'Smart home' security flaws found in popular system

May 2 2016, by Nicole Casal Moore

Smart homes act as “intelligent agents” that use sensors and software to anticipate our needs and tend to tasks that improve our health, energy efficiency, even social media. Credit: Washington State University

Cybersecurity researchers at the University of Michigan were able to hack into the leading "smart home" automation system and essentially get the PIN code to a home's front door.

Their "lock-pick malware app" was one of four attacks that the cybersecurity researchers leveled at an experimental set-up of Samsung's SmartThings, a top-selling Internet of Things platform for consumers. The work is believed to be the first platform-wide study of a real-world connected home system. The researchers didn't like what they saw.

"At least today, with the one public IoT software platform we looked at,

which has been around for several years, there are significant design vulnerabilities from a security perspective," said Atul Prakash, U-M professor of computer science and engineering. "I would say it's okay to use as a hobby right now, but I wouldn't use it where security is paramount."

Earlence Fernandes, a doctoral student in computer science and engineering who led the study, said that "letting it control your window shades is probably fine."

"One way to think about it is if you'd hand over control of the connected devices in your home to someone you don't trust and then imagine the worst they could do with that and consider whether you're okay with someone having that level of control," he said.

Regardless of how safe individual devices are or claim to be, new vulnerabilities form when hardware like electronic locks, thermostats, ovens, sprinklers, lights and motion sensors are networked and set up to be controlled remotely. That's the convenience these systems offer. And consumers are interested in that.

As a testament to SmartThings' growing use, its Android companion app that lets you manage your connected home devices remotely has been downloaded more than 100,000 times. SmartThings' app store, where third-party developers can contribute SmartApps that run in the platform's cloud and let users customize functions, holds more than 500 apps.

The researchers performed a security analysis of the SmartThings' programming framework and to show the impact of the flaws they found, they conducted four successful proof-of-concept attacks.

- They demonstrated a SmartApp that eavesdropped on someone

setting a new PIN code for a door lock, and then sent that PIN in a text message to a potential hacker. The SmartApp, which they called a "lock-pick malware app" was disguised as a battery level monitor and only expressed the need for that capability in its code.

- As an example, they showed that an existing, highly rated SmartApp could be remotely exploited to virtually make a spare door key by programming an additional PIN into the electronic lock. The exploited SmartApp was not originally designed to program PIN codes into locks.
- They showed that one SmartApp could turn off "vacation mode" in a separate app that lets you program the timing of lights, blinds, etc., while you're away to help secure the home.
- They demonstrated that a fire alarm could be made to go off by any SmartApp injecting false messages.

How is all this possible? The security loopholes the researchers uncovered fall into a few categories. One common problem is that the platform grants its SmartApps too much access to devices and to the messages those devices generate. The researchers call this "over-privilege."

"The access SmartThings grants by default is at a full device level, rather than any narrower," Prakash said. "As an analogy, say you give someone permission to change the lightbulb in your office, but the person also ends up getting access to your entire office, including the contents of your filing cabinets."

More than 40 percent of the nearly 500 apps they examined were granted capabilities the developers did not specify in their code. That's how the researchers could eavesdrop on setting of lock PIN codes.

The researchers also found that it is possible for app developers to

deploy an authentication method called OAuth incorrectly. This flaw, in combination with SmartApps being over-privileged, allowed the hackers to program their own PIN code into the lock—to make their own secret spare key.

Finally, the "event subsystem" on the platform is insecure. This is the stream of messages devices generate as they're programmed and carry out those instructions. The researchers were able to inject erroneous events to trick devices. That's how they managed the fire alarm and flipped the switch on vacation mode.

These results have implications for all smart home systems, and even the broader Internet of Things.

"The bottom line is that it's not easy to secure these systems" Prakash said. "There are multiple layers in the software stack and we found vulnerabilities across them, making fixes difficult."

The researchers told SmartThings about these issues in December 2015 and the company is working on fixes. The researchers rechecked a few weeks ago if a lock's PIN code could still be snooped and reprogrammed by a potential hacker, and it still could.

In a statement, SmartThings officials say they're continuing to explore "long-term, automated, defensive capabilities to address these vulnerabilities." They're also analyzing old and new apps in an effort to ensure that appropriate authentication is put in place, among other steps.

More information: Security Analysis of Emerging Smart Home Applications. iotsecurity.eecs.umich.edu/

Provided by University of Michigan