Critical infrastructure systems are vulnerable to a new kind of cyberattack

February 29 2024

Credit: Pixabay/CC0 Public Domain

In recent years, browser and web-based technology has become a powerful tool for operators of infrastructure and industrial systems. But it also has opened a new pathway for bad actors to seize control of these systems, potentially endangering critical power, water, and other infrastructure.

Georgia Tech researchers have found a way to hijack the computers that control these physical systems. Called programmable logic controllers (PLCs), they increasingly have embedded webservers and are accessed on site via web browsers. Attackers can exploit this approach and gain full access to the system.

That means they could spin motors out of control, shut off power relays or water pumps, disrupt internet or telephone communication, or steal critical information. They could even launch weapons—or stop the launch of weapons.

"We think there is an entirely new class of PLC malware that's just waiting to happen. We're calling it web-based PLC malware. And it gives you full device and physical process control," said Ryan Pickren, a Ph.D. student in the School of Electrical and Computer Engineering (ECE) and the lead author of a new study describing the malware and its implications.

The research team will present their findings Feb. 29 at the 2024 Network and Distributed Systems Security Symposium.

Provided by Georgia Institute of Technology

Citation: Critical infrastructure systems are vulnerable to a new kind of cyberattack (2024, February 29) retrieved 9 May 2024 from https://techxplore.com/news/2024-02-critical-infrastructure-vulnerable-kind-cyberattack.html