# Cybersecurity in the Age of IoT

## *Can my smart thermostat really be hacked?*

BY MARIA TAYLOR
*THE NEWS* STAFF

Chances are, HVAC contractors who deal with smart technology have run across the term “digital home invasions” — or some variation of it — from at least a couple customers.

“Some situations have made headlines recently where these bad actors were able to access smart home devices — lights, smart plugs, baby cameras,” said Scott Harkins, vice president and general manager, Connected Home, Resideo Technologies.

That being said, most hacking occurs when the homeowner’s internet connection is not secure or when the user has not used a strong, unique password for each app that controls their devices, Harkins said. Nor is demand dwindling. The smart home market is forecasted to include nearly 1.3 billion devices by 2022, with a five-year compound annual growth rate of 20.8 percent, Harkins noted.

“The demand for smart home technology is only increasing, which means our responsibility as an industry to make these products secure and protect consumer information is also increasing,” he said.

## HVAC HACKING: WHAT’S THE RISK?

Prashanth Shetty is chief marketing officer at Ayla Networks. Ayla is not aware of any sort of pattern of attacks against IoT devices themselves, he said, although he was able to point to some instances.

“There have been occasions when popular home security cameras and Wi-Fi routers that used default or widely known common passwords were hacked, allowing inbound connections and malware installation,” he said. “In that attack, the compromised devices were used in a bot-net scenario (think DYN attack) which had major negative impact.”

A few years ago, the Department of Homeland Security (DHS) commissioned a study (it was a penetration test) on power generation equipment, he added. After the formal test was completed, the equipment was released to the consultants, who were asked to do their worst.

**ALL ABOARD:** Security is everyone’s job – from the engineer working on product design to the contractor installing the system to the homeowner who operates the system daily. Here, a contractor installs Resideo’s Honeywell Home T10 Pro Smart Thermostat.

“Within minutes, the equipment was a smoking, destroyed piece of junk,” Shetty said. “This should be a warning to all IoT device manufacturers to protect against commands that can do damage to equipment. A hacker who takes over an HVAC system in a house or building could wreak havoc by turning on/off motors, compressors beyond what is continuously tolerable, creating a safety risk situation.”

That goes for any device with moving parts that can be manipulated via the IoT: a/c compressors, door locks, industrial equipment, and pool pumps, to name a few.

“Even IoT-controlled shutters/blinds could potentially be made to overheat or catch fire if they were continuously, rapidly moved,” he said.

## CYBERSECURITY SAFEGUARDS

Security is everyone’s job — from the engineer working on product design to the contractor installing the system to the homeowner who operates the system daily, Harkins said.

Resideo follows the principle of “secure-by-design” during the product design process.

“We incorporate the best security practices in all steps in the implementation and operation of our products,” Harkins said. “We have a rigorous secure product development life cycle that is built on the latest ISA standards, and our privacy requirements mandate that data be fully encrypted both at rest and in transit. We require features such as secure boot and code signing in our products to ensure their integrity against bad actors.”

Ayla has had a head of platform security for more than four years to ensure security best practices in product releases and in DevOps process. Over time, the company has added security certification, data privacy controls, regular penetration testing, and other forms of recurrent review of security, and a security officer to oversee it all.

“We believe security in IoT is not a bolt-on or afterthought, but needs to be designed into the product early on,” Shetty said. “We vigilantly track market developments for security incidents, and try to test for those scenarios in our QA/test process. Moreover, our close partnership with module/chipset partners also means we have increased awareness of security incidents from their channels, and we receive early access to bug patches to test as they become available from the partners.”

At the device level, Ayla’s embedded software agent runs a real-time OS (RTOS), which Shetty explained as “smaller, lightweight, and more industrial strength, compared to say Windows or Linux.” An RTOS is substantially ‘minimized,’ meaning it has less software and supports fewer commands, making it less hackable. Plus, in Ayla’s design, it’s always the device that initiates a connection to the cloud, not vice versa.

“Any attempt to open a connection into the device is rejected, which helps us better reject attempts to alter the software on the device,” he said.

At the mobile app level, Ayla’s security features include strong authentication that are part of the mobile foundry. At the platform layer, the cloud is a micro-services architecture, leverages security certificates, and follows “the principle of least privilege,” which severely restricts what information is shared with the device.

“Cloud-to-device communication is secured by TLS, characterized by short-lived connections and high rate of key changes, making communications more difficult to compromise,” Harkins said.

## PRECAUTIONS

“Safeguards should be put in place at every step, and that certainly doesn’t stop once the technology reaches the homeowner’s doorstep,” said Harkins. “Prevention is often the best protection, and most cybersecurity attacks can be prevented by being aware of the possibility and danger of cybersecurity attacks and taking elementary precautions to minimize exposure.”

If a contractor is responsible only for installing the device, he or she should ensure the adequacy of passwords and other common protections already in place in systems, Shetty advised.

“Change all default passwords,” he said. “Don’t ever, even for ‘just testing’ purposes, use simple passwords, as they tend to become permanent in the rush to finish jobs. Wi-Fi passwords should always be employed and be as complex as you can tolerate.”

If a contractor is also responsible for the selection of the device, it’s a bit more complicated, as the process now involves ensuring the security of all components in the system from the device, any mobile applications, and cloud infrastructure. This could include:

- Using multi-factor authentication on all administrative interfaces — even mobile apps, but especially web-based applications.
- Ensuring that all components are tested by their manufacturers to your security expert’s satisfaction. “For cloud-based infrastructure, this should include ISO-27001, SOC2, or similar certification or annual auditing,” Shetty said.
- Ensure the devices to be installed have been penetration tested. “While Ayla tests its Wi-Fi and cellular modules, this does nothing to ensure the security of the underlying device,” Shetty said. “Devices built on Linux, Windows, or other common platforms need to be carefully and completely secured, too. As a simple test, port-scan the device to see what interfaces it may make available, and question any that you don’t need.”
- Checking that any unnecessary interfaces are disabled to the network (Wi-Fi, cellular, or others).
- Implementing network partitioning, so that IoT devices can’t “see” each other or other devices on the network.

Through its training programs, Resideo provides guidance on cybersecurity do’s and don’ts to contractors on how to correctly install Resideo Honeywell Home™ products and use appropriate cybersecurity safeguards to improve homeowner protection, particularly for home control devices that are internet-facing.

Part of good security, of course, is making sure everything stays secure once the contractor walks out the door.

“Cybersecurity is something that demands constant vigilance against operational errors or new unanticipated threats,” Harkins said. “[Resideo’s] products have features to automatically update themselves to the latest protections and ensure that they are properly maintained and monitored.”

> “Safeguards should be put in place at every step, and that certainly doesn’t stop once the technology reaches the homeowner’s doorstep. Prevention is often the best protection, and most cybersecurity attacks can be prevented by being aware of the possibility and danger of cybersecurity attacks and taking elementary precautions to minimize exposure.”
>
> *—Scott Harkins,*
> *vice president and general manager,*
> *Connected Home Resideo Technologies*

Moving from products to practices, he recommends advising consumers to keep their systems up to date with the most current software versions, as those often contain new or updated security protocols. That goes for antivirus software as well, across all devices on the home network.

“It’s always smart, if you’re using a public Wi-Fi network, to use a virtual private network (VPN) connection to enhance security of network traffic,” he added. “A secure, password-protected internet connection is vital.”

For customers who may still be on the fence about security, Shetty emphasized that IoT devices can help make a home safer.

“Visibility to the operational and performance data can be very revealing, especially when linked to preventing a household safety incident,” he said. “And the ability to have convenient command and control at your fingertips can help with energy management and home security.”

## WHAT DOES THE FUTURE HOLD?

Harkins expects consumer expectations will drive the interoperability of smart home solutions, including the continued integration of voice assistants to automate the home. And those consumer expectations include personal privacy and security.

“We’re seeing trends in real estate and home building that point to smart homes being the standard home of the future,” Harkins said. “We believe artificial intelligence and machine learning will enable a truly smart home, anticipating the homeowner’s needs and even anticipating critical issues that can be avoided … We understand that our customers want their smart homes to be safe, comfortable, reliable, and secure. As smart thermostats, water monitoring systems, security systems, and remote monitoring become more commonplace, so will consumers’ ability to safeguard their technology.”

Companies that are serious about security build security into their products’ DNA — end to end, through design and development, he continued.

As security becomes a more central theme in the context of IoT, manufacturers and contractors could take the opportunity to expand their portfolio of services and offer cyber monitoring in the home, as home security service providers like ADT or Alarm.com are looking to offer as well.

Security tends not to be viewed very seriously until after a major incident, Shetty pointed out.

“The severity and scale of security incidents will likely increase, given the level of interoperability between devices in the connected home,” he said. “We’ll see large scale disruptions of services; then, those security problems will be taken more seriously.” N