Reprinted with permission from the May, 2017 issue of ...

MANAGEMENT

Securing "Things" in the Internet of Things

By Derek Atkins, CTO, SecureRF Corporation

With more and more things connecting to the Internet of Things (IoT) and the entire movement gathering momentum, keeping devices and information secure is a daunting task. While the number of connected devices is hardly a surprise, the key is that many of these newly-connected things will be devices that we have previously not thought of connecting.

Product managers in nearly every major consumer and industrial market are realizing the competitive advantages of sensing, locating and controlling devices through the IoT. This will certainly lead to some truly innovative and game-changing IoT-enabled devices, as well as some that will flop dismally.

However, security breaches will multiply along with smart devices because security remains an afterthought for so many manufacturers. Fallout from breaches, including revenue loss and consumer backlash, will ultimately move security to the top of the priority list. Manufacturers will be driven to incorporate effective authentication and data protection in their devices, but without making them more complicated or expensive.

IoT a Fact of Life

We will move from early adopters to more mainstream acceptance of connected devices in the home. It will no longer be a novelty to have a connected household where, for example, residents use Amazon Dash buttons to easily reorder products, or use a single voice-activated device to control the lights, locks, and kitchen appliances.

While these connected devices will provide homeowners with many conveniences, they will also pose increased risks. A single breach of an inadequately secured device could have devastating consequences for an entire structure. For example, a criminal could hack into household appliances and heat the oven or turn on the refrigerator's water dispenser, creating the risk of fire or flood. Manufacturers that fail to address these security risks before a high-profile breach occurs will likely experience their own devastating consequences in due time.

While connected devices will provide homeowners with many conveniences, a single breach of an inadequately secured device could have devastating consequences.

The need for securing IoT devices will grow, but what is uncertain at this time is who will ultimately be responsible for securing them, and how security will be deployed and managed. Even a relatively simple product like a smart lightbulb has a long supply chain that includes a chipmaker and a software vendor. As of yet, there is no industry consensus about which entity will be responsible for security. Some standards will have to emerge, but the issue will be far from settled.

Increased Focus on Security

We predict that product developers will sharpen their focus on device security. In 2016, we saw increased interest in our security solutions from developers of products including sensors, door locks and other IoT-connected devices. Many developers are realizing that legacy products with insufficient or no built-in security need to be redesigned. Where feasible, in-the-field updates will be made available to add security features.

The National Security Agency has publicly stated that impending quantum computing-based attacks will break existing security protocols like RSA and ECC. Quantum computers capable of executing these attacks are expected to be available in 10 to 15 years, though governments and some large institutions may acquire them sooner. Hence, manufacturers of products with extended lives in the field, such as aircraft, automobiles, HVAC systems, and traffic lights, will show growing interest in securing them with quantum-resistant methods.

IoT product developers will increasingly pursue quantum-resistant security solutions, like those from SecureRF, to ensure that their long-lived IoT devices will be secure today as well as in the not-so-distant future when quantum attacks become feasible.

Chip manufacturers are also showing heightened interest in quantum-resistant security methods for low-resource devices, because current cryptographic protocols, such as ECC, which is used in many chip families, are vulnerable to quantum attacks. We predict more and more chipmakers will seek quantum-resistant security solutions for fear of losing sales to competitors who make such protocols available for use in their products.

The PC industry has long been educating consumers on how to secure their computers. A similar effort by IoT industry stakeholders to educate the public on securing smart devices will gather steam. This effort will occur on a larger scale than it has for computers, as IoT products are more numerous, used by more people, and require little or no technical literacy to operate. As part of this effort we expect that user manuals will provide more information on security.

In addition, major home supply retailers may start offering classes on securing smart devices, such as thermostats and door locks, just like they offer classes on installing floor tiles. It's also likely that retailers and consumer brands will highlight IoT security as a product feature, creating preference in the market for devices that are labeled hacker-resistant. What is certain is that the IoT is, as yet, far from being safely locked down.

Contact: SecureRF Corp., 100 Beard Sawmill Road, Suite 350, Shelton, CT 06484 ☎ 203-227-3151
fax: 888-507-7364 E-mail: info@securerf.com
Web: www.securerf.com ❒