Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.
NAVSEA #2020-0408

Topic # N181-035
Network Traffic Analysis for Cybersecurity for Navy Industrial Control Systems
Fortiphyd Logic Inc

WHO

SYSCOM: NAVSEA

Sponsoring Program: NAVSEA HQ/DIR

Transition Target: TBD

TPOC:
(202)781-6731

Other transition opportunities: This technology can help secure industrial control system networks throughout the Navy, Department of Defense, and private sector operating the nation's critical infrastructure.

Photo Courtesy of US Navy, 180927-N-JS205-0002.JPG

Notes: Fortiphyd Logic was founded by Georgia Tech researchers to provide innovative cybersecurity solutions for industrial control system (ICS) networks.

WHAT

Operational Need and Improvement:
Industrial control system (ICS) networks are the foundation of the nation's critical infrastructure as well as the heart of a ship at sea, controlling the power distribution, steering and propulsion, and engine cooling systems. However, ICS networks cannot be properly secured through traditional cybersecurity solutions that do not speak obscure ICS protocols or understand the physics of the underlying process. An ICS network monitoring and intrusion detection solution is needed to alert operators of cyberattacks that threaten the safe operation of a ship's control systems.

Specifications Required:
The solution shall monitor and analyze ICS network traffic in real time to alert operators of cyberattacks that threaten the safe operation of the control systems. Anomalous behavior in both the cyber and physical realms should raise alerts to the operators, including suspicious commands and unusually large bandwidth usage as well as pump and valve failures.

Technology Developed:
Fortiphyd Logic developed a network monitoring and intrusion detection system to alert operators of anomalies in the network, controllers, and physics of an industrial control system. Our solution passively monitors ICS network traffic, parsing the obscure ICS protocols to look for abnormal commands and error messages as well as extracting physical process values and controller program behavior for deeper analysis. Machine learning algorithms then analyze the process values and controller behavior to alert operators of anomalies that could threaten the safety of the system.

Warfighter Value:
Fortiphyd Logic's patent-pending controller anomaly detection technology makes our solution the only one on the market capable of detecting attacks on industrial controllers from insiders with physical access, providing the best security against nation-state level adversaries. Operators also save time and money by detecting maintenance issues sooner to reduce unexpected downtime and by automating several ICS network management tasks.

WHEN

Contract Number: N68335-20-C-0125 **Ending on:** October 9, 2020

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Engine Cooling Testbed Demonstration	Med	Accurately detect anomalies in controller and physics of engine testbed	TRL 3	March 2020
Virtual Demonstration	Med	Accurately detect anomalies in controller and physics of virtual testbed	TRL 4	July 2020
Freshwater Generator Testbed Demonstration	Med	Accurately detect anomalies in controller and physics of freshwater generator testbed	TRL 5	October 2020
(If Option Exercised) Full Commercial Demonstration	Med	Accurately detect anomalies in controller and physics of commercial network	TRL 6	October 2021

HOW

Projected Business Model: Our business model is to sell our ICS network monitoring and intrusion detection solution directly to the Navy, DoD, and prime contractors who have ICS networks.

Company Objectives:
We are interested in making connections with Government and industry organizations who have critical ICS networks that are potential targets of nation-state level adversaries. Our short term objective is to earn a Phase III contract to deploy our ICS network security solution on a Navy ship. Meanwhile we are also looking to validate the technology in a wide range of commercial ICS networks including the power grid, water utilities, manufacturing, and petrochemicals. Long term we plan to fortify the nation's critical ICS networks by continuing to provide more secure network monitoring solutions and more effective virtual training.

Potential Commercial Applications:
This technology has a large commercial opportunity since it is directly applicable to all ICS networks, which range from the national power grid and water utilities down to escalators and roller coasters. However, the specific sectors that need it most are ones where cyberattacks have successfully caused physical consequences and continue to be the target of nation-state adversaries including the power grid, nuclear, and oil & gas.

Contact: David Formby, CEO/CTO
dformby@fortiphyd.com (803)645-0829