Device 'fingerprints' could help protect power grid, other industrial systems

February 29 2016

Georgia Tech researchers have developed a device fingerprinting technique that could improve the security of the electrical grid and other industrial systems. The system would be used in electrical substations like this one. Credit: Fitrah Hamid, Georgia Tech

Human voices are individually recognizable because they're generated by

the unique components of each person's voice box, pharynx, esophagus and other physical structures.

Researchers are using the same principle to identify devices on electrical grid control networks, using their unique electronic "voices" - fingerprints produced by the devices' individual physical characteristics - to determine which signals are legitimate and which signals might be from attackers. A similar approach could also be used to protect networked industrial control systems in oil and gas refineries, manufacturing facilities, wastewater treatment plants and other critical industrial systems.

The research, reported February 23 at the Network and Distributed System Security Symposium in San Diego, was supported in part by the National Science Foundation (NSF). While device fingerprinting isn't a complete solution in itself, the technique could help address the unique security challenges of the electrical grid and other cyber-physical systems. The approach has been successfully tested in two electrical substations.

"We have developed fingerprinting techniques that work together to protect various operations of the power grid to prevent or minimize spoofing of packets that could be injected to produce false data or false control commands into the system," said Raheem Beyah, an associate professor in the School of Electrical and Computer Engineering at the Georgia Institute of Technology. "This is the first technique that can passively fingerprint different devices that are part of critical infrastructure networks. We believe it can be used to significantly improve the security of the grid and other networks."

Georgia Tech researchers have developed a device fingerprinting technique that could improve the security of the electrical grid and other industrial systems. The system would be used in electrical substations like this one. Credit: Fitrah Hamid, Georgia Tech

The networked systems controlling the U.S. electrical grid and other industrial systems often lack the ability to run modern encryption and authentication systems, and the legacy systems connected to them were never designed for networked security. Because they are distributed around the country, often in remote areas, the systems are also difficult to update using the "patching" techniques common in computer networks. And on the electric grid, keeping the power on is a priority, so security can't cause delays or shutdowns.

"The stakes are extremely high, but the systems are very different from home or office computer networks," said Beyah. "It is critical that we secure these systems against attackers who may introduce false data or issue malicious commands."

Beyah, his students, and colleagues in Georgia Tech's George W. Woodruff School of Mechanical Engineering set out to develop security techniques that take advantage of the unique physical properties of the grid and the consistent type of operations that take place there.

For instance, control devices used in the power grid produce signals that are distinctive because of their unique physical configurations and compositions. Security devices listening to signals traversing the grid's control systems can differentiate between these legitimate devices and signals produced by equipment that's not part of the system.

Another aspect of the work takes advantage of simple physics. Devices such as circuit breakers and electrical protection systems can be told to open or close remotely, and they then report on the actions they've taken. The time required to open a breaker or a valve is determined by the physical properties of the device. If an acknowledgement arrives too soon after the command is issued - less time than it would take for a breaker or valve to open, for instance - the security system could suspect spoofing, Beyah explained.

To develop the device fingerprints, the researchers, including mechanical engineering assistant professor Jonathan Rogers, have built computer models of utility grid devices to understand how they operate. Information to build the models came from "black box" techniques - watching the information that goes into and out of the system - and "white box" techniques that utilize schematics or physical access to the systems.

"Device fingerprinting is a unique signature that indicates the identity of a specific device, or device type, or an action associated with that device type," Beyah explained. "We can use physics and mathematics to analyze and build a model using first principles based on the devices themselves. Schematics and specifications allow us to determine how the devices are actually operating."

The researchers have demonstrated the technique on two electrical substations, and plan to continue refining it until it becomes close to 100 percent accurate. Their current technique addresses the protocol used for more than half of the devices on the electrical grid, and future work will include examining application of the method to other protocols.

Because they also include devices with measurable physical properties, Beyah believes the approach could have broad application to securing industrial control systems used in manufacturing, oil and gas refining, wastewater treatment and other industries. Beyond industrial controls, the principle could also apply to the Internet of Things (IoT), where the devices being controlled have specific signatures related to switching them on and off.

"All of these IoT devices will be doing physical things, such as turning your air-conditioning on or off," Beyah said. "There will be a physical action occurring, which is similar to what we have studied with valves and actuators."

More information: David Formby, Preethi Srinivasan, Andrew Leonard, Jonathan Rogers and Raheem Beyah, "Who's in Control of Your Control System? Device Fingerprinting for Cyber-Physical Systems," (NDSS 2016). DOI: 10.14722/ndss.2016.23142.

Provided by Georgia Institute of Technology