ALMR INSIDER

Volume 18, Issue 3 July 15, 2024

ALMR Help Desk

In Anchorage: (907) 334-2567

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

E-mail: almr-helpdesk @beringstraits.com

Follow us on Twitter: @ALMR_SOA

Inside this issue:

Cyber Threats and Impacts to Land Mobile Radio

Cyber-attacks against land mobile radio (LMR) systems, while rare, are increasing and disrupting mission-critical communications for first responders. Since January 2023, three separate compromises of broadband and P25 radio networks, with two of these attacks occurring this year, resulted in an average of seven days downtime for communications systems, forcing defenders to resort to alternative channels or backup systems.

Other attacks targeting emergency radio communications occurred but did not meaningfully disrupt communications. For example, a November 2023 distributed-denial-of-services (DDoS) attack on a public safety entity's broadband radio network caused no downtime. The attack pushed DDoS protection "to the maximum" but showcased how defensive preparation can help mitigate cyber-attacks to LMR systems.

Adversaries used credential abuse and vulnerability exploitation techniques to access these systems, and in at least one instance relied on a misconfigured SSL virtual private network connection to create a network foothold.

LMR network topography can vary depending on technology and implementation; however, some risks are commonplace. Password reuse, default passwords, and misconfigured or insecure virtual private networks (VPNs) increase the likelihood of direct compromise and are frequently observed. These issues are consistent with the top cyber risks to LMR as described by the United States Cybersecurity and Infrastructure Agency (CISA). External connections involving radio networks are growing, which increases the need for effective security measures.

Adversaries regularly attempt brute force access to LMR networks during opportunistic campaigns as part of a targeted operation. In May 2024, Russian-based and proxied IP addresses attempted to log into a Virginia P25 radio network. Over a 24-hour period, there were approximately 60,000 individual failed login attempts at a rate of 41-per-minute. This campaign was malicious and designed to create access points across multiple environments through password spraying. The same IPs attempted to log into a broadband radio network in Connecticut and used similar usernames and passwords, further supporting the assessment that the activity was part of an automated campaign.

The rate of brute force login attempts on other radio networks varied widely from victim to victim. In some cases, defenders saw only double-digit login attempts over a period of months, while others contended with hundreds of thousands of failed logins, further enforcing the likelihood of opportunistic campaigns taking advantage of increased exposed connections.

The Alaska Land Mobile Radio (ALMR) system is a joint Department of Defense and State of Alaska system. Therefore, the system maintains a strong federally approved cybersecurity aspect. All equipment, software, and applications must meet the Federal Risk and Authorization Management Program (FedRamp) approval. FedRamp provides a standardized approach to security assessments and dictates what ALMR can provide to all of the system users. FedRamp approval is a long and drawn-out process that can be frustrating for individuals who are waiting to use certain radio software such as SmartConnect, push to talk location, or LTE sim cards.

The ALMR team strives to keep the system as secure as possible from cyber-attacks by routinely updating security patches and using a strenuous acceptance test for all radios.

(Article prepared by Paul Fussey with excerpts from the PSTA report May 2024)

Steps to Properly Remove Radios from ALMR

As all ALMR members work to replace their aging FDMA radios to TDMA compliant units, several steps must be undertaken, and policies and procedures must be followed to ensure the safety and security of the system.

The first step when you want to remove radios from the ALMR system is to fill out a Subscriber Request Form, which can be found on the ALMR website as Form 4 in the membership forms page. This form can be either emailed to ALMR-Helpdesk@beringstraits.com or faxed to (907) 269-6797.

After the radios have been deleted (removed from the system), the form will be returned to you as proof the radios will no longer affiliate with the ALMR system. This does not end the process but merely moves the responsibilities from the ALMR Help Desk to the owning agency.

Under the ALMR *Information Systems Clearing and Sanitization Procedure 200-4,* all ALMR system documents, equipment, and machine-readable media must be properly cleared, sanitized, and decommissioned, when appropriate.

When dealing with subscriber units (radios), all pre-existing cryptographic keys or configurations shall be cleared, or zeroed out, in a manner which prohibits the radio from having access to the ALMR system voice network. It is the responsibility of each agency to clear cryptographic keys and configurations before a subscriber unit is sent for maintenance or decommissioned.

Additionally, every ALMR key variable loader (KVL), shall be closely monitored and audited for use. With the most valuable function of the KVL being the algorithm in each device and the only known way to ensure the algorithm cannot be compromised is to physically destroy it.

Completely deleting an obsolete ALMR radio or console is the only way we can protection the security of the system.

(Article prepared by Paul Fussey with excerpts from the ALMR website and Information Systems Clearing and Sanitization Procedure 200-4, October 10, 2023)

G4 Geomagnetic Storm

On May 10 - 11, what the National Oceanic and Atmospheric Administration (NOAA) called the most extreme geomagnetic storm since 2003 struck the earth, especially Alaska.

A sufficiently intense geomagnetic storm could push satellites out of orbit, short out submarine cables, and cause massive blackouts from collapsed power grids. Of note, a 2003 geomagnetic storm took out power in Sweden and damaged power transformers in South Africa.

Due to these dangers, the Alaska NOAA office sent out warnings of possible widespread voltage control problems and the possibility that some protective systems may mistakenly trip out key assets from the power grid. Induced pipeline currents may intensify. In space, some systems may experience surface charging and increased drag on low earth satellites, and tracking orientation problems may occur and satellite navigation (GPS) may be degraded or inoperable for hours.

The OMO/SMO offices took these threats to ALMR seriously and worked on contingency plans in case radio transmissions became sporadic or blocked out due to the storm and how we would let the system users know, if we lost cell service and the internet connection. Thankfully these plans did not have to be activated and the ALMR system and State microwave backhaul were not affected by the historic storm.

While big, this storm is nowhere close to the level of the 1859 and 1921 storms and is not the extent of what we can expect to face in the coming decades as the sun heads towards the peak of its 11-year activity cycle in 2025.

Diligent preplanning and monitoring of the SWPC by ALMR and State APSCS members are key to protecting the system from outages during the next geometric storm.

(Article prepared by Paul Fussey with excerpts from the NOAA Space Weather Prediction Center (SWPC) website May 10, 2024)

Meet the New Document Specialist

Hello everyone, my name is Mary Burnham. I moved to Alaska from Vermont in 2012 looking for new adventures. I look forward to my future working with this great team of individuals.

My newest adventure was moving from Fairbanks to Anchorage on April 15 to start working for Wostmann & Associates as the new ALMR Document Specialist. I am very thankful that I have been able to learn about the position from the amazing Sherry Shafer.

Some previous positions I have held in the administrative professional field have been as an University of Alaska, Governance Support Assistant, and a Community Services Manager for North Haven Communities.

North American Land Mobile Radio Market

The North America land mobile radio (LMR) market is projected to grow from 16,023.77 million USD in 2023 to 28,468.20 million by 2032.

The LMR market is experiencing significant growth driven by the increasing demand for reliable, real-time communication in public safety, security, and utility sectors. The market is further propelled by technological advancements in digital radio systems, which offer enhanced audio quality, greater data capabilities, and improved coverage. Additionally, the integration of long-term evolution (LTE) networks with traditional LMR systems is emerging as a key trend, facilitating broader communication solutions that meet the critical needs of emergency services. This trend towards convergence and enhanced interoperability is setting the stage for the next evolution in communication technologies across the region.

Industries such as public safety, utilities, transportation, and construction rely heavily on robust and secure communication systems, especially in emergency situations or natural disasters. For instance, during the 2019 California wildfires, LMR systems were instrumental in coordinating the response efforts of over 5,000 firefighters across multiple agencies. These systems enabled the transmission of critical information, such as evacuation orders and resource deployment, with a reliability rate of 99.7 percent. In contrast, cellular networks experience a 70 percent failure rate in the same conditions. Similarly, in the transportation sector, LMR systems are used to manage over 100,000 miles of railway tracks in India, ensuring the safety of approximately 23 million passengers daily. The robustness of LMR technology allows for a communication uptime of 99.9 percent, even during extreme weather events like cyclones or floods. In the utilities sector, LMR systems support over 300,000 miles of electric power lines in the United States, providing essential communication for maintenance and emergency repair crews. For instance, during the 2020 Texas power crisis, LMR systems facilitated the coordination of power restoration efforts for nearly five million affected households.

Amidst escalating threats of terrorism and crime, the demand for secure communication systems has intensified. LMR systems are highly favored in security-sensitive environments due to their operation on dedicated frequencies, which are challenging for unauthorized users to access. For example, during emergency responses, LMR systems have been shown to increase operational efficiency by up to 30 percent, ensuring that teams can coordinate effectively in real time. During a recent national security event, LMR systems facilitated seamless communication among law enforcement agencies, intelligence services, and emergency responders. The secure channels prevented any unauthorized access to critical information.

Integration of LMR systems with advanced technologies like GPS and location tracking software has enhanced their utility, enabling better coordination and faster response times during emergencies. LMR systems can be as high as AES-256 encryption, making it nearly impossible for unauthorized interception. This high level of security ensures that critical communications remain confidential and accessible only to intended users, thereby bolstering the safety and efficiency of operations in crucial sectors.

The North America LMR market faces significant competition from cellular technologies, which are increasingly appealing due to their expansive coverage, affordability, and advanced features like push-to talk (PTT). These cellular networks often come with low upfront costs compared to traditional LMR systems, making them a more attractive option for users seeking effective communication solutions without substantial investments. Moreover, the high costs associated with establishing and maintaining LMR infrastructures, including the necessary towers and repeaters, pose additional financial challenges. These costs can be particularly prohibitive for smaller organizations or those operating in remote areas, where funding and resources are typically more constrained.

Another critical challenge in the market is the limited and costly availability of radio spectrum necessary for LMR systems. This limitation can hinder growth and innovation within the LMR market, as access to adequate spectrum is crucial for the operation and expansion of these systems. Additionally, integrating LMR systems with existing communication networks and newer technologies presents its own set of complexities and expenses. These integration challenges can deter potential new users, especially those who find the integration process too daunting or expensive to justify the benefits of LMR systems.

The United States accounts for the largest market share of approximately 80 percent in the North American LMR market. The country's vast geographical expanse, coupled with the emphasis on advanced communication systems for public safety agencies and critical infrastructure sectors, has fueled the demand for LMR solutions. Major metropolitan areas such as New York, Los Angeles, and Chicago, as well as rural regions, have witnessed significant adaptation of LMR systems to ensure seamless communications.

Canada holds a market share of around 15 percent in the North American LMR market. The country's focus on modernizing public safety communication networks, as well as the growth of industries such as mining, oil and gas, and transportation, has driven the demand for reliable LMR solutions. Major cities like Toronto, Vancouver, and Calgary have been at the forefront of adopting advanced LMR systems to support critical operations and ensure public safety.

The continued growth in LMR systems due to expanding features, reliability, and interoperability are leading reasons North America is expecting more future growth.

(Article prepared by Paul Fussey with excerpts from the Credence Research, North America Land Mobile Radio Market summary published May 30, 2024)

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

CJIS-Mandated Vulnerability-Management Deadline

Last December, the FBI's Criminal Justice Information Services (CJIS) division mandated that law-enforcement (LE) organizations wanting to access its databases must have a cybersecurity vulnerability-management program in place by October of this year.

CJIS can ill afford to have its systems/databases compromised by cyberattacks and must ensure organizations accessing those systems/databases have adequate cybersecurity protections in place as any malware infiltrating an LE organization's networks or systems could be transferred unwittingly to CJIS's.

Such an event would be disastrous, as LE organizations nationwide rely on the ability to query the CJIS databases for criminal histories, fingerprints and other biometric information, warrants issued, firearm transactions, and registered sex offenders.

CJIS plans to start auditing organizations in October. At this point, it is unclear what sanctions it will impose if an organization has not complied with the mandate. Equally unclear is the definition of what will constitute compliance. However, it is reasonable to think CJIS will deny access to its systems/databases to any organization that hasn't passed muster.

A robust vulnerability-management program is designed to identify, evaluate, and mitigate weaknesses in information systems and associated controls. This involves regular, comprehensive scanning of systems for vulnerabilities, prioritizing them based on potential impact and likelihood of exploitation, and incorporating automated tools and expert analysis to ensure timely detection of new risks. Finally, an effective vulnerability-management program also entails a well-defined process for patch management and implementation of appropriate security measures to address identified risks.

(Article excerpts from Mission Critical Partners newsletter, Jason Franks, May 8, 2024)

Help Desk (In the Anchorage Bowl): 907-334-2567

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

Fax: 907-269-6797

Email: almr-helpdesk@beringstraits.com

Website: http://www.alaskalandmobileradio.org

Follow us on Twitter: @ALMR_SOA

Remote Security Update Service (RSUS)

The ALMR remote security update was successfully completed on the first of June. This update is a three-day process and includes the SMO and OMO, Motorola, and all dispatch centers on the ALMR system. This update is conducted multiple times a year to protect the cybersecurity of the system and to make sure it is running at peak performance.