Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

NAVSEA #2020-0386

Topic # N16A-T013

Cyber Forensic Tool Kit for Machinery Control

TDI Technologies, Inc

WHO

SYSCOM: NAVSEA

Sponsoring Program: PEO Ships

Transition Target:

TPOC:

Other transition opportunities: Any platform vulnerable to Cyber attacks including any platform with SCADA Machinery Control Systems (MCSs): Ships, submarines, manufacturing facilities. Land or sea-based C4ISR systems.

Notes: Phase-II Option I was originally scheduled to end on 06/13/2020. Due to changes in work schedule and meetings from COVID-19, the project is currently under a No Cost Extension till 12/13/2020. Awaiting the next round of funding taking us into Phase-II Option-II, which will be the last year of performance.

https://www.navy.mil/view_image.asp?id=69987

WHAT

Operational Need and Improvement: Navy Machinery Controls Cybersecurity domain needs a solution with state of the art technology to defend against ever-evolving cyber threats. Vendor-locked proprietary solutions (both HW and SW) hinder the ready integration of existing cyberforensics solutions. Unique requirements of legacy and proprietary hardware (field devices) and software (OS, applications, comms protocols), within SCADA/DCS systems necessitate the development of an open architecture design in order to functionally test various tool components to be integrated into the CyFT framework.

Specifications Required: 1. Design Alternatives Modular vs Integral; 2. Solution Architecture Closed vs Open; 3. API Specifications Open Standard vs Custom; 4. Evaluation Models Formal/Abstract vs Simulation/Prototype; and 5. Tool Execution Memory Resident (e.g., Terminate & Stay Resident (TRS)) vs Disk Resident.

Technology Developed: Open Systems Architecture-based Cyber Forensics Toolkit (CyFT) Framework that is portable, lightweight and modular that allows the user plug-in support to live/memory forensics. This method allows for use on legacy systems without the need for expensive and time consuming hard/middle/software changes.

Warfighter Value: Incorporation of the Cyber Forensic Toolkit in the existing PLC helps alleviate future incidents and provides a real-time solution to combat cyber threats. This cost conscious tool saves the government time and money in assessing gap vulnerabilities and link to patches. This portable, lightweight solution does not require on site IT support staff.

WHEN

Contract Number: N68335-18-C-0282 **Ending on:** December 13, 2020

Milestone	Risk Level	Measure of Success	Ending TRL	Date
PLC/field-device memory acquisition and analysis	Low	Remote dump of PLC/field-device memory	6	April 2020
Inject malware (static-memory-exploits) into running PLC processor board	Med	Detection of malware in static memory	6	June 2020
Man-in-the-middle packet injection attack/detection	Low	Detection of altered command in memory	6	July 2020
Correlation of raw traffic and memory dump for malware analysis	Med	Link malware in raw traffic to malware in memory	5	December 2020
Inject malware (dynamic-memory-exploits) into running PLC processor board	Med	Detection of malware in dynamic memory	5	January 2021
Traffic and memory analysis using eBPFs	High	eBPF tools deployed on running system(s)	4	March 2021

HOW

Projected Business Model: Licensing software to various original equipment manufacturers and to be integrated into the program.

Company Objectives: TDI Technologies offers its customers technology-driven solutions focused around core competencies in research and development, cybersecurity, software development and engineering, and engineering services. TDI's objective is to meet with Program Managers in PEO Ships and Tech Warrant Holders at SEA 05 as well as system integrators to demonstrate how the tool kit defines and develops security and cyber-forensics ontologies that prevent future cyber threats by integrating CyFT in existing machinery-controls. This eliminates the need for expensive machinery-control recapitalization or purchasing proprietary information. TDI intends to exhibit this open architecture capability at government/industry sponsored events. TDI will license and support CyFT by leveraging commercialization in the automotive, energy and pharmaceutical industries to drive down the cost to the government.

Potential Commercial Applications: In addition to the current military application, this technology is applicable to cyber physical systems broadly spanning the domains of Transportation and Energy, with possible applications to Environment and Pharmaceutical industries. Current prime contractor, Fairmount Automation will be testing this technology in various machinery systems.

Contact: Dr. Avinash Srinivasan , Director - CyberOps & Forensics Solutions; Ph.D., CEH, CHFI
avinash@tditek.com (484) 473-1877