Department of the Navy SBIR/STTR Transition Program

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

ONR Approval #43-7504-20

Topic # N182-131

RedBox: Red Team in a Box

ObjectSecurity LLC

WHO

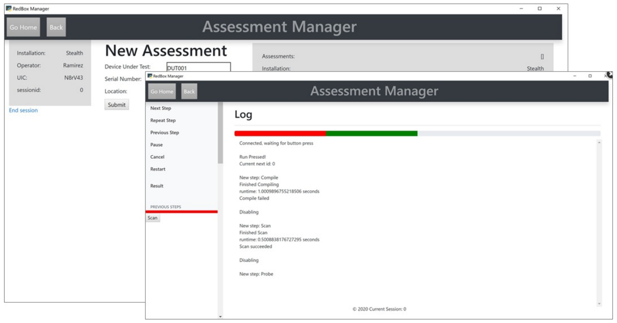
SYSCOM: ONR

Sponsoring Program: Resilient Hull, Mechanical, and Electrical Security (RHIMES) system, FNC

Transition Target:

TPOC:
Dr. Dan Koller
daniel.koller1@navy.mil

Other transition opportunities: The developed solution is general in nature and thus widely applicable across all services.



New Assessment

Installation: Stealth
Operator: Ramirez
UIC: N8rV43
sessionid: 0

Device Under Test: DUT001
Serial Number:
Location:

Assessments: []
Installation: Stealth

Log

```
Connected, waiting for button press

Run Pressed!
Current next id: 0

New step: Compile
Finished Compiling
runtime: 1.0009896755218506 seconds
Compile failed

Disabling

New step: Scan
Finished Scan
runtime: 0.5008838176727295 seconds
Scan succeeded

Disabling

New step: Probe
```

© 2020 Current Session: 0

RedBox UI and assessment log (Copyright 2020, ObjectSecurity LLC)

Notes: We are in discussions with the Philadelphia Navy Shipyard, Naval Air Warfare Center Aircraft Division, and Test Resource Management Center (TRMC).

Also ongoing discussions with Lockheed Martin, and commercial pilots;

We have a working prototype of RedBox that is being piloted;

We have a good customer track record - sample customers include: Navy (SPAWAR, ONR, NRL), General Electric, UCI Medical, Agilent, IBM, Boeing, DARPA, Army, Air Force (AFWERX, AFRL), Missile Defense Agency, NIST, Smartronics, QinetiQ, UK MOD, BAA Airports, Intel, ESG, SAP AG, Royal Bank of Scotland, HP, BMVIT, Twinsoft, Deutsche Telekom, European Space Agency (ESA), Lufthansa Systems, Eurocontrol, UL VS, Promia, RTI, Hornbach, Schoenhofer, and more.

WHAT

Operational Need and Improvement: The Navy's embedded (microelectronics) systems are not assessed at scale for software vulnerabilities because currently no portable, automated, easy-to-use, non-destructive, and offline tools are available for non-experts to test already-deployed systems. The Navy (and civilian government and industry) needs such a tool. In contrast, conventional software vulnerability assessment tools are often Software as a Service (SaaS) only, intended for manual use by experts, and focused on network vulnerabilities. Use case: A non-expert user can carry a "RedBox" device on board and plug it into embedded system. RedBox then automatically assesses the embedded system, and the user can view a "traffic light" (or advanced) report

Specifications Required: Portable software vulnerability assessment device that non-experts can carry on and around a site (e.g. ship) and connect to embedded systems (ES) via common connectors. It is automated, battery-powered, non-destructive, and does not require internet. Is usable by non-experts, and is able to assess ES without prior knowledge about the assessed ES.

Technology Developed: - Connect: to external connectors (D-Sub , USB , serial, SDcard), and internal UART/JTAG (Universal Async. Receiver/Transmitter, Joint Test Action Group) on the circuit board.
- Extract: gains access to the system (using basic automated pen-testing), ideally via a command shell. It then automatically extracts the firmware from the device.
- Analyze: the extracted firmware for known and zero-day vulnerabilities, including binary vulnerabilities assessments, decompiling or disassembling and analyzing the decompiled source. Results are aggregated, filtered, mapped to a standard, and prioritized by potential impact
- Report: simple user output on the device for non-experts (e.g. traffic light), and details are stored for further aggregation and analysis (and uploaded to a backend when RedBox has internet connection).
- Adapt: uses artificial intelligence (AI) to learn and adapt from every device analysis

Warfighter Value: Warfighters critically depend on equipment to work. Embedded systems (ES) drive most equipment. With the long lifecycles of Navy vehicles etc., most ES are already deployed and have initially often not been designed for be interconnected etc. (gao.gov/products/GAO-19-128). These already-deployed ES need to be analyzed for vulnerabilities, which requires a portable device that can handle non-mainstream/commercial systems.

WHEN

Contract Number: N68335-20-C-0094 **Ending on:** June 30, 2021

Milestone	Risk Level	Measure of Success	Ending TRL	Date
MVP	Med	Minimum Viable Product (MVP) works (prototype)	4	2nd QTR FY20
Base Working Prototype	Med	prototype works	4	3rd QTR FY21
Option I Working Prototype	Med	adv. prototype works	6	1st QTR FY23
Option II Working Prototype	Low	adv. prototype works	6	3rd QTR FY23

HOW

Projected Business Model: - sell (hardware + software) product direct (one-off) with ongoing maintenance contract (recurring), maybe also operate backend analytics (or assist prime/Navy to do that). Also potentially whitelabel
- integrate hardware (Commercial off the Shelf - COTS - computer/components) for the RedBox device
- also provide other business models, such as
    - RedBox with suitcase server for offloading
    - RedBox with SaaS offloading
    - Network-based vuln assessment (virtual/physical appliance)
    - "Freemium" SaaS with binary upload & result
    - Integration into Continuous Integration/Development (CI/CD) deployment pipelines
    - RedBox with specific device knowledge (w. manufacturer cooperation)
    - white label within other solutions

Company Objectives: 1) from FST program/events:
- pilot users/customers at Navy and primes
- gather feedback and market intel

2) Long-term:
- become a standalone vendor for RedBox at Navy and elsewhere. Product is ideally suited for that because it is not a component within a larger Navy platform, but can be independently sold/supported

Potential Commercial Applications: - same as for Navy
- more relevant: cloud/SaaS offerings that are faster and more convenient, because commercial applications are likely going to have internet
- tie into CI/CD deployment platforms and automatically test code before deployed on embedded systems.

Contact: Ulrich Lang, PhD, CEO
ulrich.lang@objectsecurity.com 6505153391