



IN SHORT

NIJ

 TOWARD CRIMINAL JUSTICE SOLUTIONS

www.ojp.usdoj.gov/nij MAR. 07

NCJ 217103

Voice Encryption for Radios

Key Points

- Unencrypted public safety voice transmissions can be intercepted, abetting criminal activity, thwarting public safety efforts, and endangering the public and public safety personnel.
- Voice encryption helps ensure that voice transmissions can be accessed only by authorized personnel, thereby increasing the safety and efficiency of public safety personnel.
- Voice encryption adds complexity and cost to public safety voice networks.
- Effective management is essential to implementing an encrypted voice network successfully.

OVERVIEW

Public safety land mobile radio systems are vulnerable to eavesdropping and can easily be exploited by criminals. Readily available scanners and other devices can be used to receive voice signals from analog and digital public safety radio systems, including trunked radio systems. Lists of frequencies and channel assignments used in public safety jurisdictions are easily obtained from numerous print and online sources.

To ensure that sensitive information is shared only among authorized individuals or organizations, public safety operators need to ensure the confidentiality of sensitive radio traffic. This is typically accomplished through voice encryption.

THE ENCRYPTION PROCESS

Securing the message. A voice message is first digitized and then encrypted (or locked). The process requires the use of an algorithm and a unique cryptographic key, which are analogous to

a door lock and its key—although many houses may use the same brand of lock, how the lock is keyed makes it unique. The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are two well-known algorithms. Cryptographic keys are usually expressed in terms of number of bits. Typical key sizes are 56 bits for the DES, and 128 to 256 bits for the AES.

Transmitting the message. Once the voice message has been encrypted and transmitted, the receiver can only decrypt (or unlock) the message using the same algorithm and unique key as the transmitter. For security purposes, only the sender and the intended recipient(s) of the encrypted message should know the key. If members of a group need to communicate securely with each other, all radios belonging to the group must share the same key. When several radios share the same key, the group is known as a cryptonet. If a radio is used to participate in more than one cryptonet, it must hold a unique key for each cryptonet.

When it is necessary to communicate with persons who do not have access to the cryptonet, a gateway device is often employed.¹ Such devices can compromise communication security because the voice message has to be unlocked to pass through the gateway. Also, there is no assurance of the level of security of the system through which the voice message is passed.

ADVANTAGES OF VOICE ENCRYPTION

- Provides confidentiality for sensitive radio traffic.
- Prevents unauthorized parties from successfully monitoring radio traffic.
- Enhances personnel security.
- Provides some user authentication on radio traffic.

DISADVANTAGES OF VOICE ENCRYPTION

- Requires cryptographic key management and distribution to each radio.
- Requires keys to be changed at defined intervals.
- Inhibits secure interoperability among agencies that do not have the same keys.
- Adds expenses related to the subscribers' radios, system infrastructure, and personnel required to support encryption.

EFFECTIVE ENCRYPTION MANAGEMENT

Management of cryptographic keys is an important consideration in implementing a cryptographically secure voice network. Because patterns can be identified and keys decoded, keys should be changed regularly.

For smaller systems, keys can be manually changed in all radios on a policy-defined schedule. In some cases, as when a radio is lost or stolen,

keys must be changed immediately. For larger systems, however, this is impractical and requires automated key management functions. The Project 25 (P25) standards suite addresses this issue with a standard for Over the Air Rekeying (OTAR).² With OTAR, keys only have to be manually loaded the first time they are installed; subsequent changes are loaded remotely.

CONCLUSION

Adding encryption to a radio system involves much more than the purchase of radios with encryption capability. Users must be fully aware of the additional and sometimes significant burden of key management, which is vital to encryption. Poor key management practices negate any benefits of voice encryption and may result in a compromised system.

FOR MORE INFORMATION

- NIJ's Communications Technologies (CommTech) Web site:
www.ojp.usdoj.gov/nij/topics/commtech
- Regional National Law Enforcement and Corrections Technology Centers:
 - Northeast (Rome, NY) 888-338-0584
 - Southeast (Charleston, SC) 800-292-4385
 - Rocky Mountain (Denver, CO) 800-416-8086
 - Western (El Segundo, CA) 888-548-1618
 - Northwest (Anchorage, AK) 866-569-2969
 - Rural Law Enforcement Technology Center 866-787-2553

NOTES

1. See NIJ InShort, *Interoperability Gateways/Interconnects*, NCJ 217105, March 2007.
2. P25 is a user-driven process to define an open interface standards suite for public safety communications products. The Telecommunications Industry Association (TIA) provides a forum, via its TR-8 Private Wireless Committee, to develop P25 interface standards, specifically within its TIA-102 series of standards documents (www.tiaonline.org).

