OpDefender security system from INL protects computer-controlled industrial networks from cyberattacks

Idaho National Laboratory

Researchers from Idaho National Laboratory have engineered a technology that can protect utilities and other users of computer-controlled industrial systems from cyberattacks.

The effort was inspired by years of assessments showing that industrial control systems (ICS) are vulnerable to cyberattack, with unauthorized commands posing a particularly insidious threat since they're relatively easy to perpetrate and difficult to block. Attackers with the right level of knowledge and access can have a major effect on a power grid, for example, using the same software and commands that the grid's legitimate operators would use.

Called OpDefender, the new patent-pending technology consists of two main components: a network switching appliance and a network human-machine interface (HMI).

The network switching appliance can serve as a drop-in replacement for a typical network switch, or it can be used in conjunction with existing network switches. It protects ICS from cyberattack by adding intelligence to the network switch to make it ICS-aware.

OpDefender is configured and controlled in real time via a custom-built, web-based HMI designed with the operator in mind. It is secured using strong public-key encryption technology (RSA certificates) that allows for mutual authentication only between hosts that have the correct certificate installed. This helps ensure that an attacker can't compromise the control channel to enable communications without the operator's knowledge or consent.

OpDefender starts with the premise that no device on a control system network can be trusted. It operates under whitelisting rules, meaning that no device is allowed to communicate on the network until the OpDefender is configured to allow that device. Any data transmitted by a device that is not already whitelisted triggers an alarm, alerting operators of a rogue device on the network.

Once a device is allowed on the network, then the protocols and specific commands it can receive are further whitelisted. By default, OpDefender limits network traffic to the most basic communication, which in most cases consists almost exclusively of status requests from one or more operator workstations to field devices that are installed throughout a plant, utility or other system.

Above: OpDefender network switching appliance.

Above: OpDefender human-machine interface (HMI).

OpDefender's efficacy was demonstrated during a recent full-scale test at Idaho National Laboratory's Critical Infrastructure Test Range, cybersecurity researchers launched 14 different novel attacks at a system protected by OpDefender. The attacks targeted multiple different control devices from multiple vendors. OpDefender blocked each of these attacks and generated alarms for each, alerting the operator that an attack was taking place.

OpDefender is currently at a Technology Readiness Level 6, meaning it has a fully functional prototype or representational model. Additional work is needed to make it commercially viable, but results to date show that it could make a difference in the fight to secure industrial control systems.