L3HARRIS
FAST. FORWARD.

Project 25 Encryption

Overview and Recommendations

L3Harris Technologies, Inc.

WHITE PAPER

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

Project 25 Encryption

Overview and Recommendations

INTRODUCTION

To ensure the safety of personnel and operations, public-safety officials are increasingly turning to encryption to prevent monitoring or radio communications. The proliferation of inexpensive digital scanners and smartphone apps has made it easy for anyone to listen to public-safety and other two-way communications. Most listeners are casual eavesdroppers, journalists, or radio enthusiasts, but others are criminals whose objective is to undermine the safety and security of law enforcement operations.

It can be a controversial subject. Some argue that allowing the public to monitor local public-safety communications is vital to maintain government transparency. Others point out that criminals sometimes monitor public-safety communications to escape pursuit. Private citizens listening to scanners have occasionally helped apprehend dangerous criminals, but some organized criminal gangs monitor public safety communications to avoid arrest or expose agents working undercover.

This paper discusses encryption, what it is, and what options are available, particularly for Project 25 (P25) land mobile radio (LMR) subscriber units and radio systems.

Figure 1: Example of mobile applications and scanners used by citizens

WHAT IT IS

Encryption

Encryption is the process of applying a mathematical transformation to a digital information source (plaintext) to render the information unintelligible (ciphertext). Decryption is the reverse process of transforming ciphertext to make the data intelligible again. Modern encryption methods require one or more encryption keys to encrypt data at the source and decrypt the information at the destination. An encryption key is a random numerical code of a certain length (specified in bits). Most common LMR encryption methods use symmetric cryptography, where source and destination use the same key.

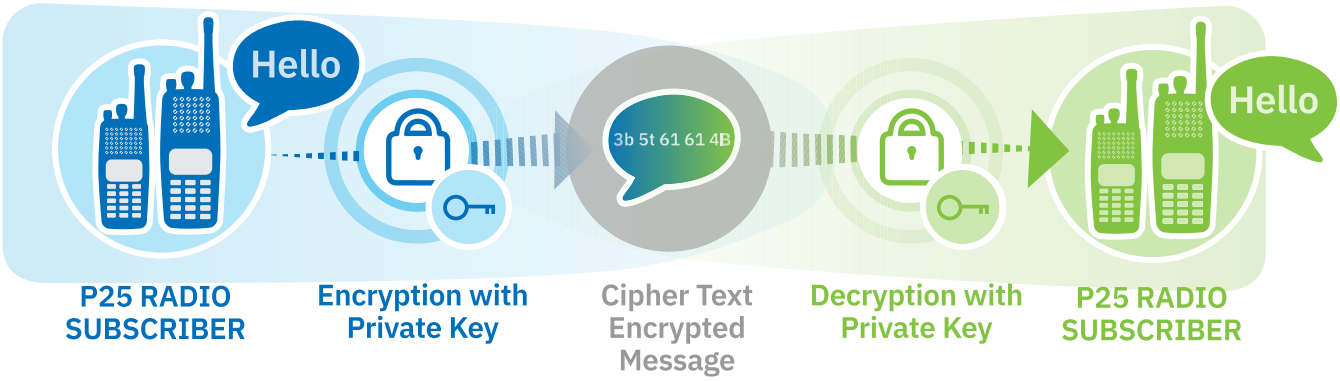

Figure 2: AES-256 encryption example

Encryption Types

The National Security Agency (NSA) categorizes four types of cryptographic products:[1]

- **Type 1:** Cryptographic equipment, assembly, or component classified or certified by NSA for encrypting and decrypting classified and sensitive national security information when appropriately keyed. Developed using established NSA business processes and having NSA-approved algorithms. Used to protect systems requiring the most stringent protection mechanisms.
- **Type 2:** Cryptographic equipment, assembly, or component certified by NSA for encrypting and decrypting sensitive national security information when appropriately keyed. Developed using established NSA business processes and containing NSA approved algorithms. Used to protect systems requiring protection mechanisms exceeding best commercial practices including methods used to protect unclassified national security information.

[1] Committee on National Security Systems Instruction No. 4009 (CNSSI 4009), *National Information Assurance Glossary*, April 26, 2010.

- **Type 3:** Unclassified cryptographic equipment, assembly, or component used, when appropriately keyed, for encrypting or decrypting unclassified sensitive U.S. Government or commercial information and to protect systems requiring protection mechanisms consistent with standard commercial practices. Developed using established commercial standards and containing NIST-approved cryptographic algorithms/modules or successfully evaluated by the National Information Assurance Partnership (NIAP).
- **Type 4:** Unevaluated commercial cryptographic equipment, assemblies, or components that neither NSA nor NIST certifies for any Government usage. These products may contain proprietary vendor algorithms, algorithms registered by NIST and published in a FIPS (Federal Information Processing Standard). These products are typically delivered as part of commercial offerings and are commensurate with the vendor's commercial practices.

Type 1 and Type 2 encryption products are certified by the NSA and are not available outside national security communications systems. This document primarily discusses Type 3 and Type 4 encryption products available for LMR communications.

ENCRYPTION OPTIONS

Scrambling

Voice scrambling is not encryption. There is no "cryptographic transformation" but rather a signal modification so a standard FM receiver cannot understand it. A common method of scrambling is called "voice inversion scrambling." In this method, the analog audio signal is inverted so that low-frequency audio sounds high and high-frequency audio sounds low. The audio is unintelligible on a standard receiver but easily understood with a properly programmed audio processor. Several LMR vendors offer scrambling as a standard feature. Scrambling does little to prevent unauthorized and determined eavesdroppers from listening to radio communications. It does not protect sensitive communications.

RC4/ARC4/ADP/Encryption Lite

Motorola Advanced Data Privacy (ADP) and L3Harris Encryption Lite are implementations of a Type 4 public-domain encryption algorithm known as Alleged RC4 (ARC4), which is a version of a proprietary algorithm known as Rivest Cipher 4 (RC4). "Alleged" is in the name because the RC4 algorithm was never officially published, and the term "RC4" is trademarked.

ARC4, as implemented in LMR systems, uses a 40-bit key. It provides inexpensive, easily implemented, "quick and dirty" security to prevent casual eavesdropping on communications. However, weaknesses in the algorithm make it vulnerable to attack. ARC4 is not recommended for sensitive communications where operational security is a concern.

Data Encryption Standard

The Data Encryption Standard (DES) was developed in the 1970s and released as Federal Information Processing Standards (FIPS) Publication 46 in 1977. DES was the official Government Type 3 standard until the early 2000s for sensitive but unclassified (SBU) information. DES uses a 56-bit key, allowing for 7.2×10^{16} unique keys. By the late 1990s, increases in computing power allow a DES key to be broken in a relatively short period.

DES can be implemented in four different modes. P25 standards for DES use the output feedback (OFB) mode. The Advanced Encryption Standard (AES) eventually superseded DES, and the DES standard was withdrawn in 2005, meaning it is no longer allowed for the protection of federal information. It is still available and provides limited security against casual eavesdroppers.

Other Proprietary Algorithms

One vendor has developed several proprietary encryption algorithms (or proprietary implementations of DES), including Digital Voice Privacy (DVP), DES (or DES-CFB), DVP-XL, DES-XL, and Digital Voice International (DVI)-XL. The original DVP and DES algorithms, developed in the 1970's, used continuously variable slope delta (CVSD) modulation to convert an analog signal into a 12kbps digital bitstream, then apply an encryption algorithm to create ciphertext. The -XL versions offered synchronization improvements to avoid a loss of range associated with the original implementations. DVI-XL is a version of DVP-XL intended for the international market. DES-XL, DVP-XL, and DVI-XL are available for P25 systems, but they are not P25 standards.

These encryption algorithms are obsolete and are not recommended for the protection of sensitive communications.

Advanced Encryption Standard

Published in 2001 as FIPS PUB 197, AES was designed to replace DES and can be implemented with 128-, 192- or 256-bit keys. The sheer number of possible keys (1.158×10^{77} keys) makes a "brute-force attack" (an attempt to decrypt the message by trying all possible keys) impractical with current computer processing power.

AES-256 is the standard encryption for P25 voice communications and is the only approved encryption algorithm for federal SBU communications.

Public-safety officials have for many years expressed concern about the use of non-standard (non-AES) encryption in public-safety LMR systems. The concern is two-fold: Non-AES encryption provides users a false sense of security regarding their communications; and there may be a lack of communications interoperability between agencies when responding to a significant crisis.

In response to these concerns, in March 2017, the Department of Homeland Security (DHS) mandated that if P25 radio equipment includes a non-standard (non-AES) encryption, it must also have AES-256 encryption to be approved via the Department's Office of Interoperable Communications (OIC) P25 Compliance Assessment Program (CAP).[2]

[2] DHS OIC P25 Compliance Assessment Bulletin P25-CAB-ENC_REQ, ***Project 25 Compliance Assessment Program Encryption Requirements***, March 2017.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

The National Institute of Standards and Technology (NIST) is responsible for federal standards and guidelines on information security for non-national security systems. This includes setting the standards for and validating the proper implementation of cryptographic modules.

Cryptographic Module Validation Program (CMVP)

The NIST Cryptographic Module Validation Program (CMVP) established proper design and implementation of cryptographic modules to protect federal information systems. Validated modules receive a certificate. After five years, those certificates move to the "historical" list. These modules are not invalid, but they are not included in new federal procurements.[3]

FIPS 140-2

Since 2001, FIPS 140-2, *Security Requirements for Cryptographic Modules*, published by NIST, has been the standard for designing and implementing cryptographic modules.

Cryptographic Module Security Levels

FIPS 140-2 defines four security levels for cryptographic modules (not to be confused with the four types of encryption products defined by the NSA): [4]

- **Security Level 1:** Level 1 encryption modules use an approved security algorithm (e.g., AES, SHA-256). They provide no physical security (e.g., tamper evidence) mechanisms. According to FIPS 140-2, Level 1:

  > "...may be appropriate for some low-level security applications when other controls, such as physical security, network security, and administrative procedures are limited or nonexistent. The implementation of cryptographic software may be more cost-effective than corresponding hardware-based mechanisms, enabling organizations to select from alternative cryptographic solutions to meet lower-level security requirements." [5]

- **Security Level 2:** Level 2 adds the requirement for tamper-evident seals or coatings on the encryption module hardware. It also requires role-based user authentication.

- **Security Level 3:** In addition to the tamper evidence of Level 2, Level 3 requires that the module be able to detect tampering and prevent access to the cryptographic keys or "critical security parameters" (CSP's). Security Level 3 requires strong physical enclosures and methods to zeroize CSPs when tampering is detected. Level 3 also builds upon the role-based authentication of Level 2 to require identity authentication. Finally, it requires the entry of key material via a dedicated port or interface that is physically or logically separated from other ports or interfaces.

[3] https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules, accessed June 17, 2020.

[4] NIST FIPS 140-2, ***Security Requirements for Cryptographic Modules***, March 22, 2019.

[5] ***Ibid, p. 2.***

› **Security Level 4:** Level 4 is the highest level of security for a cryptographic module. Besides the physical security features to detect and defeat tampering in Level 3, it also protects from temperature and voltage fluctuations that may be used to compromise module security.

Table 1 summarizes the four security levels.

SECURITY REQUIREMENT	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
Approved encryption algorithm	√	√	√	√
Tamper evidence	X	√	√	√
Role-based user authentication	X	√	√	√
Tamper resistance	X	X	√	√
Identity-based user authentication	X	X	√	√
Dedicated physical and/or logical port or interface for entry of key material	X	X	√	√
Environmental protection	X	X	X	√

Table 1: FIPS 140 Security Levels

FIPS 140-3

In March 2019, NIST published FIPS 140-3, *Security Requirements for Cryptographic Modules*. FIPS 140-3 supersedes FIPS 140-2. One significant change to the standard is a reference to the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 19790:2012(E), *Information technology — Security techniques — Security requirements for cryptographic modules* and ISO/IEC 24759:2017(E), *Information technology — Security techniques — Test requirements for cryptographic modules.*

FIPS 140-2 will be gradually phased out. In September 2020, NIST began accepting applications for 140-3 validation. In September 2021, NIST stopped accepting new applications for 140-2 validations.[6] As of December 2021, no encryption modules have received FIPS 140-3 validation.

[6] https://csrc.nist.gov/Projects/fips-140-3-transition-effort, accessed December 21, 2021.

LIMITS OF P25 ENCRYPTION

Unencrypted Signaling

P25 FIPS-certified encryption provides for the secure transmission of voice packets. However, at this time, other parts of the P25 signaling protocol remain unencrypted, such as control channel messages and unit IDs. This may allow a sophisticated eavesdropper to gain intelligence based on traffic volume, active units, and talk groups. The P25 committees are working on standards for Link Layer Encryption, which would allow encryption of the associated signaling so that unit IDs and other data regarding encrypted communications would be protected from monitoring.

Proprietary Data Encryption

Whereas P25 contains standards for applying encryption to voice packets, there is no corresponding standard for the encryption of data packets. In light of this, major LMR vendors have developed proprietary encryption methods for mobile data. These methods use standard encryption algorithms but apply them in different ways to data packets. For this reason, the use of encryption on mobile data leads to incompatibilities between one vendor's infrastructure and another vendor's subscriber radios.

OVER-THE-AIR REKEYING

The proper management of encryption keys includes distributing, updating, and destroying keys. In the past, these elements of key management were time- and resource-intensive. Each radio had to connect manually to a key fill device (KFD) for insertion, change or deletion of keys. The logistics of scheduling personnel to turn radios in, making sure that all members of a crypto group have received the required keys, and orchestrating a key changeover made for a tremendous burden on administrative personnel.

A more efficient method to manage these functions is over-the-air rekeying (OTAR). OTAR sends keys and key-management messages securely over the radio channel from a central key management facility (KMF).

OTAR is a P25 standard, so radios and infrastructure from multiple vendors are compatible.

CONCLUSION

In conclusion, we offer the following practical considerations.

To Encrypt or Not to Encrypt

As the technological sophistication of criminals and foreign agents increases, encryption is an essential tool to maintain the operational security of sensitive communications. Each agency must decide when and how to deploy it, whether on all channels, including dispatch, or only on sensitive channels, like tactical or criminal investigations communications. Some agencies have deployed encryption on their radio channels but provide a delayed feed on the Internet. This way, the public can monitor communications, but not in real-time while an incident is in progress. Agencies must balance the public's desire for government transparency with a legitimate need to protect public-safety operations.

Use FIPS-approved Encryption Algorithms

DES, ARC4, and other proprietary encryption methods are helpful to prevent casual eavesdropping, but FIPS-approved encryption algorithms are essential for true information security. Today, for LMR communications, AES is the approved algorithm. In the future, as computing power increases and potential weaknesses to AES are discovered, other algorithms will be published by NIST and implemented by LMR vendors.

Certification Is Required

When implementing AES encryption, it is essential that the cryptographic module be validated (certified) by the CMVP. Without this certification, one cannot ensure that encryption has been properly implemented or communications adequately secured. Do not accept an unvalidated encryption module.

> "FIPS 140-2 precludes the use of unvalidated cryptography ***for the cryptographic protection*** of sensitive or valuable data within Federal systems. Unvalidated cryptography is viewed by NIST as providing ***no protection*** to the information or data—in effect the data would be considered unprotected plaintext. ***If the agency specifies that the information or data be cryptographically protected,*** then FIPS 140-2 is applicable. In essence, if cryptography is required, then it must be validated." [7]

Level 1 or Level 3

Several LMR vendors offer FIPS 140-2 Level 1-certified encryption modules. Only one vendor offers a Level 3-certified module.

Level 3 offers some advantages over Level 1: When a module is tampered with, Level 3-certified encryption prevents access to the encryption keys by deleting (zeroizing) the keys. It may prevent third parties from eavesdropping

[7] https://csrc.nist.gov/projects/cryptographic-module-validation-program, accessed June 12, 2020.

on encrypted communications from a lost or stolen radio. In addition, all aspects of manual or over-the-air key filling are encrypted, preventing anyone from manually copying the text of a key.

The most serious disadvantage to Level 3 mode is entering a password when the radio is powered on. Imagine a police officer during a life-threatening situation whose radio is powered off accidentally. To call for help, not only does he have to turn the radio back on, he must re-enter his password as well. Any delay in making that call may be the difference between life and death. To most public-safety users, this risk far outweighs the additional security provided by Level 3.

While Level 3-certified encryption modules may prevent eavesdropping on encrypted communications, P25 offers system administrators other ways to prevent eavesdropping via lost or stolen radios. Radio system administrators, through OTAR and other standard P25 messages, have the ability to zeroize keys and disable a radio, making it useless to the one who steals or finds it.

It is common for individuals in most areas of life to have a preferred vendor for specific products. Sometimes, purchasers for governmental agencies will use product differentiators, such as Level 3-certified encryption as a means to sole-source purchases to a single vendor. However, when competition is eliminated, a vendor can and will charge premium pricing for its products. This leads to higher costs for users, often for a feature that users do not use. Indeed, many agencies that demand Level 3-certified encryption do not use it because of the operational issues cited above.

OTAR Makes Encryption Manageable

Management of encryption keys and resources requires a significant investment of time and money. Decisions must be made to designate crypto officers, define crypto groups and users, and determine how frequently keys should be changed. OTAR is a valuable tool to manage encryption efficiently.

L3HARRIS
FAST. FORWARD.