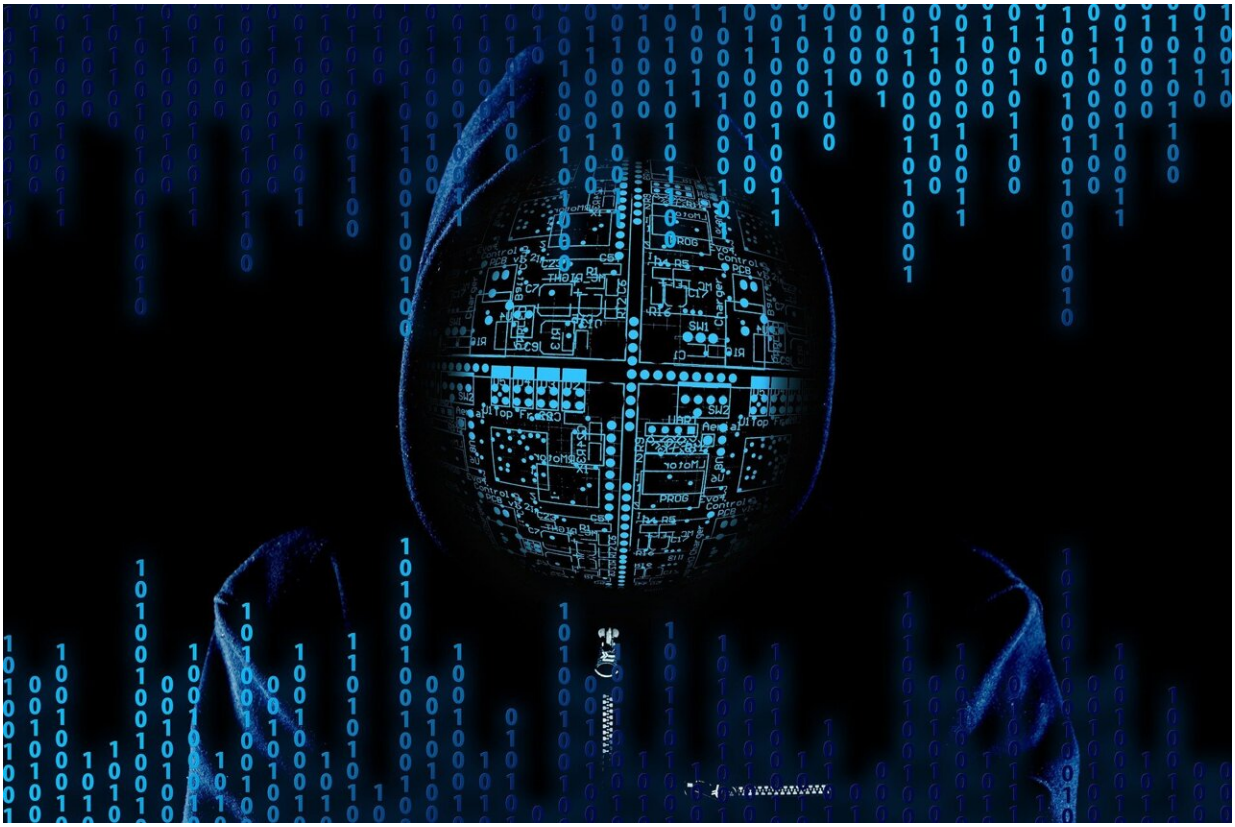
Securing systems from cyber-physical system hackers

June 2 2022, by Brandie Jefferson



Credit: Pixabay/CC0 Public Domain

When it comes to computer security, there are three main objectives: confidentiality—ensuring no one can steal your data; integrity—ensuring that your data has not been changed in any unauthorized way; and

availability—making sure that you have access to the resources you need to do what you need to do.

Most research focuses on the first two, said Ning Zhang, assistant professor of computer science and engineering at the McKelvey School of Engineering at Washington University in St. Louis. It's easy to see why. "If you are stopping me from using my credit card, that's fine. It's not as bad as if it were stolen and used by a thief," he said, but what about when it comes to a self-driving car that's barreling down a pothole-riddled road at 80 mph surrounded by other vehicles doing the same? In that situation, a little access—to the brakes, maybe?—would come in handy.

Zhang's student presented research at the 43rd IEEE Symposium on Security and Privacy in San Francisco, May 23-25, which outlined a new framework for system availability in cyber-physical systems such as self-driving cars. It ensures the user has availability assurance to some of the mission controls so that, in the event of a cyber attack, the system remains safe.

The method Zhang outlined relies on two principles, isolation between critical and non-critical components and complete mediation over critical system resources. In order to keep critical components out of a hacker's reach, it needs to be isolated from the rest of complex system. "It's like a fortified castle," Zhang said, referring to the isolated environment where computers keep potentially dangerous software away from its critical components.

In order to keep the trusted computing base small, this trusted execution environment maintains a very narrow bit of functionality for the cyber-physical system, such as the ability to brake, or disengage the gas or maybe to turn the wheel a little. These functionalities remain accessible to the vehicle's operator even if the car's operating system is under

attack.

Maintaining availability is not a trivial matter; after all, the operating system is controlling everything in the car. "If the system is being controlled by a hacker," Zhang said, "then of course it's not going to give you control."

That's where attack surface reduction comes in order to limit the points at which an attacker can impact the trusted environment via its influence over the operating system. To do this, the trusted environment will only respond to a particular set of commands. If the request falls outside those commands, access is denied.

This process is known as a reference monitor, and it works in two parts. "First, for example, I tell you, "You can only write me letters. No calls. No emails. No texts,'" Zhang said. If you send an email, it gets deleted without even being read.

"Once I do get a letter, it's only allowed to make certain requests," he said. Turning left or right may be acceptable, "But if you request anything else? I'm kicking you out." No access.

After that, there might be a parameter for how many degrees the wheel can turn, for how long the wheel can stay in that position and so on. The information needs to come from a certain place and the request needs to fall within certain parameters to get access to this limited functionality.

"Because they interact with the physical environment, cyber-physical systems must ensure real-time performance of computational tasks such as controllers," said Chenyang Lu, the Fullgraf Professor of computer science and engineering and an author on the paper.

"Traditionally, this is achieved by a real-time scheduler in the operating

system, which, however, may be comprised. A key advancement of RT-TEE is providing a secure real-time scheduling framework that maintains real-time performance guarantees to safety-critical tasks even when the rest of the system is compromised," Lu said.

The idea that someone's car might be hacked isn't a concern for a far-off future. It has been done before. Zhang says that for self-driving cars—and all cyber-physical systems—it's crucial that the third pillar of security—availability— is also protected.

"When it comes to the safety of critical systems I develop, I ask, 'Would I be willing to sit in a car with such an advanced hacker attacking the car?' If I wouldn't, then I'm not doing a good job."

More information: 43rd IEEE Symposium on Security and Privacy

Provided by Washington University in St. Louis