Off-the-shelf smart devices found easy to hack

13 March 2018

Credit: CC0 Public Domain

Off-the-shelf devices that include baby monitors, home security cameras, doorbells, and thermostats were easily co-opted by cyber researchers at Ben-Gurion University of the Negev (BGU). As part of their ongoing research into detecting vulnerabilities of devices and networks expanding in the smart home and Internet of Things (IoT), the researchers disassembled and reverse engineered many common devices and quickly uncovered serious security issues.

"It is truly frightening how easily a criminal, voyeur or pedophile can take over these devices," says Dr. Yossi Oren, a senior lecturer in BGU's Department of Software and Information Systems Engineering and head of the Implementation Security and Side-Channel Attacks Lab at Cyber@BGU. "Using these devices in our lab, we were able to play loud music through a baby monitor, turn off a thermostat and turn on a camera remotely, much to the concern of our researchers who themselves use these products."

"It only took 30 minutes to find passwords for most of the devices and some of them were found only through a Google search of the brand," says Omer Shwartz, a Ph.D. student and member of Dr. Oren's lab. "Once hackers can access an IoT device, like a camera, they can create an entire network of these camera models controlled remotely."

The BGU researchers discovered several ways hackers can take advantage of poorly secured devices. They discovered that similar products under different brands share the same common default passwords. Consumers and businesses rarely change device passwords when purchased so they could be operating infected with malicious code for years.

They were also able to logon to entire Wi-Fi networks simply be retrieving the password stored in a device to gain network access.

Dr. Oren urges manufacturers to stop using easy, hard-coded passwords, to disable remote access capabilities, and to make it harder to get information from shared ports, like an audio jack which was proven vulnerable in other studies by Cyber@BGU researchers. "It seems getting IoT products to market at an attractive price is often more important than securing them properly," he says.

Tips for IoT Product Security

With the goal of making consumers smarter about smart home device protection, BGU researchers offer a number of tips to keep IoT devices, families and businesses more secure:

1. Buy IoT devices only from reputable manufacturers and vendors.

2. Avoid used IoT devices. They could already have malware installed.

3. Research each device online to determine if it has a default password and if so change before

installing.

4. Use strong passwords with a minimum of 16 letters. These are hard to crack.

5. Multiple devices shouldn't share the same passwords.

6. Update software regularly which you will only get from reputable manufacturers.

7. Carefully consider the benefits and risks of connecting a device to the internet.

"The increase in IoT technology popularity holds many benefits, but this surge of new, innovative and cheap devices reveals complex security and privacy challenges," says Yael Mathov, who also participated in the research. "We hope our findings will hold manufacturers more accountable and help alert both manufacturers and consumers to the dangers inherent in the widespread use of unsecured IoT devices."

More information: Omer Shwartz et al. Opening Pandora's Box: Effective Techniques for Reverse Engineering IoT Devices, *Smart Card Research and Advanced Applications* (2018). DOI: 10.1007/978-3-319-75208-2_1

Provided by American Associates, Ben-Gurion University of the Negev