Guidelines for Encryption in Land Mobile Radio Systems

February 8, 2016

NCSWIC

Federal Partnership for
FPIC
Interoperable Communications

SAFECOM

PREFACE

The state, local, and tribal public safety community requested guidelines providing clear and factual information regarding the use of encryption and its ability to protect mission critical communications and maintain interoperability among agencies at all levels of government. The importance of this request was elevated when non-standard and "weak" encryption solutions were introduced to a number of public safety agencies as they implemented Project 25 digital communications technology to support their mission critical voice and data communications needs. Although most felt these non-standard encryption protocols could not ensure the level of security necessary, the cost of these solutions was attractive and many were not aware of the actual lack of protection and the potential detrimental impacts on communications interoperability.

Although federal agencies have been required to protect Sensitive but Unclassified (SBU) information for several years, most public safety agencies felt the cost of implementing encryption could not be justified. However, these organizations' interest in encryption and information protection increased as the importance of protecting sensitive information became evident, coupled with the introduction and implementation of digital technology such as Project 25.

A significant number of public safety officials and system administrators recognized the need for encryption in specific applications. This group also recognized there was significant confusion and competing information regarding voice and data encryption in the Land Mobile Radio (LMR) environment. Many public safety communications officials and system managers, including representatives from federal agencies, strongly felt guidelines needed to be developed to provide factual and consistent information.

The initial request for such a document was introduced to the Federal Partnership for Interoperable Communications (FPIC) by several state and county public safety agencies. The FPIC Security Working Group agreed to develop a document to satisfy the demand to encourage consistency in deploying a common and consistent encryption methodology across federal, state, and local public safety communications platforms. A wide range of public safety information security and encryption experts at all levels of government also provided valuable input to develop this document, and their contributions ensured consistent content and efficacy. Although many individuals and organizations took part in the development of this document, the organizations listed in the Appendix were especially helpful in assuring the content is both timely and accurate.

Although this document was developed as a result of a joint, cooperative effort of public safety agency representatives, the group agreed to identify the FPIC as the common coordinating entity. The contributing representatives anticipate acceptance and release of this document by the appropriate authority within the SAFECOM and National Committee for Statewide Interoperability Coordinators (NCSWIC) as an informative guide that can be disseminated to all public safety user agencies and organizations as appropriate. This document is not intended to be a policy directive or procedure. It is important to note that there are significant governance, policy, and training implications that must be considered with the use of encryption. SAFECOM and NCSWIC also developed a comprehensive Governance Guide[1] for emergency communications issues that can assist in addressing these complex challenges through best practices and proven real-world solutions.

[1] http://www.dhs.gov/safecom/governance

1. EXECUTIVE SUMMARY

As a result of a number of security risk and vulnerability assessments, the public safety community has recognized the increasing effort to protect sensitive information transmitted over its wireless communications systems. Additionally, as the users continue to implement digital land mobile radio (LMR) technology, such as Project 25, they have realized the relative cost of employing encryption services to protect this information has decreased with digital technology. Most public safety system administrators and managers want to minimize the possibility of sensitive information being monitored with low-cost scanners, but are concerned with the cost of standards compliant encryption. The purpose of this document is to provide information that should be considered when evaluating encryption solutions.

The key to protecting sensitive operational or life safety radio transmissions is to deploy an encryption system with an algorithm that assures information is adequately protected from eavesdropping. A number of encryption algorithms exist that include encryption key lengths from 56 bits to 256 bits. These techniques are being used in LMR systems throughout the United States and the world, but all do not provide the protection needed to ensure information security.

Standards compliant algorithms, such as the Advanced Encryption Standard (AES), offer the greatest opportunity for achieving maximum interoperability while providing a high level of protection. The AES algorithm is specified in the National Institute of Standards and Technology (NIST) FIPS PUB-197[2]. Unlike proprietary or non- standard algorithms, AES is freely available to any manufacturer who wishes to use it. There are no intellectual property restrictions or royalty payments involved in its use. While key lengths of 128-bit and 192-bit are authorized for use, it is strongly recommended that the 256-bit key is utilized in public safety wireless systems in accordance with the published standard for Project 25 Block Encryption Protocol (TIA-102.AAAD-B).

NIST has concluded that a cryptographically strong algorithm with a key length of 128 bits or longer is the most effective way to protect sensitive information from compromise and has strongly recommended the use of the NIST certified AES as the only encryption technique for federal LMR systems. Federal departments and agencies require NIST-approved encryption for Sensitive but Unclassified (SBU) information and do not allow the use of proprietary encryption algorithms. The P25 Standard relies on AES 256-bit to ensure the best level of protection and interoperability.

2. BACKGROUND

As the public safety user community continues to implement digital technology to support mission-critical voice communications, they have recognized an increasing need to protect sensitive information transmitted over the air and within the network. As these users realize the cost delta for encryption is significantly reduced when implemented in a digital wireless communications network, such as Project 25, the interest in encryption has increased.

[2] http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

While any electronic communications system is vulnerable to exploitation by interception (eavesdropping), radio communications systems are one of the most vulnerable. Interception can occur anywhere in the radio coverage area, is difficult to detect (since no physical interconnection is required), and can be accomplished with equipment that is readily available or easily acquired.

The purpose of this document is to discuss methods that may be used to ensure the confidentiality of sensitive public safety LMR communications. These methods mainly involve the use of encryption. However, the use of encryption can adversely impact interoperability with other agencies if due consideration is not given. For example, ensuring that all agencies support the same cryptographic algorithms is the first step in protecting sensitive communications while still allowing for interoperability.

3. ENCRYPTION

Cryptography[3] can be used to provide several security services including: Confidentiality (the protection of message contents from disclosure); Authentication (the verification of the identity of message sender); and to ensure message Integrity (the message contents have not been modified). Encryption is commonly used to mitigate the threat of interception by providing the Confidentiality service.

Encryption, in simple terms, is the conversion of data into a form called cipher text that cannot be understood by unauthorized entities. Decryption is the process of converting encrypted data (cipher text) back into its original form.

Encryption and decryption require the selection and use of a common cryptographic algorithm. Examples of encryption algorithms include the Data Encryption Standard (DES), AES, Rivest, Shamir, Adelman (RSA), and various other algorithms. Encryption requires not only the use of an algorithm, but also an encryption key chosen by the message originator and a decryption key known to the message receiver. Algorithms that use the same key for encryption and decryption are known as symmetric key algorithms, and it is this type of algorithm that is used for the encryption of voice and data in LMR applications. The aforementioned DES and AES are symmetric key algorithms. When a symmetric key algorithm is used, the key used for both encryption and decryption must be protected from unauthorized disclosure.

A “cryptographically strong” encryption algorithm is one that is highly resistant to unauthorized decryption and cryptanalysis. For a cryptographically strong encryption algorithm, the “cryptographic strength” of an algorithm directly corresponds to its key length, or number of possible keys[4]. Roughly, this means that the plaintext that corresponds to encrypted data (cipher text) can only be determined by an adversary by trying each possible key until he finds the key used to encrypt the data (a process known as exhaustive key search), and the amount of time it takes to do this is significantly longer than the useful lifetime of the information transmitted by

[3] Although Cryptography is the proper term in most government environments, the term encryption is also commonly used by many users and manufacturers.

[4] An analogy to this is the size of passwords, where a 12-character password is inherently stronger than an 8-character password.

the plaintext.

For cryptographic algorithms, key length is typically specified in terms of the number of bits used. The encryption algorithm formerly used by the U.S. Government, DES, has a key length of 56-bits, which allows 2^{56} or approximately 10^{17} (100,000,000,000,000,000) unique keys. AES has a minimum key length of 128-bits and can use additional key lengths of 192-bits and 256-bits. This gives 3.4 x 10^{38} possible 128-bit keys; 6.2 x 10^{57} possible 192-bit keys; and 1.1 x 10^{77} possible 256-bit keys.

While the DES key length of 56-bits seems to allow an enormous number of keys, it has been shown to be subject to compromise through exhaustive key search using modern computer systems. More sophisticated cryptanalysis can further reduce the work factor of recovering a DES key to significantly less than 2^{56} operations. Most knowledgeable cryptographic experts currently recommend a ***minimum cryptographic strength*** of 112 to 128-bits for use in new systems. In fact, DES has already been withdrawn (de-certified) for use in U.S. Government applications. It should be noted that as key size is reduced below the recommended values, the vulnerability to exhaustive key search increases, especially as advances in computing speed and power occur. This is true regardless of the cryptographic algorithm used.

One encryption algorithm commonly accepted as “strong” is the NIST AES[3] a publically specified algorithm selected in 2001 for U.S. Government use after a multi-year open selection process. AES has been scrutinized by leading cryptographers and security organizations worldwide. Few weaknesses (i.e., mathematical shortcuts that can be used to circumvent an exhaustive key search) have been identified. NIST adopted AES as an approved standard for the protection of U.S. Government sensitive information. In addition, the National Security Agency (NSA) allows its use for the protection for certain levels of classified information.[5]

One might contrast this open public process with a proprietary developed algorithm. In most cases, proprietary algorithms are neither published nor subject to public scrutiny prior to deployment. One must take the word of the developer that a particular algorithm is strong and capable of providing security. An example of a security implementation that was not publicly reviewed is Wired Equivalent Privacy (WEP) that was used for 802.11 Wi-Fi networks. WEP is the implementation of a communication protocol that uses an encryption algorithm RC4[6] as part of the protocol. It was developed using an open-standard process in the IEEE. However, a public review identified a number of significant weaknesses in the algorithm and its implementation that allowed it to be broken with little effort.

Data encryption algorithms may prevent unauthorized disclosure of potentially sensitive information, but mismanagement of cryptographic material can lead to a possible disclosure or unauthorized access. Official procedures for handling cryptographic material must minimize the risk of unauthorized access. The strength of an encryption method can be compromised by poor

[5] http://www.cnss.gov/Assets/pdf/CNSSP_No%2015_minorUpdate1_Oct12012.pdf

[6] RC4 is a stream cipher. It is initialized with a variable length key, typically between 40 and 256 bits, using the *key-scheduling* algorithm (KSA). The key stream of bits is generated using a pseudo-random generation algorithm (PRGA).

management of the keys. Therefore, securing access to keys is as important as the encryption method itself.

4. ALGORITHM CHOICE

Products containing cryptographic algorithms receive “type” designations based on: the conditions under which they are certified for use by public safety agencies; the authority who approved the algorithm; and whether the algorithm is vendor proprietary. In general, there are four designations for land-mobile radios: Type I, Type II, Type III, and Type IV. Type III is the predominant designation for public safety LMR and is approved by NIST for the protection of SBU information.

There are a number of choices for encryption algorithms for use in public safety land mobile radios, including AES, Triple-DES, DES and proprietary algorithms. AES is approved by NIST for protecting SBU information. Some advantages and disadvantages of each algorithm are given below:

AES – AES was evaluated for several years prior to being selected as an accredited technical standard. It provides key lengths of 128, 192 or 256-bits, capable of providing protection from exhaustive key search for 20 to 30 years. Although agencies may choose to use any of the three key lengths, the Project 25 Statement of Requirements specifies 256-bit AES as the preferred encryption algorithm for new Project 25 systems. Consequently, the U.S. Government recommends that agencies adopt this standard. The current SAFECOM Grant Guidance requires NIST Compliant AES be implemented in Project 25 public systems when encryption is required and federal grant funds are used.

DES – DES was developed in the mid-1970s to protect U.S. Government communications. Given advances in computing speed and power that have occurred in the last 30 years, DES’ 56-bit key size no longer provides adequate protection. In 1988 an exhaustive key search using dedicated equipment determined the key in 56 hours. Since then this time has been reduced. DES should not be used in new systems and only used when backwards interoperability with systems that do not support newer algorithms is required.

While all new systems should be procured with the AES encryption algorithm, system administrators should exercise caution and identify existing systems incapable of supporting AES encryption. The security of these systems must be considered when surrounding systems are being upgraded or replaced.

Triple-DES (3 DES) – 3 DES encrypts data three times using the DES "engine". Two-key and three-key Triple DES are assessed at a security strength of 80 bits and 112 bits, respectively. The algorithm uses a DES encryption and decryption engine to encrypt, decrypt, and then encrypt again. It can use two DES keys, with the first and last encryption using the same key (two key triple DES), or three DES keys, with each encryption and decryption using a unique key (three key triple DES). It was mainly used as an interim algorithm while the AES was being developed. While currently capable of providing adequate security, its use is not recommended for new applications. Triple-DES also suffers from some performance issues since it must encrypt data three times. Triple-DES is not offered in any current public safety land mobile radios.

Proprietary/Unapproved algorithms – Proprietary and unapproved algorithms may not provide adequate protection regardless of advertised key length. The risk is that the algorithm is less cryptologically secure than the developer claims. Proprietary solutions can also adversely affect interoperability because an agency that uses proprietary encryption can only interoperate in an encrypted mode with agencies that use the same proprietary encryption algorithm. NIST advises against the use of proprietary and unapproved algorithms for U.S. Government systems. Consequently, these algorithms cannot be used by federal departments and agencies, who are prohibited from using encryption algorithms that do not meet NIST standards for the protection of SBU information. Most departments and agencies mandate the use of AES 256 bit encryption in their LMR Systems. None authorize the use of proprietary algorithms**.**

Table 1 – Algorithm Reference Matrix

Algorithm	Key Length (bits)	Recommended Use
AES	128, 196, 256	Unclassified but sensitive, all secure communications
Triple DES	112, 168	Not currently offered in LMR radios supporting public-safety communications
DES	56	Legacy secure communications, interoperability mode only
Non-standard	Varies	Not recommended for secure communications

5. CRYPTOGRAPHIC MODULE

The cryptographic algorithm is stored and executed in a cryptographic module, which stores and uses the key to allow for encryption and decryption of voice and data communications. A cryptographic module supporting secure voice and data communications within a LMR system must be significantly enhanced to protect the keying material housed within the module. Since protecting the key is vital to protecting the information, care must be taken to ensure the module is designed properly. NIST developed the FIPS140-2 standard to test and report the integrity of the module. Any radio that does not implement the algorithm on a FIPS 140-2 compliant module risks the integrity of the key for all users. Therefore, it is recommended that all interoperating in secure mode have encryption modules certified to FIPS 140-2.

6. INTEROPERABILITY ISSUES

Standard algorithms, such as the AES which is specified in NIST FIPS PUB-197, offer the greatest opportunity for achieving maximum interoperability. Unlike proprietary algorithms, AES is freely available to any manufacturer, has no intellectual property restrictions, and is royalty-free. While the AES document authorizes 128-bit and 192-bit key lengths, the Project 25 Block Encryption Protocol strongly recommends 256-bit key length for public safety.

Since federal users may have limited resources to evaluate encryption-based products, NIST standards offer guidance for manufacturers to ensure AES-encrypted products are adequately secure.

Today, all federal public safety agencies are transitioning to AES. Therefore, non-federal agencies seeking secure federal interoperability must also transition to AES.

Algorithm choice is one of many issues that must be addressed in order to achieve secure interoperability. A thorough discussion of all the issues is beyond the scope of this basic document, but some assurance comes from knowing that most standards-based encryption solutions take these additional considerations into account. This is particularly the case with the security standards developed for Project 25 interoperability.

7. SUMMARY

In light of the potential security risks and interoperability challenges associated with non-standard or proprietary encryption technology, AES-based solutions are highly recommended for users who require robust security and federal interoperability. Further, agencies should opt for cryptographic modules that have been validated according to the NIST cryptographic module validation program. The use of these modules ensures that AES and associated cryptographic functions are implemented correctly. A list of NIST validated modules is available at http://csrc.nist.gov/groups/STM/cmvp/validation.html.

References:

FIPS 140-2, *Security Requirements for Cryptographic Modules*, National Institute of Standards and Technology, May 2001 as annexed

FIPS 197, *Specification for the Advanced Encryption Standard (AES),* National Institute of Standards and Technology, Nov 2001

TIA-102.AAAD-B, *Project 25 Digital Land Mobile Radio Block Encryption Protocol,* Telecommunications Industry Association, December 2015

APPENDIX – REPORT CONTRIBUTORS

The following federal, state, and local public safety departments and agencies contributed to the creation and completion of this document. These contributions represent the combined opinions of recognized subject matter experts in the field of wireless encryption operations and technology.

- U.S. Department of Justice, Wireless Management Office
- Federal Bureau of Investigation, Operational Technology Division, Technical Programs Section, Radio Systems Development Unit
- U.S. Drug Enforcement Administration, Office of Investigative Technology
- National Institute of Standards and Technology, Information Technology Laboratory, Computer Security Division
- Wyoming Public Safety Communications Commission
- Connecticut Department of Emergency Services and Public Protection, Division of State Police
- Missouri Department of Public Safety, Missouri Interoperability Center
- U.S. Department of Homeland Security, Customs and Border Protection, National Law Enforcement Communications Center
- U.S. Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations
- Treasury Inspector General for Tax Administration, Technical and Firearms Division
- Fairfax County (Virginia) Office of Information Technology, Radio Services Division
- Orange County (California) Sheriff’s Department, Radio-Microwave Unit
- U.S. Marine Corps, MCAS Yuma, Communications Data Electronics Department
- Loudon County (Virginia) Department of Information Technology, Public Safety Division
- Metropolitan Washington Airports Authority, Wireless and Radio Systems Department
- Montgomery County (Maryland) Police Department Montana Department of

Administration, Public Safety Services Bureau

- Montana Department of Justice, Highway Patrol Division
- U.S. Coast Guard – Headquarters
- SAFECOM – NCSWIC Technology Policy Committee

Federal Partnership for

FPIC

Interoperable Communications

NCSWIC

SAFECOM