A new defense for Navy ships: Protection from cyber attacks

September 17 2015

Sailors monitor ship propulsion and fuel levels in an enclosed operating station aboard the amphibious dock landing ship USS Harpers Ferry (LSD 49). The Office of Naval Research is developing cyber protections for shipboard mechanical systems like this. Credit: (US Navy photo by Mass Communication Specialist 3rd Class Mark El-Rayes/Released)

For most people, the term "cyber security" calls to mind stories of data theft like the recent hacks of the OPM database, or network spying like the 2012 breach of the Navy-Marine Corps Intranet.

But in this networked world, hackers might also try to disable or take control of machines in our physical world—from large systems like electric power grids and industrial plants, to transportations assets like cars, trains, planes or even ships at sea.

In response, the U.S. Navy is developing the Resilient Hull, Mechanical, and Electrical Security (RHIMES) system, a cyber protection system designed to make its shipboard mechanical and electrical control systems resilient to cyber attacks.

"The purpose of RHIMES is to enable us to fight through a cyber attack," said Chief of Naval Research Rear Adm. Mat Winter. "This technology will help the Navy protect its shipboard physical systems, but it may also have important applications to protecting our nation's physical infrastructure."

Dr. Ryan Craven, a program officer of the Cyber Security and Complex Software Systems Program in the Mathematics Computer and Information Sciences Division of the Office of Naval Research, explained that RHIMES is designed to prevent an attacker from disabling or taking control of programmable logic controllers—the hardware components that interface with physical systems on the ship.

"Some examples of the types of shipboard systems that RHIMES is looking to protect include damage control and firefighting, anchoring, climate control, electric power, hydraulics, steering and engine control," explained Craven. "It essentially touches all parts of the ship."

Attacks on mechanical systems that are operated by computers have

happened before. Stuxnet, the famous industrial "computer worm" discovered in 2010 was designed to attack controllers of Iranian centrifuges, causing the centrifuges to run at very high speeds, effectively tearing themselves apart.

"Another powerful example is the hacking of a German steel mill in 2014," Craven said. "The hackers reportedly got in and overheated a blast furnace, and even made it so that the plant workers couldn't properly shut down the furnace, causing massive damage to the system."

Traditionally, computer security systems protect against previously identified malicious code. When new threats appear, security firms have to update their databases and issue new signatures. Because security companies react to the appearance of new threats, they are always one step behind. Plus, a hacker can make small changes to their virus to avoid being detected by a signature.

"Instead, RHIMES relies on advanced cyber resiliency techniques to introduce diversity and stop entire classes of attacks at once," Craven said. Most physical controllers have redundant backups in place that have the same core programming, he explained. These backups allow the system to remain operational in the event of a controller failure. But without diversity in their programming, if one gets hacked, they all get hacked.

"Functionally, all of the controllers do the same thing, but RHIMES introduces diversity via a slightly different implementation for each controller's program," Craven explained. "In the event of a cyber attack, RHIMES makes it so that a different hack is required to exploit each controller. The same exact exploit can't be used against more than one controller."

This work aligns with higher level strategic guidance to protect against

cyber threats, like the U.S. Navy's "Cyber Power 2020," but the technology may also have benefits outside of the Navy.

"Vulnerabilities exist wherever computing intersects with the physical world, such as in factories, cars and aircraft," Craven said, "and these vulnerabilities could potentially benefit from the same techniques for cyber resilience."

More information: www.opm.gov/cybersecurity

Provided by Office of Naval Research