Giving Customers a Heightened Sensor of Security

Wireless edge devices can be an easy backdoor for hackers to exploit. For security systems, this means sensors and new add-ons like doorbell cameras, smart locks and thermostats. Find out what manufacturers are doing about it and what dealers/integrators ought to be doing about it. ***By Kirk MacDowell***

HACKED! In every sense, the word instills fear in government, corporations, small businesses and homeowners. The consequences can be devastating. Individuals and organizations hire electronic security industry companies to protect people and assets. If a breach or hack can be attributable back to these companies, it is tantamount to betraying the trust that those customers expect.

Many dealers and integrators understand their responsibility to ensure that they have taken appropriate steps to safeguard a customer's premises, including data and intrusion device integrity — both hardwired and wireless. Have their manufacturing partners stepped up to the task as well? Moreover, as all manufacturers compete with one another to launch new wireless products into the marketplace, are they in sync with the dealer community making sure that their products are safe?

To get a better grip on how wireless intrusion detection equipment manufacturers and security alarm dealers are addressing this new frontier of hackers vs. encryption, *SSI* checked in with several suppliers and their channel partners. In a nutshell, the discussion indicates manufacturers have taken encryption to a new level in which they now say virtually eliminates the breach of a wireless sensor. While the "choke" points of wireless vulnerability also include the control panel and network to which it connects, the focus here is on sensor security, as that appears to be the last threshold needing more attention.

Vulnerabilities Come to Light

Encrypted wireless sensors can be one- or two-way, meaning they are pinging the receiver often and the panel/receiver pings the sensor back. There are many advan-

DMP's encrypted 900MHz commercial-grade spread-spectrum technology with frequency hopping changes channels 32 times a second. The 1100 Series wireless sensors with 128-bit AES encryption technology are two-way, allowing the sensor and panel to be in communication constantly.

tages to two-way sensors, but that's a story for another day. Here, the conversation is strictly hardening wireless sensors as a potential hacking target — ensuring they are not a cybersecurity liability.

As the labor pool shrinks for qualified installers, manufacturers have demonstrated their ability to help fill the gap by engineering quality wireless sensors and peripheral devices to offset expensive labor dollars. These sensors save dealers and integrators labor hours every day.

Before the advent of wireless door and window sensors, most companies, especially in the residential space, would allocate one hour for each door/window installation as wire would need to be concealed in the baseboards, attic or basement. When wireless sensors were introduced, the hour per device was reduced to 15 minutes per wireless sensor for installation, testing and programming. Some sporadic wireless range issues notwithstanding, the world seemed pretty perfect.

Enter spy vs. spy type people who hack security systems for gain or as a challenge. These attacks have been reported in numerous articles and television shows, including "20/20." When the sensor activates, it sends a wireless code and identifier to the intrusion panel. In some circumstances, these codes were electronically captured by a person, who using a device later disarmed the system or rendered the sensor useless by bypassing the sensor, thus gaining entry into the premises undetected. Even if you've never seen this breach performed in person, it nonetheless places doubts and fear into consumers' minds.

Suppliers Step Up

The research for this article revealed that most security manufacturers are taking sensor integrity and encryption very seriously. For example, DMP uses encrypted 900MHz commercial-grade spread-spectrum technology with frequency hopping that changes channels 32 times a second. This practice has long been used by U.S. government-type communications. According to DMP Executive Director of Marketing Mark Hillenburg, the company's 1100 Series wireless sensors with 128-bit AES encryption technology are two-way, allowing the sensor and panel to be in communication constantly. These safeguards have helped earn DMP's 1100 Series a Commercial Burg and Fire UL Listing.

Rob Post, owner of Post Alarm Systems of Arcadia, Calif., says that "customers are asking more than ever before about hacking of security systems." Post Operations Manager Anthony Franco agrees, and adds, "Consumers may ask if the system can be hacked, but we see it as much more robust question." The fact is that while consumers are asking about hacking, what they really should be focused on are more detailed questions encompassing wireless encryption, Z-Wave device security and communication path integrity.

The team at EMC Security in Suwanee, Ga., recently made the decision to transition a large portion of its installations to Alula. There were many reasons for this but near the top of the list was the encrypted sensors the manufacturer offers within its family of products. EMC Vice President of Sales Michael Morton related that while few customers use the term "encrypted" they do ask what safeguards

Not only are DSC's PowerG wireless sensors engineered with 128-bit AES encryption but the 900MHz frequency allows for an extended communications range. This is useful when consumers change décor by adding metal, glass, etc., which could play havoc with wireless range.

the dealer uses to ensure the security of the system. Unquestionably, dealers and integrators today are talking about security integrity of system and sensors during the sales and installation process.

State of Encryption

Encrypted sensors, especially two-way devices, are more costly to dealers with some indicating they are paying a $4 premium for bidirectional encrypted sensors. Whether one- or two-way models, these devices cost more because they do more, and they allow dealers an opportunity to offer complete security to their customers. While many believe the electronic security industry has been in a freefall race to the bottom in terms of what dealers and consumers are willing to pay for systems, here is a means to help restore value to installed security solutions.

Steve Shapiro, general manager of security and connected home products for Johnson Controls/Tyco Security Products and former vice president of product solutions at ADT, has an interesting perspective on two-way encryption, especially those using the 900MHz radio frequencies for security applications. He conveyed that not only are DSC's PowerG wireless sensors engineered with 128-bit AES encryption but the 900MHz frequency allows for an extended communications range. This is especially important when consumers change décor by adding metal, glass and the like, which could play havoc with wireless range.

Qolsys also offers encrypted sensors. The manufacturer's panels can take over older one-way sensors while enhancing the security installation by adding one- and two-way encrypted sensors to the original installation.

Shapiro pointed out that Qolsys also offers encrypted sensors. The manufacturer's panels can take over older one-way sensors while enhancing the security installation by adding one- and two-way encrypted sensors to the original installation. DMP is also well known for its ability to produce new, innovative sensors and products that are backward compatible on legacy systems. Imagine taking a five-year-old intrusion panel and adding encrypted sensors, thus bringing the system up to current consumer expectations.

New Standards of Security

New, advanced devices such as lights, locks and thermostats are, for the most part, Z-Wave or ZigBee enabled and are increasingly being tied into the security alarm system to some degree. Recent news reports have demonstrated a common thread in the means by which hackers have gained access to these types of devices, bypassing their security or lack thereof.

Z-Wave Alliance Executive Director Mitchell Klein indicates that the newer Z-Wave devices with S2 (launched in 2017) have three different layers of security, depending on the security requirement of the device. For instance, access control would have the highest level of protection as it is the moat through which someone has to penetrate to gain entry. This level of encryption has to be authenticated by a fingerprint. However, most dealers seem to believe that all newer Z-Wave devices have the encryption necessary to mitigate a hacker. Security manufacturers agree, but remind dealers to make sure the Z-Wave device is version S2.

Within the next few years, virtually all security manufacturers will standardize on encrypted devices. For now, conscientious dealers and integrators can gain an edge by creating a more secure environment for their customers, and in doing so move away from the winless race to the bottom. SSI

KIRK MACDOWELL is the principal of MacGuard Security Advisors. He can be reached at kirk.macdowell@macguard.com.

4 Ways to Gain an Encryption Edge

As dealers and integrators compete for their share of the market, they should keep in mind a few things.

1. Stop the race to the bottom! Offer encrypted sensors as the norm and walk the client through why you are providing them "real" security.
2. If your current system provider does not offer encrypted sensors, ask why not?
3. Most manufacturers will allow encrypted and nonencrypted sensors to coexist into the intrusion panel, which can save the user money. When taking over a system (installed by another company) this may be viewed as an inexpensive way to gain an account. However, consider that it may be more advisable to guide the client through the benefits of encryption and instead offer to change out the existing sensors.
4. Many dealers have an addendum on the contract that says something like, "Clients offered full perimeter protection but declined." Check with your legal counsel about adding, "Client offered encrypted sensors but declined."