Department of the Navy SBIR/STTR Transition Program

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

NAVSEA #2019-0541

Topic # N171-056

Detecting Anomalies in Application Memory Space (DAAMS)

Charles River Analytics Inc.

WHO

SYSCOM: NAVSEA

Sponsoring Program: Program Executive Office Integrated Warfare Systems (PEO IWS) 1.0 – AEGIS Combat System; PEO IWS 10.0 – Ship Self Defense System (SSDS) Integrated Combat System

Transition Target: AEGIS Combat System; Ship Self Defense System (SSDS) Integrated Combat System

TPOC:
(540)653-6334

Other transition opportunities:
Product may be integrated into the Navy's embedded control systems for various ship-board naval applications or any number of military and commercial systems that must defend cyber physical systems from attack such as satellite (e.g. CubeSat), unmanned underwater vehicles, weapons systems, ISR platforms, avionics, and industrial control systems.

https://www.navy.mil/management/photodb/webphoto/web_160421-N-OR652-048.JPG

WHAT

Operational Need and Improvement: A major component of the combat systems cybersecurity Defense-in-Depth (DiD) strategy is the assurance of system integrity. DiD is an approach to defend systems by implementing multiple capabilities that detect and protect against multiple cyber attacks. An application's memory is one of many areas that can be exploited by a cyber-attack. The ability to monitor the overall integrity of the combat system is necessary to its ability to detect and respond to a cyber-attack. Combat system and computing memory is divided into the operating systems' kernel memory space and the application's memory space. There are current capabilities that make memory integrity cyber-attacks more difficult. There is an additional capability that monitors and detects kernel memory integrity violations. No capability exists that passively monitors and detects individual applications' memory integrity violations.

Specifications Required: The combat systems environment is defined as a real-time operating system with high availability requirements. The ability to monitor the integrity of an applications memory space would provide the combat system the ability to detect memory integrity attacks and respond to them. The innovative technology must have the ability to understand an application's memory space under normal conditions, to detect with minimal false positives when it is exploited via a cyber-attack against it, and to report those detections without impacting the performance of real-time applications being monitored. Developing this monitoring and detection capability for use within a combat system environment with little or no impact to the combat system will help ensure a more effective cybersecurity DiD strategy.

Technology Developed: DAAMS will provide attack-detection capabilities for applications' memory space that extend state-of-the-art anomaly detection techniques. We complement these anomaly detectors with an intelligent scenario generator that generates a representative range of scenarios and inputs for the application to create offline learning data that we use to train our system how to detect normal and abnormal memory behavior during operations. This approach lets DAAMS detect memory-space anomalies without affecting the application's mission-time performance.

Warfighter Value: The benefits of this capability will enable surface navy combat systems to field systems that are in a better position to endure a cyber-attack against an applications memory space. DAAMS will provide detection capabilities for a broad range of cyber attacks against applications.

WHEN

Contract Number: N68335-19-C-0085 **Ending on:** December 9, 2019

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Design and evaluate proof-of-concept prototype	N/A	Proof of concept of application memory monitoring and attack detection	3	February 2019
Develop and evaluate full-scope prototype in simulated environment	Med	Performance evaluation of monitoring and attack detection mechanisms	5	December 2019
Field test prototype on Navy platform in an operational scenario	High	Performance requirements met in an operational scenario	7	December 2020
Transition technology into Navy Program and/or integrate with commercial platform	Med	Operational requirements met in developmental test and evaluation	8	December 2021

HOW

Projected Business Model: Charles River has over 30 years of steady growth providing innovative, cost-effective solutions through intelligent systems R&D. Over 100 Charles River projects have produced a wealth of advanced-technology prototype software that can facilitate the rapid integration of critical technology into operational systems. Charles River will license DAAMS technology to large system integrators and integrate into Navy platforms, such as ship-based weapon systems and embedded control systems. Once integrated, Charles River will provide users with full documentation on how to use features of DAAMS. For example, we have licensed our VisionKit ®, partly funded by DoD and NASA SBIRs, to developers of image and video analysis solutions.

Company Objectives: Cyber security, system resilience, and machine learning are core business areas for Charles River, making the success of this effort fall squarely within our corporate interests and competencies. Charles River expertise will ensure the success of the innovations developed under the DAAMS program beyond the SBIR contract. In particular, Charles River plans to pursue a multi-part plan to transition this technology to the U.S. Navy and other U.S. Government customers, as well as provide benefits to commercial markets and customers seeking to enhance security and resilience of IT systems.

Potential Commercial Applications: The ability to define and monitor an application's memory integrity should be able to support any computing environment. In the commercial sector, just the like in the combat system environment, companies are seeking development of cybersecurity Defense-in-Depth (DiD) strategies to defend their systems against cyber-attacks. These systems consist of various components including networks, operating systems, and applications. There are various types of cyber-attacks that target the memory space used by applications. Just as the combat systems DiD will benefit from the ability to monitor its application memory's cyber health, so would commercial sector systems.

Contact: Gerald Fry, Scientist
gfry@cra.com (617) 491-3474 x538