the problem will reduce to how and when you let [other agencies] into your security domain," said A. Riley Eller, vice president of Seattle-based CoCo Communications, a vendor of secure, interoperable communications solutions. "Almost always there is a gateway process. There are models that say you can carry fully encrypted traffic from network to network, but effectively what you're doing is creating one large security domain."

Instead, CoCo advises a peer-to-peer model to create secure interoperable "bridges" as needed. "Everyone else says you should join a larger security domain," Eller said. "You get a big bureaucracy, a barge. We say rather than buy a barge for everyone to climb on, you should get a vine and string together a bunch of rafts to make a barge."

CoCo's security model incorporates the same secure SSL certificate technology that is used in online banking. Unlike online banking transactions, however, authentication in a public-safety application is bidirectional, meaning that each party has to verify its identity and the identity of the other party. After the two parties have authenticated each other, virtual voice and data circuits can be set up at the click of a button to create radio talk groups and online conferences. Dispatchers can use off-the-shelf software to patch together parties in a drag-and-drop fashion.

"We've found that … you can use the common channel [frequency] rather than shoving off a talk group to a corner frequency," Eller said. "You can suspend the daily chatter. It seems to work, and is proportionate and appropriate for disasters."

CoCo's open-standards approach was successfully demonstrated in November during a disaster drill at Dallas Love Field. The system, funded through a competitive DHS grant program in 2005, connected the Dallas Department of Aviation and the city's fire-rescue and police agencies, as well as non-traditional participants such as the Texas Departments of Public Safety and Health, Centers for Disease Control and Prevention, and Southwest Airlines.

Perhaps the biggest challenge to using CoCo's system is getting all the agencies to buy into its software and hardware. While much more affordable on a per-agency basis than a traditional gateway solution, organizations have enough difficulty agreeing on the type of radio communications and encryption they will use during a major event — even in a standardized P25 world.

Back to Top

RESOURCES

EDITORS PICKS NEWSLETTERS WHITE PAPERS JOBZONE

BUYERS GUIDE ADVERTISING CALENDAR RSS