Link Layer Authentication and Link Layer Encryption: Are You Really Secure?

The Need for Radio Authentication (Are You Really Secure?)

In August 2018, the Stark County, Ohio, Sheriff's Office, and Canton, Ohio, Police Department conducted a joint investigation into stolen radio identifications (ID) on the trunked Ohio Multi-Agency Radio Communications System (MARCS) used by numerous public safety agencies in Ohio. Authorities were notified of suspicious activity, which led investigators to execute seven search warrants in the Canton area in connection with stolen radio IDs. These stolen IDs were used to illegally program additional radios to access and operate on the public safety system as legitimate users. This allowed the criminal actors to eavesdrop[1] on police activities and alter their activities to avoid apprehension, causing potential impacts to officer safety and mission execution. **Had Link Layer Authentication (LLA) been available on the MARCS system, these duplicate radios would not have been able to register and operate on the system.**

Seized radios and laptops were analyzed by program engineers from MARCS and the manufacturer, and they discovered 44 illegal and/or hacked copies of programming software for a variety of radio device models. Additionally, investigators found several copies of a Russian system key generator tool (and a significant amount of system keys) and a vast number of radios with unauthorized programming and transmitting capabilities. The search warrants led to the investigation of nearly a dozen individuals. One suspect was convicted and served 48 months in prison.

Purpose/Executive Summary

Are you really secure when using your land mobile radio? As the opening use case above shows, most Project 25 (P25) radio systems come with built-in safeguards, but the availability of software key generators and other attack vectors used by threat actors means that new P25 features are needed to maintain P25 communications security. Over the past few years, Link Layer Security (LLS) features such as Link Layer Authentication (LLA) and Link Layer Encryption (LLE) have received increased attention from manufacturers and users looking to improve communications security. This paper explains these features and their impact on secure public safety communications.

While both LLA and LLE sound similar and improve P25 security, they serve different purposes and are in different stages of development and adoption. **Figure 1** summarizes the differences between LLA and LLE. In short, LLA uses the air interface link layer (i.e., control channel messages) to authenticate users on trunked systems, and LLE will use encryption to protect currently unencrypted air-interface "metadata[2]" found on both conventional and trunked systems.

---

[1] It should be noted that while LLA addresses uses cases where threat actors directly access trunked talk groups using cloned or spoofed radios (such as in this case study), it does not prevent monitoring of over-the-air P25 non-encrypted channels. LLA is a tool in the toolbox for P25 system security and should be used in conjunction with voice/data encryption and strong security policies, procedures, and governance for maximum impact.

[2] Metadata is a non-P25 term used to broadly describe addressing information, IDs and other data embedded in P25 messages.

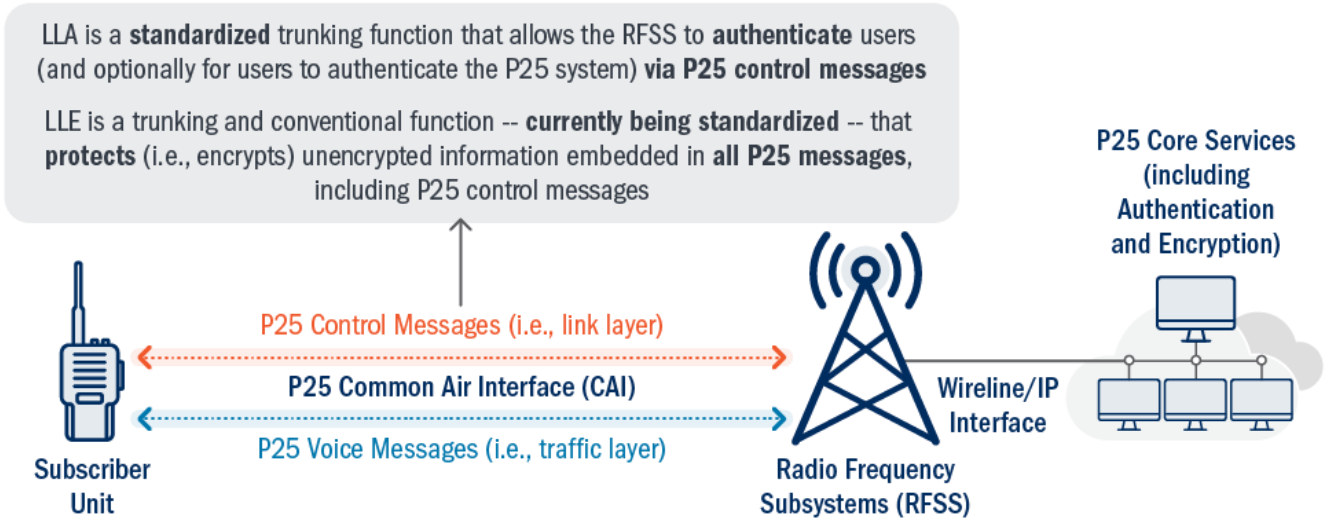

Figure 1. LLA and LLE Overview

First included in the P25 Standards in 2005, LLA is available from most (if not all) radio manufacturers and some infrastructure manufacturers. However, this function has seen limited adoption to date. LLE, on the other hand, is still under standards development and not available on any P25 systems today.

What is LLA?

Initially published as a P25 standard in 2005 and revised in 2011, LLA was introduced to minimize known vulnerabilities of unauthorized subscriber units (SU) registering with P25 trunked systems. As the name indicates, the function uses the link layer between the SU and the P25 system infrastructure to authenticate users:

- Link layer: The control plane/call setup functions that establish links between SUs and the radio system and enables voice and supplementary data services. This is achieved with control channel messages in trunked systems.
- Authentication: The process of verifying the claimed identity of a session requestor. [National Institute of Standards and Technology [NIST] definition[3]]

Because the authentication messages are sent via trunked control channel messages, this feature is available only on trunked P25 systems. When implemented and enabled, LLA ensures that only authorized radios with the appropriate radio unit identification (ID) and matching authentication keys can register on the P25 system.

The authentication service is applicable to frequency division multiple access (FDMA) (Phase 1) and time division multiple access (TDMA) (Phase 2) P25 trunked systems. LLA comes in two forms: unit authentication where the P25 infrastructure authenticates the registering SU, and an optional mutual authentication[4] where both the SU and P25 infrastructure authenticate each other.

[3] NIST Glossary Link: https://csrc.nist.gov/glossary/term/authentication
[4] Mutual authentication is an optional feature included in the P25 standards. To date, manufacturers and users have not prioritized nor implemented this function.

Why is LLA important?

LLA gives system administrators and planners a useful tool for combating unauthorized access to their P25 systems, which can occur if a threat actor gains access to a cloned or spoofed subscriber unit ID (SUID). For decades, public safety systems prevented unauthorized access by restricting access to radio programming equipment and requiring a "system key" for radio programming. These system keys can be hardware based (more secure) or take the form of a software file (less secure). With the increased use of software keys and greater access to pirated programming software designed to replicate system key files, savvy adversaries can spoof a valid radio ID and/or load compromised encryption keys[5] to listen to radio communications. As the capabilities (and tools) to steal or disrupt public safety communications become easier to acquire, additional security measures such as LLA offer another barrier against unauthorized access to public safety communications systems.

Public safety system operators and radios users are becoming more aware of the vulnerabilities that can be exploited with unauthorized radios. Despite programming and system-level safeguards already in place, illegitimate users present a clear hazard to public safety communications. The most harmful of these may be the use of a cloned radio with a duplicate system key that can be used to access a P25 system to monitor, steal, spoof/impersonate, alter, or repeat public safety communications.

How Does LLA Work?

Authentication services are handled by an authentication facility. Depending on the system manufacturer's product offering, the authentication facility could be an on-premises server or an application service running on an existing system infrastructure device.

The P25 radio system initiates the authentication process as the SU registers with the system. This is done by sending an authentication challenge to the subscriber radio over the air interface. The SU returns a response to this challenge, which requires knowledge of a unique advanced encryption standard (AES) 128-bit authentication key that is programmed when the SU is initially provisioned. The radio system then compares the subscriber radio's response. 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.

[5] P25 system-level security features (i.e., LLA and LLE) and voice traffic security features (i.e., voice enryption) are distinct functions and not directly dependent on each other. However, all security features contribute to an in-depth defense strategy that improves the system's overall security posture and reduces available attack vectors.

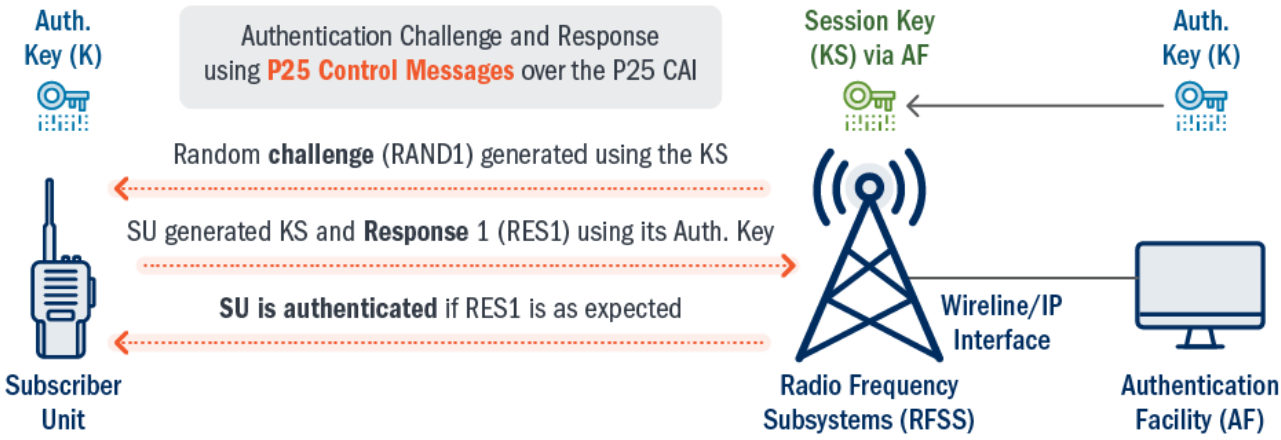

Figure 2. Link Layer Authentication Overview

Mutual authentication is optionally supported where the SU authenticates the radio system, which minimizes opportunities for rogue SU's to imitate a valid radio system. While authentication is usually carried out during registration, the P25 standard also allows for ad hoc/on-demand authentication as needed. As illustrated in **Figure 2**, the authentication key is the primary mechanism for ensuring a user (i.e., SU) is authorized to access the system. Each SUID is linked to a unique authentication key – typically generated by a Key Fill Device (KFD)/Key Variable Loader (KVL)[6] – known only to the SU and the authentication facility. The cryptographic challenge and response use a "session key" generated from the authentication key but does not require the actual authentication key to be shared with the P25 infrastructure or any other endpoints, thus keeping it secure.

LINK LAYER AUTHENTICATION GIVES SYSTEM ADMINISTRATORS AND PLANNERS A USEFUL TOOL FOR COMBATING UNAUTHORIZED ACCESS TO THEIR P25 SYSTEMS.

LLA is a feature that I was adamant about implementing in our new P25 trunked phase 2 radio system (PA-STARNet). It has proven to be an enhanced security feature and an asset on the system.

Hermina (Nina) Koshinski, Pennsylvania State Police

What are the current challenges with LLA?

As with many P25 Standards, optionality and differences in implementation can lead to operational challenges. Currently, many manufacturers are offering LLA to further secure the P25 trunked system environment from criminal actors compromising or eavesdropping on encrypted transmissions. LLA has not seen widespread acceptance or use to date. Many owner/operators do not want or are unable to invest in the additional cost and ongoing maintenance of infrastructure, updates, or additional features for SUs to support LLA.

A short list of common challenges include:

- Lack of adoption/use

[6] Although both can be managed using KFDs (KVLs), authentications keys are unrelated to voice encryption keys.

- Interoperability across some disparate manufacturers
- Challenges in setting up authentication across large scale multi-radio frequency subsystems (RFSS) network environments
- Challenges of use in inter-RF subsystem interface (ISSI) environments
- Additional key management operations needed for LLA features
- Older SUs may not support the LLA feature set and may require replacement or software upgrades

Feedback from public safety members introducing LLA indicates significant complexities in implementation and management of LLA and challenges using LLA in multi-RFSS environments of the same manufacturer. Challenges include, but are not limited to the following:

- LLA in single-manufacturer environments can be challenging due to different system settings and the need to install and configure authentication servers on all connected systems
- LLA in disparate manufacturer environments is operationally challenging as an SU authenticated on one manufacturer's system will need to be reauthenticated upon joining a disparate system. Sharing of the authentication information from the authentication facility as well as the status of authenticated SUs does not appear to work seamlessly across ISSI connections

What is Link Layer Encryption (LLE)?

LLE, once standardized and implemented, is a feature that encrypts air interface messages on both trunked and conventional P25 systems. These messages contain important identity and signaling information related to user IDs, talkgroups, and supplementary data services.

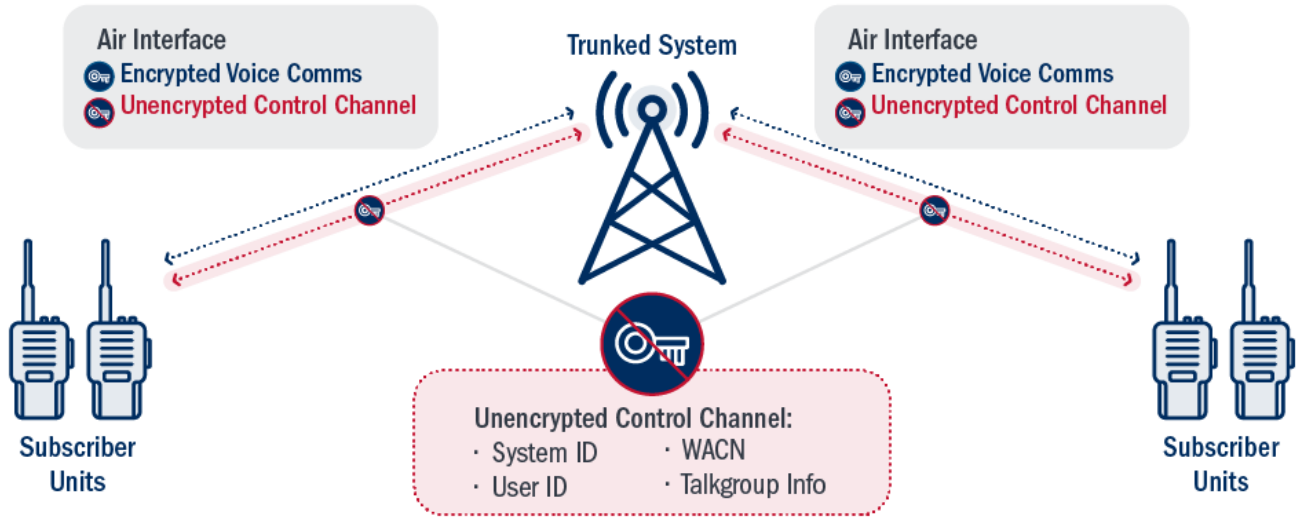

Figure 3. Unencrypted Control Channel Overview

Figure 3 illustrates the currently unencrypted control channel and control messages that could be protected with the implementation of LLE. Beyond control messages on the trunked control channel, conventional channels also contain unencrypted headers and addressing information. Once standardized and implemented, LLE would serve as a solution for securing air interface metadata across all control, voice, and data channels.

Why is LLE needed?

Without LLE, the voice traffic can still be encrypted by the P25 block encryption protocol (if the talkgroup or unit to unit call is encrypted); however, the link layer information will remain unencrypted. This means that adversaries with the right tools can intercept P25 communications and discover information about public safety agencies and possibly individual users. This information can also be used to spoof calls, intercept messages, clone radios, and conduct other activities that undermine the integrity and confidentiality of P25 communications. **Figure 4** shows the types of channels and modes that could benefit from the development and implementation of LLE.

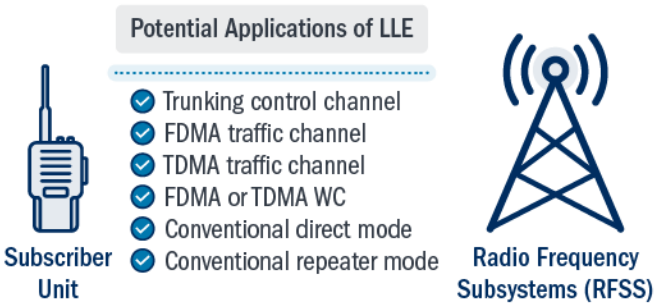

Figure 4. Conceptual Applications of LLE

> *With a $32 Software Defined Radio (SDR) and free software anyone can listen to P25 trunked control channels and log/record unprotected signaling. The same SDRs can receive and play unencrypted P25 voice, whether from a P25 conventional or trunked channel.*
>
> **Alan Massie, Federal Bureau of Investigation**

What is Next for LLA and LLE?

The definition of an LLE Security Service is in progress. This work is occurring in the APCO P25 Interface Committee (APIC) Encryption Task Group (ETG) and is expected to impact several published Telecommunications Industry Association (TIA) P25 accredited technical standards. APIC ETG members include representatives from the TIA TR-8 Engineering Committee responsible for developing P25 Standards and the P25 Steering Committee, and they are charged with arriving at encryption related standards acceptable to both the user and the manufacturing communities. The overview of the new service is considered complete, along with the TDMA Air Interface material. Material covering Trunked Control Channel Key Management is in progress. Material covering FDMA Common Air Interface modifications and Key Fill Interface modifications are pending review. This is the first big new technology upgrade for improved security for all air interfaces within the P25 standards. It protects control channel messages and masks group and individual IDs.

The Key Fill Device (KFD) interface protocol is also being updated to account for LLA and future LLE key management.

> *The State of Connecticut is anticipating the adoption of LLA to enhance system security. While other system security methods can be bypassed or spoofed, LLA provides a layer of system protection that can't be exploited. The availability of the information sent as part of the P25 messages provides a great deal of intelligence about the users of the system, intelligence that can be used against those users. The adoption of LLE will eliminate this potential security vulnerability. System managers should be aware of these potential vulnerabilities and take precautions to protect their systems.*
>
> **Scott Wright, Connecticut Department of Emergency Services and Public Protection**

Resources/Links:

For additional/more in-depth information on LLA and LLE, please consult the following resources:

Project 25 Technology Interest Group (PTIG) White Paper on Authentication:

- P25_Authentication_LLA_for_PTIG_v6.pdf (project25.org)

P25 Standards Update and Future Projects March 2022:

- New P25 Products and Services for IWCE 2021 (project25.org)

P25 Standards Documents:

- TIA-102.AAAB, Security Services Overview
- TIA-102.AACE-A, Link Layer Authentication
- TIA-102.AABC-E, Trunking Control Channel Messages
- TIA-102.AACD, Key Fill Device (KFD) Interface Protocol