SAFECOM Federal Partnership for FPIC Interoperable Communications NCSWIC

Guidelines for Encryption in Land Mobile Radio Systems

Determining what Encryption Method to use for Public Safety Radios

As a result of a growing number of incidents involving the vulnerability and subsequent compromise of sensitive information, the public safety community recognizes the importance of protecting information transmitted over its wireless communications systems. The implementation of digital land mobile radio (LMR) technology, such as Project 25, increases the awareness that encryption provides required protection more readily than was available for analog systems.

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

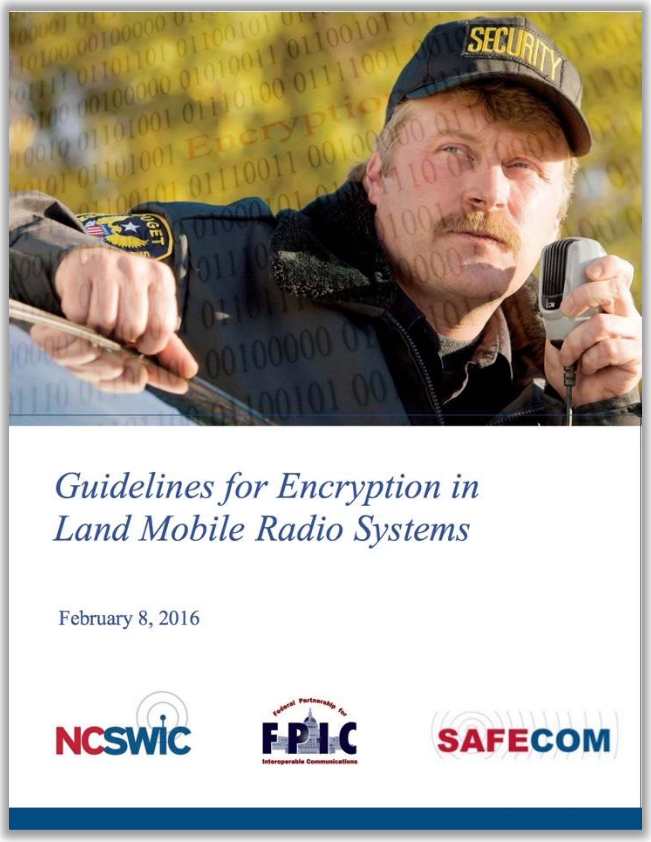
Standards-compliant algorithms, such as the Advanced Encryption Standard (AES), offer the greatest opportunity for achieving maximum interoperability while providing a high level of information security. The AES algorithm is specified in the National Institute of Standards and Technology (NIST) FIPS PUB-197[1]. 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 with 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).

THE REPORT

Most public safety system administrators and managers want to minimize the possibility of sensitive information being monitored by the use of low-cost scanners or other devices and are concerned with the added complexity and cost of standards-compliant encryption. Other documents, in a series of encryption-related reports published by SAFECOM/NCSWIC/FPIC, will outline these issues. The goal of this document is to provide information that should be considered when evaluating encryption solutions, especially what encryption techniques to consider and those to avoid.

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

The primary objective of this document is to discuss methods that may be used to ensure the privacy of sensitive public safety LMR communications. These methods mainly involve the use of a variety of encryption techniques. The report outlines what encryption algorithms are considered safe or “cryptographically strong” enough to be highly resistant to unauthorized decryption. For the protection of sensitive public safety information, the “strongest” algorithm available for LMR systems today is AES, with a 256-bit key length. In general, the “strength” of an algorithm directly corresponds to its key length, or the number of possible keys… the greater the number of keys, the less likely the key can be determined by an adversary.



Guidelines for Encryption in Land Mobile Radio Systems

February 8, 2016

NCSWIC FPIC SAFECOM

IMPLICATIONS FOR THE PUBLIC SAFETY COMMUNITY

Encryption provides the best way to protect critical information from compromise and disclosure, it can also complicate the implementation of interoperable land mobile radio systems. In order to be interoperable in an encrypted environment, LMR systems must use the same type of encryption and share the same key management parameters. Those that use non-standard encryption algorithms or techniques will not interoperate with systems that use P25 Standard encryption. Although DES and AES are P25 Standards compliant, they will not interoperate, so consideration should be given to which technique to implement.

SAFECOM, NCSWIC, and FPIC recommend that AES-256 encryption is the goal for all public safety agencies to ensure the greatest protection against potential compromise of sensitive information and the best chance to improve encrypted interoperability. The DHS Office of Emergency Communications, in its National Emergency Communications Plan (NECP) of 2008, detailed an initiative to “… *implement the Advanced Encryption Standard (AES) for Federal responders. A standard nationwide encryption method will diminish the interoperability challenges faced by Federal responders (who previously used different methods) and will provide guidance to local and State agencies when working with Federal agencies”* and…to establish “*AES as the uniform standard for State, local, and tribal emergency responders who decide to use encryption*”. Although the NECP has since been updated, the soundness of the initiative remains valid today and extends to all public safety agencies. Simply put, encryption for the Nation’s first responder communications systems assures the protection of sensitive information from unauthorized use.

This Fact Sheet is a brief summary of the SAFECOM/NCSWIC/FPIC encryption document entitled *Guidelines for Encryption in Land Mobile Radio Systems*, published on the DHS Technology Website at http://dhs.gov/Technology under “Encryption”.