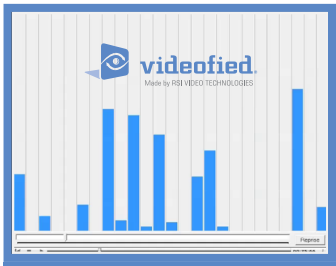
Videofied's Secure Wireless Communications Make Alarms Secure

ENCRYPTION

In the world of IT networks, cyber security experts stress the need for encryption and strong authentication to defend a network from a malicious hacker. This same encryption and authentication secures a Videofied wireless alarm system. All wireless communications, including wireless alarm systems, have become more vulnerable to attacks because new low-cost Software-Defined Radios (SDRs) have virtualized expensive radio components (e.g. mixers, filters, amplifiers, modulators/demodulators, detectors, etc.) into an inexpensive accessory or laptop computer. Videofied's encryption mitigates this risk and adds the equivalent of a one-time password to all wireless messages on the network. People using an SDR to intercept wireless signals find only digital gibberish. With Videofied's encrypted alarm system, the panel and all peripherals have a hidden numeric "electronic key" that is never placed in the message and never transmitted across the network. Instead, the panel or peripheral inserts the key into a complex equation that creates a one-time password protecting the message. When the message is received, the panel/sensor reverses the complex equation to verify the identity of the sender and read the message. The military developed encryption to keep prying eyes from reading their mail and it is at the core of Videofied wireless alarms. While there are many types and levels of encryption, Videofied uses Advanced Encryption Standard known as AES. AES encryption keeps hackers from communicating to secure military, corporate and enterprise networks and also secures Videofied wireless panels, sensors and MotionViewer cameras. Ultimately, all encryption can be broken with enough time and computer horsepower, but this is the realm of the National Security Agency (NSA) and not a burglar.



The video frame shown above is of a Videofied message being transmitted across many different frequencies (spread spectrum). If there is interference or "jamming" on a frequency, the system works around it to find an open lane to transmit the message/video of the alarm.

SPREAD SPECTRUM

Videofied goes beyond encryption to secure their radios and prevent interference/jamming that might compromise a system. Interference occurs when an outside radio signal overpowers the frequency used to communicate, blocking the channel and preventing or degrading the ability to transmit a message. Videofied uses "spread spectrum" radios to minimize interference between the alarm system and any other radio networks in the same vicinity. Spread spectrum broadcasts the message over multiple frequencies, hopping from one frequency to another to avoid those that are busy or jammed, something like a multi-lane highway where the messages change lanes to avoid other vehicles blocking traffic. In a sense, spread spectrum is a predecessor to cyber security, developed in WWII to secure radio communications and prevent the enemy from jamming battlefield radios. Spread spectrum is a robust approach to secure wireless.

Videofied alarm systems use BOTH encryption and spread spectrum to provide our clients with the most secure radio communications possible. There is no good reason anybody should install anything but alarms using encryption on a spread spectrum wireless to secure their property. Videofied manufactures secure wireless alarms and they include video verification built directly into the MotionViewer sensor/cameras to deliver faster police response. Why settle for anything less?

About the Author: Keith Jentoft is president of Videofied and has worked selling encrypted authentication to clients like the Defense Information Systems Agency (DISA) and large financial networks and holds a patent in encryption/authentication. For more information go to www.videofied.com.

videofied®
Made by RSI VIDEO TECHNOLOGIES