UC SANTA BARBARA

THE Current

October 20, 2020
Harrison Tasoff

Securing the Internet of Things

National Cyber Security Awareness Month provides an opportunity to explore emerging fields in information security. Perhaps none is as overlooked as the rapid emergence of network-enabled smart devices, what researchers call the Internet of Things.

We're used to thinking about applications on computers, but we are increasingly surrounded by networked devices: voice-activated assistants, smart appliances, Wi-Fi cameras, video doorbells and more. These electronics are the new forefront in cyber security.

Giovanni Vigna focuses on this new frontier. "There is concern that there are a lot of hidden vulnerabilities in these devices," he said. Vigna, a professor of computer science at UC Santa Barbara, serves as director of the campus's Center for Cybersecurity and co-director of the Security Lab.

Manufacturers optimize networked electronics for ease of use, and that sometimes comes at the cost of eliminating security features. "Convenience versus security: this has been a tradeoff since the beginning of computing," Vigna said.

What's more, if you want your phone to communicate with your bathroom scale, your watch and your thermostat, you have to resort to the lowest common denominator between all the devices, he explained.

"A lot of people think that we can take current security analysis and, with little effort, repurpose it for smart devices. After all, it's still code," Vigna said. "But the

vast majority cannot be simply repurposed.”

For instance, unlike applications such as Microsoft Word, these programs don’t live in a convenient folder on a hard drive that security experts can access. These gadgets use a variety of different architectures and bespoke hardware. Just extracting the source code is a challenge, Vigna said, let alone analyzing it.

“You actually need new approaches to be able to take this wide variety of targets and execute them and analyze their security,” Vigna explained.

That’s why the Security Lab is developing ways to extract the code from these devices and run them on virtual hardware, a technique called emulation. The researchers can train a machine learning algorithm by setting it to observe how the code interacts with the environment over hundreds of thousands of iterations. The algorithm can then begin to reproduce the functionality of a device’s hardware without the scientists ever having physical access to it.

“It is reverse engineering at its best,” said Vigna. The team can emulate the hardware on their computers and execute the code without the physical device. In fact, virtualization and emulation have become key tools in tackling a variety of different research problems in this emerging field.

Dealing with custom hardware is just one of the challenges of securing smart devices. Computers and phones have fully fledged operating systems, which include all sorts of security features. But the bare-bones operating systems on smart devices aren’t nearly as robust, Vigna explained. Because of the limited capacity of these devices, many resource-intensive security mechanisms can’t be implemented.

In addition, when you purchase a computer or phone, the company behind it will issue updates and patches to address any vulnerabilities that present themselves. But there’s no guarantee the companies making smart devices will do the same, according to Vigna. A company could even go out of business, he said, and suddenly you’ll have, say, a whole system of cameras without any security support.

The global supply chain further complicates this already messy landscape. A device is only as secure as its most vulnerable component. But when a company purchases a part from a supplier, they don’t receive the source code to check for vulnerabilities. This issue is exacerbated by the number of disparate components that go into the final product.

The increasing number of devices with minimal security has created an opportunity for cyber criminals to assemble vast networks of compromised equipment relatively surreptitiously.

“This already has happened,” said Vigna. “Just look at the MIRAI botnet.”

The MIRAI malware is one of many programs that can take advantage of lax security on smart electronics to create a network of compromised devices, or botnet.

“The biggest denial of service attack that ever happened was a bunch of these cameras that were compromised, not even in a sophisticated fashion,” Vigna continued. The cameras all had default accounts and passwords and were exposed to the internet. A malicious actor logged into them and used them to launch denial of service attacks, in which internet traffic overwhelms a server by sheer volume.

“We use the MIRAI botnet to provide motivation for any of our research projects,” Vigna said. “You remember the MIRAI botnet? Yeah? That could happen again.”

The Security Lab’s ability to reverse engineer and emulate devices is a useful research tool, but only automation will enable it to scale to a practical level. A lot of analysis requires performing actions tens to hundreds of thousands of times. What’s more, this analysis generally occurs in the lowest level of code: binary. “Data structure, functions, types, they are all gone,” Vigna said, “which makes the whole process incredibly hard.” Automating the process is the only way to do this efficiently and economically.

“That’s why it’s a research topic,” he continued. “It’s not something that the industry can do at scale right now.”

About UC Santa Barbara

The University of California, Santa Barbara is a leading research institution that also provides a comprehensive liberal arts learning experience. Our academic community of faculty, students, and staff is characterized by a culture of interdisciplinary collaboration that is responsive to the needs of our multicultural and global society. All of this takes place within a living and learning environment like no other, as we draw inspiration from the beauty and resources of our extraordinary location at the edge of the Pacific Ocean.