When your house spreads gossip about you

May 2 2023, by Mads Wang-Svendsen

Credit: Unsplash/CC0 Public Domain

More and more of the devices that we surround ourselves with on a daily basis are connected to the internet. This makes them not only smart, but also vulnerable to cyberattacks and criminal acts.

Before long, we might have smart fridges that help us keep track of what foods are about to expire and when to shop. How could this be harmful? Who would be interested in the expiry date of your milk or monitoring your food inventory?

When you think about it, everyday objects in a modern smart home process a lot of data that you probably don't wish to share with all and sundry.

Your thermostat, for example, could give clues about when you are away from home. Your fitness equipment often stores health information about you and your family.

And as an American software developer recently demonstrated—your smart speaker may have security holes that allow eavesdropping on your private conversations.

In the wrong hands, this is information can be misused for everything from burglary to identity theft and extortion. Smart devices are increasingly finding their way into large companies and government institutions, a trend that does not exactly make the situation any less serious.

Automating ethical hacking looks more promising

The work of uncovering security holes in computer systems is today largely carried out manually by so-called penetration testers or ethical hackers. This is time-consuming and expensive work, and the results entirely depend on the individual tester's expertise.

Many people have therefore wanted to automate the process. This goal has turned out to be a far more difficult task than imagined— especially in connection with smart devices.

Researchers from NTNU in Gjøvik recently published an article in the journal *Sensors*. In addition to reporting on their progress in automating security testing on smart devices, the researchers also revealed that critical devices in maritime shipping are still being manufactured with well-known security holes.

Multitude of smart devices complicate matters

Security testing of smart devices is in principle no different than testing any other computer system. The problem with the smart devices is their vast number of different applications. The technologies can vary considerably, and often they have very different areas of use.

"A smart speaker has been created with completely different tasks in mind than a smart thermostat. Its vulnerabilities may be linked to its own completely unique functions, sensors or other components that a smart thermostat does not have," says Basel Katt, an associate professor at NTNU's Department of Information Security and Communication Technology in Gjøvik.

"Smart devices use a lot of different protocols," says the researcher, "and they have many sets of specific rules to communicate between the computer systems."

The tools that have been developed to automatically test security so far have therefore been of limited use on smart devices. They have mostly been used for very specific tasks, usually only as part of an otherwise manual process, and have not performed nearly as well as human testers.

The NTNU researchers have developed a system that draws from several existing tools and combines them in coordinated simulation attacks on smart devices.

They have developed an independent software agent based on previous work by Fartein Lemjan Færøy, postdoc Muhammad Mudassar Yamin and Katt.

An independent software agent is a computer program that reacts to changes and events in the environment it is in, completely independently of direct instructions from humans. Instead, it acts according to a predetermined decision model. The model in question in this case was developed by Yamin and Katt to specify a software agent's behavior, especially in cyber ranges.

Cyber range—for training

Let us explain: A cyber range is an virtual training arena that gives users and systems the opportunity to test themselves against simulated computer attacks under controlled conditions, not unlike a military training ground.

Katt explains that an automated testing system could cover several roles in a cyber range and potentially make such exercises less time- and resource-consuming.

He further believes that such a system could be of great use both in developing and producing new smart devices, as well as in teaching and research.

"The testing system can demonstrate different ways of hacking and how vulnerabilities can be exploited," Katt says. "It can also be used to show students the consequences of various vulnerabilities."

Put device out of play

The researchers describe in their technical article how they try out their automated test system on an AIS unit. AIS stands for "automatic identification system." This is a widely used technology in shipping that communicates important information about vessels to the Norwegian Coastal Administration and other ships and ports in the vicinity.

Many Norwegian leisure boats are equipped with AIS transmitters, and the technology is required on board larger vessels, such as yachts, cruise ships and cargo ships. The transmitters must also be operational at all times.

"Just figuring out that the automated test system could relatively easily disable an expensive and widely used AIS system was a major discovery in itself," says Katt.

The severity level increased considerably when the researchers found that the connection could also be "spoofed."

Spoofing is when a person or computer program pretends to be someone else by using falsified data. In a maritime context, this could take the form of someone sending out false GPS signals via the AIS system. Worst case scenarios could lead to grounding or colliding with other ships or ports.

The manufacturer of the AIS product in question could probably have caught and rectified the weakness long ago if they had had access to a similar test system during the development and production phase.

Still a way to go

Despite the promising results, Katt emphasizes that the work on automating ethical hacking in smart devices is far from finished.

"Significant progress still needs to be made in working with information exchange across different protocols, in order to develop a fully functional system that can uncover security holes in smart devices with minimal human intervention," says Katt.

More information: Fartein Færøy et al, Automatic Verification and Execution of Cyber Attack on IoT Devices, *Sensors* (2023). DOI: 10.3390/s23020733

Provided by Norwegian University of Science and Technology

Citation: When your house spreads gossip about you (2023, May 2) retrieved 27 April 2024 from https://techxplore.com/news/2023-05-house-gossip.html