Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.
ONR Approval #Not Approved-Pending ONR Release Authorization

Topic # N152-120
Binary code Randomization for Attack Sensitive Software (BRASS)
Intelligent Automation, Inc.

WHO

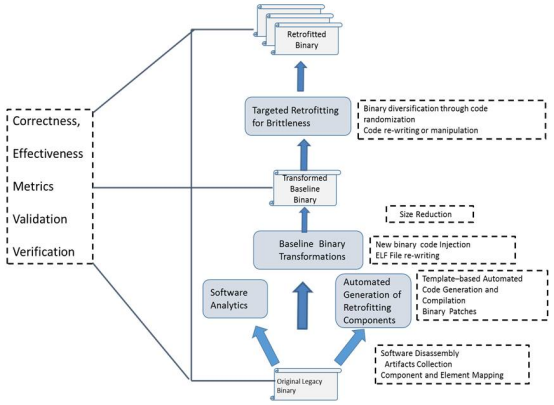
SYSCOM: ONR

Sponsoring Program: PEO-SHIPS, PEO-C4I, PMW-13

Transition Target: The Resilient Hull, Mechanical, and Electrical Security (RHIMES) system.

TPOC:
Dr. Dan Koller
daniel.koller@navy.mil

Other transition opportunities:
NAVAIR Systems Command, Naval Sea Systems Command, US Fleet Cyber Command



WHAT

Operational Need and Improvement: Navy is looking to develop transformation mechanisms that can be applied to software to increase software brittleness and achieve "fast-crash" property where successful attacks/compromises will cause the software to cease operating rather than continuing to operate in an unsafe or compromised state. The aim for the fast-crash to be automatically triggered when program control is lost due to a cyber-attack. The faster failure and timely switch-over would minimize the disruption/damage and actually enhance overall resilience in situations when diversified backup systems are readily available

Specifications Required: (i)Binary code transformation methods are generic and uniformed across each supported software architecture (ARM, MIPS, PowerPC, Intel). (ii) BRASS enhances 3rd party legacy software with the "fast-crash" property which guarantees that cyber-attacks/compromises will cause the software to cease operating rather than continuing to operate in an unsafe state. (iii) BRASS operates on binary code only and does not require source or compiling information.(iv) Functionality of the original targeted software is preserved with a small computational overheads (performance: < 3%, size < 6%).

Technology Developed: BRASS system automatically applies novel binary code randomization and transformation techniques to legacy software, in order to achieve "fast-crash" property of prompt execution termination in cases of cyber-attacks which might cause the compromised software to operate in some unsafe state. BRASS approach features an architecture that offers transparent and automatic binary code diversification that guarantees that a generated binary software variance would terminate quickly and consistently when under a cyber-attack.

Warfighter Value: BRASS will provide warfighters with the ability to transform and diversify a binary software code for the purpose of cyber-protection of cyber-physical systems. Especially beneficial in operational environments where: (i) operating legacy software with a long lifespan, source code and development infrastructure is not available; (ii)mission critical software infrastructure is under APT threat and software integrity and confidentiality is more important than resiliency, e.g. operating in degraded and potentially compromised state is not allowed; (iii) BRASS-diversified backup software and redundant systems are readily available.

WHEN

Contract Number: N68335-17-C-0133 **Ending on:** March 28, 2019

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Initial prototype to prove the feasibility of the approach	High	Successful demonstration of fast-crash property	TRL 3	May 2016
Augmented BRASS prototype with the harness to measure the effectiveness against performance metrics .	Med	Minimums size and performance overhead	TRL 3	December 2016
Complete BRASS prototype with the demonstrable workflow on multiple software platforms against multiple types of cyber-attacks	Med	Successful demonstration of fast-crash property against multiple types of attacks, supported on multiple software platforms	TRL 4	March 2019
BRASS prototype augmented with user control, configuration and feedback capabilities	Med	Successful demonstration of fast-crash property in user-guided environment	TRL 5	June 2019
Support for Navy-relevant proprietary software/hardware platforms	Med	Successful demonstration of fast-crash property on the selected software platforms	TRL 6	June 2020

HOW

Projected Business Model:
IAI will investigate both inserting the technology into government programs and licensing the technology to a commercial partner. Raytheon Integrated Defense Systems is a strong potential transition partner due to their success and experience in cyber security, and software integration for the DoD and Intelligence Communities with the strong infrastructure resources, market presence, and domain expertise. Commercialization revenues may come from technology licensing to embedded software vendors and various government contractors, such as Raytheon, and, also product or services sales to various Fortune 1000 companies and government agencies that have made significant investments in software with a long life cycle.

Company Objectives:
IAI envisions developing BRASS technology as a part of multi-prong strategy aimed, in short-term at integrating BRASS in existing cyber- defense systems or a standalone tool for binary retrofitting of legacy software in post-production environment and, in long term as an essential part of IAI's multi-layer cyber-resilience solutions for cyber-physical and traditional computer systems.

Potential Commercial Applications:
BRASS has significant commercial potentials as a binary code transformation framework that can be applied to mission critical software systems operating in a hostile Internet environment. BRASS will target the market segments whereas integrity and confidentiality requirements are much more important than availability, and compromised or misbehaving software could be much more dangerous than simple unavailability. In such environments, redundant and diversified backup systems are readily available.

Contact: Gregory Briskin, Associate Director
gbriskin@i-a-i.com 301-294-4755