ALMR INSIDER

Volume 12, Issue 1 January 15, 2018

ALMR Help Desk

In Anchorage:
334-2567

Toll Free within Alaska (outside of Anchorage):
888-334-2567

E-mail:
almr-helpdesk
@inuitservices.com

Follow us on Twitter:
@ALMR_SOA

Inside this issue:

Project 25 Radio Authentication

For decades, public safety communications system operators were protected from unauthorized access through the restrictions that equipment manufacturers placed on radio programming equipment. So even if an unauthorized individual had radio equipment and programming software, without the 'system key,' programming a radio for an individual radio system was not possible.

Of growing concern is the ability to purchase public safety grade communications equipment over the internet. Access to such equipment can provide unauthorized individuals the same access to a radio system as legitimate users. System keys, which can be a software file, or can be a hardware-based key, can help prevent this. Software keys are somewhat more difficult to secure, as they can be copied or transferred to unauthorized individuals with relative ease, but hardware key devices provide an increased level of security as they can be copy protected and configured with other security provisions like expiration dates, cycle limits and restricted rights.

Individuals with access to pirated programming software or system keys can monitor control channel traffic to determine a valid radio ID and program a radio with a duplicate, but valid, ID. Therefore, as technological abilities of those wishing to steal service or disrupt public safety communications systems expand, additional measures to protect unauthorized access to public safety communications systems are required. New Project 25 radio standards explore the need for, and functionality of, P25 link layer authentication services on trunked radio systems and provide a method for the radio system to prevent unauthorized access by authenticating subscriber radios for operation on P25 trunked radio system using a registrations authorization database that identifies valid/invalid unit IDs.

Public safety system operators and radios users have long been aware of the vulnerabilities that can be caused by unauthorized radios or radios with duplicate IDs on the system. The Project 25 standard defines a challenge response system that allows the radio system and/or subscriber radio to authenticate itself before service is granted. Authentication services are handled by an authentication facility, which could be a standalone server, or an application service running on an existing system device. Authentication uses a secret key, which is stored in the radio system and subscriber radio. Each subscriber radio has its own unique authentication key, which is associated with the subscriber radio unit ID. For subscriber radios that are operating with multiple systems or multiple unit IDs, multiple authentication keys are assigned.

The P25 radio system initiates the authentication process once the subscriber radio registers with the system. This is done by sending an authentication challenge to the subscriber radio. The subscriber radio returns a response to this challenge, which requires knowledge of the unique authentication key. The radio system then compares the subscriber radio response, and if correct, the authentication is successful and the subscriber radio is considered valid. If authentication fails, then the subscriber radio is denied access to the radio system. Of course, the system will not interfere with an authenticated subscriber in the event that an invalid radio attempts to authenticate using the same radio ID. While authentication generally occurs at initial registration with the system, the P25 standard allows for authentication commands to be sent to subscriber radios at any time.

If a radio with an authentication key is lost or stolen, the authentication key can be disabled in the authentication facility, preventing the unaccounted for radio from gaining access to the system. The P25 authentication standard also provides support for mutual authentication. If this option is supported, not only can the system (continued on page 2)

Global Cyberattacks Provide Stark Reminder of Need for Secure Systems

Mid-2017, ransomware was activated across unprotected Windows computers located in more than 150 countries around the world. As a result, users of an estimated 300,000-plus computers were locked out of their data, which hackers said would be released at a cost of $300 in bitcoin currency, which would allow the recipients to collect anonymously.

Multiple media reports indicated that the ransomware exploited a vulnerability in Microsoft's Windows operating system, using a tool developed by the National Security Agency (NSA) that was released to the public by WikiLeaks earlier in the year. Microsoft issued a software patch to address the vulnerability prior to the attack, but the patch clearly was not installed by everyone for a variety of reasons, ranging from laziness to a need to avoid updates that would prevent old software applications from operating properly.

Known as WannaCry, the ransomware did not just hit individuals; many enterprises were victimized, including a host of computers associated with the health system in the United Kingdom (UK) - a circumstance that created a myriad of issues for medical staff and patients.

This unfortunate episode served as yet another reminder that cybersecurity needs to be at the forefront of future developments, particularly as society becomes increasingly reliant on technology to do tasks that have greater importance.

Most of us are big fans of technology - learning about advances and innovations being developed by engineers, both from a hardware and software perspective. The functionalities and efficiencies that such solutions promise to bring to society are expected to be critical in the future, from drones to the Internet of Things (IoT), to a wide variety of analytics.

When functioning in harmony, these interconnected advancements should make life safer and more convenient, and the power of software allows many of these solutions to be updated and upgraded quickly, without the need to buy and install new hardware all the time.

But these characteristics also could prove to be problematic, as this cyberattack highlighted. The WannaCry ransomware was able to spread throughout a computer system, searching for vulnerable devices to attack. Users were not required to click on a phishing e-mail to be victimized, according to security experts.

Not being able to access patient records was a huge problem for UK hospitals, but the scenarios could have been much worse given that in the future robotics could be used to perform increasingly important tasks. Similarly, wearable health devices offer tremendous promise to enable monitoring the condition of patients while having minimal impact on their quality of life. The impact of a cyberattack, or even an unintentional "software glitch," could have significant implications on a patient.

The healthcare system is not unique in this regard. Advancements in remote-controlled drones and autonomous vehicles have the potential to provide tremendous convenience, efficiencies and safety, but the notion of a cyberattack or other disruption to the underlying communications networks - for instance, jamming of critical control signals - is frightful. It's not hard to imagine how an orderly flow of traffic could turn into a demolition derby, if proper safeguards are not in place.

With all of this in mind, it is vital that the security of the communications networks, such as ALMR - both physically and in the cyber realm - is ensured when critical functions are performed. Public safety entities have long embraced this notion with their land mobile radio systems, and it will be even more important as first responders begin to utilize FirstNet and next-generation 9-1-1.

(Excerpts taken from article by Donny Jackson, Urgent Communications, May 16, 2017)

Project 25 Radio Authentication (continued)

authenticate a subscriber radio, but the subscriber can authenticate the radio system. Mutual authentication provides protection against adversaries that attempt to disrupt service to subscriber radios by imitating a valid radio system. At present, not all P25 infrastructure providers are offering radio authentication support for mutual authentication.

Authentication services in P25 systems utilize the Advanced Encryption Standard (AES) with a key size of 128 bits. This provides a high level of cryptographic security with over 3.4x10^{38} possible authentication key combinations. AES-128 is also approved for use in FIPS-140-2 validated cryptographic modules. Appropriate P25 standards have been updated to ensure the P25 ecosystem supports radio authentication. For example, the P25 Key Fill Device Interface has been updated to support loading of 128 bit AES keys for radio authentication into both subscriber radios and authentication centers.

P25 subscriber and infrastructure manufacturers are currently shipping products with P25 link layer authentication and public safety agencies have successfully deployed link layer authentication on fielded P25 radio systems. P25 link layer authentication is just one of many strategies available to protect P25 mission critical communications systems from unauthorized access.

(Excerpts taken from Project 25 Technology Interest Group (PTIG) website, article by Mr. Jim Holthaus, Vice President, Chief Technical Officer, BK Technologies, December 2017)

The Power of Proactive Radio Maintenance

First responders put their lives on the line each day to protect the public from harm, whether it is a routine traffic stop or an emergency situation. It is vital their radio equipment works properly to provide them with clear and reliable communications when they need it the most.

Currently, the only way for public safety agencies to determine whether a radio is functioning to specification is to bring the radio in for annual maintenance or wait for a user to report a problem. This means scheduling thousands of radios for costly annual service checks that require hundreds of technician man-hours. It also means taking radios out of the field, where they are needed most.

Approximately 15 to 20 percent of subscriber radios can drift out of alignment annually, causing them to fail at anytime. Many public safety agencies have anywhere from 2,000 to 10,000 radios or more on their LMR systems. Technicians do not know which radios need to be aligned, and which ones are working well, without bringing all the radios in for testing. The common practice of testing all radios leads to spending hundreds of thousands of dollars in time and manpower each year.

The two-way radios that public safety agencies use rely on an internal reference oscillator to maintain the radio on the proper frequency. Over time, these oscillators drift off frequency, eventually causing the radios to fail. In order to measure a radio's alignment, a technician has to physically connect an analyzer device to the radio. Due to budget constraints, many users skip these annual checks and rely instead on reactive radio maintenance. Adopting a 'fix it when it fails' policy, they leave the reliability of their communication lifeline to chance for first responders.

So how do agency radio managers keep ahead of this issue and identify radios at risk for failing? Given the large number of subscriber radios on an LMR system, managers often determine if a subscriber radio is working correctly or not, by scheduling them for routine maintenance or by waiting for the user to complain of a problem. Neither is an ideal scenario.

The radio maintenance challenge that many face is straightforward: How to identify a particular radio at risk of failure and service it, when there isn't the time or money to provide preventive maintenance (PM) for every radio? The answer lies with new technology. There have been substantial technological advancements that have changed the traditional approach to radio maintenance for LMR systems.

The Department of Homeland Security Science and Technology Directorate has been exploring a hardware and software technology called DiagnostX that can evaluate radios at long-range and over-the-air, while deployed in the field.

DiagnostX constantly monitors and evaluates active radios on an LMR system. This ensures minimum hardware and personnel downtime and assures peak operational readiness. The over-the-air radio waveform analyzer system can be installed at any system site at the receive antenna multicoupler, or it can use any other receive antenna.

DiagnostX has an intelligent RF (radio frequency) receiver that scans the radio network's downlink (outbound) control channel frequencies to identify the frequency in use. Once the active downlink frequency has been identified, the system monitors the corresponding uplink (inbound) frequency and analyzes all control channel transmissions. After tuning to the uplink control channel frequency, DiagnostX monitors and characterizes all transmissions, distinguishing "suitable" from "non-suitable."

By identifying radios with operational problems and addressing them, an agency will experience a higher level of system performance and reduce maintenance costs by 50 percent or more. Servicing only those radios that are out of alignment will free up more time for technicians to focus on other system issues that need attention.

Regardless of the challenges associated with dwindling budgets and personnel cuts, the bottom line for first responders, who risk their lives on a daily basis, is their commitment to protect and serve the public. DiagnostX has already proven to be a powerful tool for public safety agencies ensuring that police, fire and EMS personnel can feel confident that their radios will work whenever and wherever they are needed.

(Excerpts taken from "The Power of Proactive Radio Maintenance," LocusUSA White Paper, November 7, 2017)

Real-world Incident Highlights Need for Subscriber Maintenance and Training

The importance of subscriber maintenance was recently highlighted in a real-world situation involving an ALMR agency response to an early evening vehicle accident. One on-site responding agency encountered difficulties in communicating with their dispatch center and contacted the System Manager, who sent a technician to the ALMR offices and verified the System was operating correctly. The next day, the System Manager traveled to the area in question and determined the sites there were also performing properly. A review of one responder's radio revealed substantial issues with the codeplug and frequency alignment. The radio was properly aligned by the System Manager and the agency will be assisted in updating their codeplug. A review of radio traffic during the incident also revealed the dispatch center and responder were on different incident command (IC) talk groups and different regional IC zones for at least some of the transmissions.
(Article by Mr. Del Smith, ALMR Operations Manager)

Alaska Gets Waiver for VHF Base Station Using Nonstandard Channel Centers

Alaska operates a wide area, VHF, public-safety trunked radio system known as the Alaska Land Mobile Radio (ALMR) System, which serves local, state and federal agencies throughout much of the state on a single shared infrastructure. ALMR operates using Project 25 (P25) technology, and pairs about 1.5 megahertz of spectrum from the public-safety pool (150 MHz band) with an equal amount of spectrum from the federal government (138 – 144 MHz band) to create 110 channel pairs with 12.5-kilohertz bandwidth.

On February 7, 2017, Alaska filed an application to add a base station to be located in Delta Junction. Users operating mobile units near Delta Junction had often experienced coverage issues due to a ridge through the town, which shields it from the nearest ALMR base station. Therefore, Alaska sought to license five public-safety pool channels at the proposed new base station and asked for a waiver to operate four of the five channels with center frequencies offset 2.5 kilohertz above or below the standard channel centers.

"Without the ability to operate on rechannelized public-safety pool channels, Alaska would either need to reprogram the more than 20,000 subscribers in use on its system, or forego adding the base station..." the FCC order said. "In making our decision, we find persuasive the fact that Alaska's frequency coordinator considered incumbents operating on the adjacent-standard channel centers as co-channel to Alaska when it coordinated Alaska's proposed operation on offset channels."

(Excerpts from article in Mission Critical Transmission e-newsletter, November 30, 2017)

Help Desk (In Anchorage Bowl):
334-2567

Toll Free within Alaska:
888-334-2567

Fax: 907-269-6797

Email: almr-helpdesk@
inuitservices.com

Website: http://www.
alaskalandmobileradio.org

Follow us on Twitter: @ALMR_SOA

2017 ALMR Statistics

Group Calls (cumulative):
12,809,576

Busies (cumulative)/
Percentage rate of calls:
6,523 / .05 percent

Agencies (end of year):
127

Subscribers (end of year):
21,731

Alaska Land Mobile Radio
Operations Management Office
5900 E. Tudor Road, Suite 121
Anchorage, AK 99507-1245

ALASKA MUNICIPAL LEAGUE