Mitigating Security Risks with Alarm Communication Systems for Mission Critical Applications

By Owais Hassan

Today's cybersecurity landscape is faced with a wide range of threats from sophisticated hackers to malware infections and malicious attacks that can threaten the delivery of essential services. These advanced persistent threats have changed the security industry and how organizations protect their networks. Traditional security solutions fail and security must expand beyond the physical perimeter when it comes to life safety and intrusion. Mission critical infrastructure such as embassies, federal buildings, and military bases are particularly vulnerable targets. Cybersecurity attacks also impact commercial installations at banks, museums, campuses, and enterprises that have high-value assets. Physical perimeter security alone is not enough, it needs to be supported by the underlying communication infrastructure. The delivery of alarm information must be by a trusted source that provides a stable network in a secure environment.

Wireless Alarm Communications Security

A typical wireless alarm communication system consists of various components connected to the alarm panel, as illustrated in the network diagram.

Every component of the alarm communication system, from the alarm panel to the communication subscriber, receiver and automation system, needs to satisfy the following security requirements:

- Physical security (tamper detection)
- Transmission security
- Substitution security (rogue and stolen equipment)
- Information security (data encryption and information assurance)
- Real-time mitigation controls (logging and network management)

Public vs. Private

Traditional methods of alarm communication are exposed to potential threats, posing serious security risks. The communication infrastructure starts from the transport layer security. Some alarm communication systems utilize the cellular spectrum where a public service provider is common knowledge (GSM, 3G, LTE, etc.), therefore susceptible to jamming. In the U.S. and most countries, it is illegal for private citizens to jam cell phone transmission. However, some countries are allowing businesses and government organizations to install jammers in areas where cell phone use is seen as a public nuisance. There are plenty of low cost commercial off-the-shelf handheld jamming devices readily available over the Internet. Therefore, any alarm communication system leveraging either unlicensed or cellular licensed spectrum is vulnerable to radio frequency interference and jamming. This issue impacts deployment of alarm communication networks serving mission critical needs.

All equipment deployed in the theater, government, and commercial installations needs to be designed to effectively safeguard and protect information against common security threats found in wireless networks:

- Loss of data confidentiality
- Data corruption and loss of integrity
- Replay attacks
- Spoofing, substitution, and masquerading
- Stolen field equipment
- Denial of services

Next-Generation Security

Technical solutions are being developed as a countermeasure to mitigate security risks. Next-generation alarm communication systems shall be designed to provide end-to-end encryption, ensure data is transmitted without eavesdropping, data tampering, and message forging.

The implementation of this next-generation security system shall use advanced authentication techniques such as dynamic key management, distributed denial-of-service firewall, and digital certificates that require digital signing before any equipment is authorized to be added to the network.

The wireless mesh radio technology shall use licensed spectrum, an unknown and covert frequency band along with frequency agility, and cognitive radio capabilities to combat jamming to head-end equipment.

The packet delivery communication protocol shall use dynamic mesh protocol which is proven to be less disruptive and more tolerable under jamming or radio frequency interference conditions. This distributed architecture is preferable compared to centralized base station cellular architecture where localized jamming at the single cellular base station could impact a large volume of customer premise equipment or shut down a substantial territory serviced by a single base station tower.

Network Management

The high security alarm communication system installation should be routinely evaluated to identify any threats arising out of potential vulnerabilities. The impact of a security threat should be quantified with Mean Time Between Hazardous Events measurements based on the following factors:

- Difficulty level of exploiting a threat
- Degree of harm caused by exploitation of the threat
- Mitigation and control techniques and their effectiveness

To rapidly mitigate any security risk as it unfolds in the real-world, the next-generation security system infrastructure shall have:

- An encrypted file system
- Secured executable image and critical data storages
- Anti-tamper and anti-cloning capabilities
- A flexible architecture
- Secured software upgrade capabilities to proactively harden the system

Expert implementation is key and network management is critically important. This modern approach to network security is the most reliable option for protecting the delivery of alarm information to the central monitoring station.

Owais Hassan is Vice President of Engineering at AES Corporation. He can be contacted at ohassan@aes-corp.com.