Smart Home Product Security Risks Can Be Alarming

NWC ALLIANCE · WEDNESDAY, JULY 3, 2019·READING TIME: 5 MINUTES

By TAMARA DIETRICH, The Daily Press | January 3, 2019

Say you're on your laptop at Starbucks, minding your own business, when an acquaintance of yours across the room isn't minding his.

Unbeknownst to you, he's using the same store Wi-Fi as you to conduct a virtual invasion of your smart home, accessing your light switch app and using it to disable your home's security camera so real thieves can break in – or walk in, if he's disabling the smart lock, too.

And you're none the wiser – until you get home and discover your home's been hacked. And burgled.

This is just one scenario demonstrating one of many inherent flaws that computer scientists at the College of William and Mary discovered in internet-connected smart home devices during tests they conducted over the summer.

This particular flaw allows hackers to attack a smart home's low-security device – a light switch or thermostat, for instance – and use that access to attack a high-security device they could not otherwise access.

It's one example of what's called lateral privilege escalation, and experts warn that such smart home hacks are easier than you might think. They can lead to all kinds of potential mischief, if not outright harm, from switching off your security system to cranking up your smart oven until it overheats and burns the house down.

"The possibilities are limitless," said Adwait Nadkarni, lead investigator and assistant professor of computer science. "There are so many devices in the home that affect your security, affect the integrity of your home."

Experts say that in just two years there will be 20 billion smart home products in use.

"You can imagine the possible combinations of these kinds of attacks will obviously increase as we'll have more interconnected devices," said associate professor Denys Poshyvanyk. "At this point, it's hard for us to imagine what else people will do."

Nadkarni and Poshyvanyk co-authored a paper on their work that they'll present at the 9th annual ACM Conference on Data and Application Security and Privacy in Dallas in March.

Student co-authors include Kaushal Kafle and Sunil Manandhar and post-doctoral fellow Kevin Moran.

In the paper, they lay out the potential misuses of the computer routines or portions of code that control smart home products and offer 10 key findings with “serious security implications.”

“The diversity of these products is staggering,” the paper states, “ranging from small physical devices with embedded computers such as smart locks and light bulbs to full-fledged appliances such as refrigerators and HVAC systems.”

And the risks, it states, can be rather alarming.

“Because many of these products are tied to the user’s security or privacy (e.g., door locks, cameras), it is important to understand the attack surface of such devices and platforms in order build practical defenses without sacrificing utility.”

For their research, Nadkarni and Poshyvanyk focused on two of the most popular smart home platforms – Google Nest and Philips Hue – that implement home automation “routines.”

Routines are the interactions between smart home devices and the apps that control them. They are becoming the heart of seamless home automation.

Two Routines

According to the paper, there are two broad categories of routines: one that allows users to “chain together” a variety of devices using a third-party app interface, and one that uses a “centralized data store” as a sort of switchboard where devices and apps can communicate with each other over the internet.

Both are intended to make smart home automation more seamless for the user, and both were found to be vulnerable, giving hackers the ability to attack all the internet-connected devices in the home.

For the centralized data store platform, for instance, when you use your mobile app to communicate with a low-security device – say, a light switch – the device accesses your smart home using an authorization token.

“Anybody can steal that access token,” Nadkarni said, and use it to, say, make your smart home think you’re inside and turn off the security camera.

The scientists insist it’s not that hard.

“You don’t need any specialized education,” said Poshyvanyk. ‘You just need to know how to run certain programs. Even a high schooler could do that.”

They blame the vulnerabilities on consumer demand and the headlong rush to meet it.

“Manufacturers race to release these systems without having a good understanding of how they will be used in the wild,” Poshyvanyk said.

After the researchers identified the security flaws, they contacted platform vendors Google and Philips and app developer and manufacturer TP Link to report what they found.

TP Link fixed the flaw in its latest Kasa Switch light dimmer app, which prevents the type of theoretical lateral attack outlined earlier. Philips is expected to roll out a fix to its platform and Google is working to address vulnerabilities.

But the issue is bigger than one company – it’s the industry overall that needs to get smarter.

“We’re basically arguing that we need a systemic effort in terms of properly designing these systems with security in mind,” Poshyvanyk said.

“Because these problems will get worse with time. More devices will be added. (If) they’re not thinking about designing in security in the first place, we’re going to be having even bigger problems down the road.”

NWC Alliance

https://nwcalliance.com/home/wise-insure/cyber-insurance/

https://nwcalliance.wordpress.com/home/wise-insure/

https://www.insurancejournal.com/news/national/2019/01/03/513394.htm