Hacking cybersecurity to anticipate attacks

August 8 2017, by Allie Nicodemo

Imagine two groups at war. One defends every attack as it comes. The other anticipates threats before they happen. Which is more likely to win?

In cybersecurity, understanding the potential for attacks is critical. This is especially true for mobile and wireless devices, since they are constantly connected and continuously streaming and collecting data.

"We have these devices with us all the time. We trust them with many things—with the microphone they can hear us, with the camera they can see everything, we put all our pictures there. Our lives are on these devices," said Guevara Noubir, professor in the College of Computer and Information Science.

Noubir recently organized the 2017 Conference on Security and Privacy in Wireless and Mobile Networks, hosted at Northeastern in July. The conference included some of the foremost experts in mobile security. One of the keynote speakers, Silvio Micali, is a winner of the Turing award, which is widely recognized as the "Nobel Prize" of computer science.

Researchers and students from all over the world convened at the conference to discuss mobile and wireless security, an area of cybersecurity Noubir says is "booming." They shared new research, held tutorials, and listened to some of the brightest minds in the field debate one of society's most pressing challenges.

The importance of reproducibility

As the organizer of the conference, Noubir implemented a new feature this year—the reproducibility label. Reproducibility—the premise that all studies should be replicable—is at the core of all good science. But Noubir explains that in wireless research, studies can be especially difficult to replicate, even if researchers provide every detail of how they conducted an experiment. That's because unbeknownst to them, there are often other factors at play. For example, if a car drives by as one device is measuring the activity of another, signals from the car's computer system might subtly interfere with the measurement.

To check reproducibility, Noubir provided conference participants with a software program that employs a "virtual machine" that analyzes all the data, graphs, charts, and tables in a study and tries to reproduce them. Of the 26 papers submitted to the virtual machine, only six of them were granted the reproducibility label, which underscores how challenging wireless studies can be to replicate.

One of the papers that achieved the reproducibility label involved smartphone jamming. In mobile security, jamming means blocking communication. The researchers in this study showed that with a combination of tools, they could remotely gain access to a cellphone's computer chip and and modify the Wi-Fi chipset code to transmit radio jamming signals. The signals can block other targeted devices or applications from sending or receiving data.

Researchers carried out this project as a way of anticipating a potential cyberattack.

"You want to understand what is possible so you can defend against these kinds of things" Noubir said. "You have to also ask yourself, 'what could someone do?'"

Self-authentication still a major cybersecurity challenge

In his keynote speech at the conference, John Manferdelli, director of the Northeastern University Cybersecurity and Privacy Institute, recalled the early 2000s when he worked at some of the country's largest technology companies. He remembers telling leaders at many companies that there were serious security flaws in many of the systems the companies were building. But many of those leaders weren't worried. They acknowledged there might be risks, but said it didn't matter because nobody knew about them.

"I was incensed," said Manferdelli. And for good reason. Not long after his warning, various cyberattacks made it clear that people were not only finding the vulnerabilities, but exploiting them. After that, companies changed their tune. They decided to fix some security flaws—but only those they knew had been exploited.

Of course, that wasn't enough. New attacks sprang up, often getting more creative and advanced. Eventually, tech companies started to realize they had to anticipate exploitation and protect against attacks before they occurred.

Fast-forward to 2017, and massive cyberattacks have already plagued the first half of the year. They range from the hacked emails of political leaders, to ransomware targeting utility companies, to stolen CIA documents. "I don't have to argue quite as much anymore that cybersecurity is important," Manferdelli said.

One of the biggest pitfalls of internet security is that people authenticate themselves online with passwords. "Everybody knows that's a disaster," Manferdelli said. "Once I know your password, I can masquerade for

you anywhere."

Even though websites have required passwords to be increasingly long and complex, most of them are still relatively easy for a hacker to guess. And once a single employee's account has been compromised, the entire company they work for could be at risk.

Manferdelli said another major challenge is that unlike the physical world, a virtual security breach is rarely immediately obvious.

"You have a really good sense that your apartment is safe and hasn't been broken into. I'd like that same thing to happen on computers," Manferdelli said.

But hackers are tricky. When they can't break into a person's device or information directly, they exploit side channels. For example, electromagnetic radiation emanating from a device can reveal a person's location, even if no one has actually hacked the person's phone.

With more than 4.8 billion mobile subscribers and 275,000 different apps available, there are plenty of opportunities for security and privacy breaches. And in the wireless world, they are typically not isolated to one feature of the phone, tablet, or computer. A cyber-assault can infect the entire machine.

"It's not like a car where the broken door affects just the door," Manferdelli says. "The broken door affects your steering."

More information: DOI: 10.1145/3100000/3098253

Provided by Northeastern University