

SACOM™

SACOM Encryption. Mission-Critical Security*

Encryption is one of the key advantages of digital wireless microphones. Anybody with a common scanner can remotely listen in on analog wireless microphone transmissions, but SACOM systems conform to the security encryption standard AES FIPS 197 established by the US Government for its agencies (<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>) and approved by the US National Security Agency (NSA) http://en.wikipedia.org/wiki/NSA_cryptography.

DECT: Not all encryption methods are equally secure. The DECT method used in some popular digital microphone systems is the standard established for cordless house phones and some baby monitors. DECT Standard Cipher (DSC) encryption is considered to be fairly weak, using a 35-bit initialization vector and encrypting the voice stream with only 64-bit encryption. The security algorithm has been broken. Another attack involves impersonating a DECT base station, which allows calls to be listened to, recorded, and re-routed to a different destination. (http://en.wikipedia.org/wiki/Digital_Enhanced_Cordless_Telecommunications).

Frequency Hopping: Another common encryption method used by some wireless conference room systems is called frequency hopping. The actress Hedy Lamarr is credited with developing this method in 1941 with her neighbor. Frequency hopping and its derivatives, HFSS and DSSS is old art. It does not provide a high level of encryption. (http://www.packetnexus.com/docs/20010419_frequencyHopping.pdf)

Proprietary Encryption: Some wireless microphone companies claim a “proprietary” encryption method. Proprietary typically describes a method that is developed internally by the microphone manufacturer without independent verification by a government agency. Without independent verification, companies who develop their own encryption method cannot say with certainty that their methods are secure.

On the other hand, all SACOM DS8000 series systems employ AES FIPS 197, approved by the NSA.

How SACOM Encryption works:

1. Each SACOM transmitter and receiver pair is programmed with its own random 256-bit encryption key which scrambles the signal one of 10^{77} (that's 10 followed by 77 zeros) different ways. The transmitter uses the key, along with other critical elements defined in AES FIPS 197, to scramble the signal before it sends it through the air. Then the matching receiver de-scrambles the signal back into audio. Anyone listening in will hear only white noise.
2. Transmitter and receiver pairs acquire a different random 256-bit encryption key every time they are sync'ed via the IR link. Any SACOM transmitter can be sync'ed to any SACOM receiver, but only one unique transmitter and one unique receiver can operate together at a time.

Establishing a new random encryption key is as easy as pushing two buttons on the receiver. If it was an agency's protocol to change the key often, there would be plenty of time during coffee breaks to re-key all the mics in a system.

3. In addition, the IR link that establishes the encryption key in the transmitter - receiver pair is itself encrypted so there is no way learn the encryption key.

4. For further security, several of the system's electronic components are protected from tampering with their own unique encryption keys. Even if the enemy was given an encryption key, it could not be programmed into a receiver.
5. All SACOM DS8000 systems are encrypted. If it is from SACOM, it is Mission-Critical Secure.