Department of the Navy SBIR/STTR Transition Program

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

ONR Approval #43-4388-18

Topic # N161-070

Retrofitting Code into Embedded Binaries

BlueRISC, Inc.

WHO

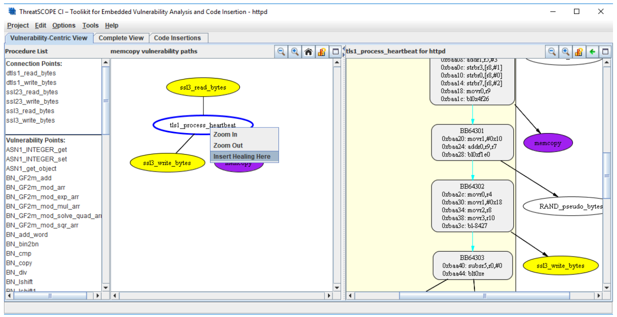
SYSCOM: ONR

Sponsoring Program: ONR Code 31

Transition Target: Resilient Hull/Infrastructure Mechanical & Electrical Security (RHIMES)

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

Other transition opportunities:
UAS's, Avionics, Critical infrastructure. In general, Navy and Department of Defense (DoD) programs with embedded software assurance and/or information assurance requirements.



```
Connection Points:
dtls1_read_bytes
dtls1_write_bytes
ssl23_read_bytes
ssl23_write_bytes
ssl3_read_bytes
ssl3_write_bytes
Vulnerability Points:
ASN1_INTEGER_get
ASN1_INTEGER_set
ASN1_get_object
BN_GF2m_add
BN_GF2m_mod_arr
BN_GF2m_mod_exp_arr
BN_GF2m_mod_mul_arr
BN_GF2m_mod_solve_quad_arr
BN_GF2m_mod_sqr_arr
BN_add_word
BN_bin2bn
BN_cmp
BN_copy
BN_div
BN_lshift
```

```
0xbaa0c: strbr3,[r8,#1]
0xbaa10: strbr0,[r8,#0]
0xbaa14: strbr7,[r8,#2]
0xbaa18: movr0,r9
0xbaa1c: bl0x4f26

BB64301
0xbaa20: movr1,#0x10
0xbaa24: addr0,r9,r7
0xbaa28: bl0xf1e0

BB64302
0xbaa2c: movr0,r4
0xbaa30: movr1,#0x18
0xbaa34: movr2,r8
0xbaa38: movr3,r10
0xbaa3c: bl-8427

BB64303
0xbaa40: subsr5,r0,#0
0xbaa44: blt0xe
```

Image courtesy of BlueRISC, Inc., Copyright 2018,

Notes: This image depicts the ThreatSCOPE Code Injection (CI) toolkit. On the left is a list of procedures/functions, extracted directly from an embedded executable, that contain vulnerability-relevant artifacts. The center panel shows a visualization of an identified exploitable path with the option to perform automated code insertion on this path. The right panel shows a detailed control-flow graph view of the selected procedure/function - fine-grain code insertion is possible in this panel. Upon insertion of the cyber hardening code via the user interface, the toolkit automatically generates an updated executable/image containing the inserted code and provides this as an output.

WHAT

Operational Need and Improvement: Effectively securing the growing array of embedded devices in use on military platforms is a critical challenge. Furthermore, embedded devices play a central role in critical infrastructure and control key mechanical systems in the industrial, energy, and transportation sectors. In such applications, errors and vulnerabilities in the software running on these devices can have devastating impacts due to their ability to cause failures in the physical world. ThreatSCOPE CI not only performs an automated vulnerability characterization of these embedded software components, without the requirement of source code, but also enables the user of the tool to insert functionality into the software for the purpose of cyber-hardening or otherwise (e.g. new functionality in legacy systems, etc.).

Specifications Required: Critical embedded systems must be hardened against cyber-attack. For many of these systems (e.g. legacy), source code and/or a relevant development environment is not easily obtainable. Additionally, the insertion of codes (for cyber-hardening or otherwise) can have an impact on performance which must be managed.

Technology Developed: ThreatSCOPE Code Injection (CI) is a binary-level, vulnerability analysis toolkit (i.e. no source code required) enabling automated insertion of code into embedded executables/firmware. It provides vulnerability and performance guidance for the insertion of generic and cyber-hardening codes via an interactive GUI. The tool ensures that the inserted code operates within the existing constraints of the embedded software maintaining intended functionality while minimizing performance overhead. ThreatSCOPE CI has been validated on real-world embedded firmware (e.g. Apache web server, avionics Operational Flight Program - OFP) and shown to enable the patching of identified vulnerabilities (e.g. Heartbleed).

Warfighter Value: ThreatSCOPE CI enables vulnerability analysis and cyber hardening of embedded software without the requirement of source code. The solution is directly applicable to a number of military and commercial embedded systems including unmanned systems (e.g. drones), avionics, industrial control systems as well as legacy embedded systems. ThreatSCOPE CI will give warfighter's assurance that mission-critical embedded systems can be hardened against malicious cyber-attacks while maintaining operational mission functions.

WHEN

Contract Number: N68335-17-C-0453 **Ending on:** October 31, 2019

Milestone	Risk Level	Measure of Success	Ending TRL	Date
SBIR Phase I proof-of-concept prototype demonstration	N/A	Proof-of-concept vulnerability analysis and cyber hardening via code injection in vulnerable Apache Web Server embedded executable	5	1st QTR FY17
ThreatSCOPE CI vulnerability characterization and generic code insertion support	Low	Prototype toolkit validated through test and evaluation	6	3rd QTR FY19
ThreatSCOPE CI UAS Demonstration	Med	Cyber hardening while maintaining functional correctness on a relevant embedded system application	7	1st QTR FY20
ThreatSCOPE CI Avionics OFP Demonstration	Med	Cyber operational requirements met in developmental test and evaluation of avionics system	8	1st QTR FY21
Transition solution into Navy/DoD program(s) and/or commercial offering	Med	Cyber operational requirements met in operational test and evaluation	9	1st QTR FY22

HOW

Projected Business Model: Since 2002, BlueRISC has worked with the government to provide innovative solutions to cutting-edge problems in the cyber-security space. BlueRISC will license the ThreatSCOPE CI toolkit to large system integrators for utilization with Navy and DoD platforms, such as unmanned aircraft, avionics systems and embedded control systems. BlueRISC will provide users with full documentation, as well as example use-cases, on how to use the ThreatSCOPE CI toolkit. BlueRISC has commercialized toolkits resulting from SBIR efforts in the past and will leverage its existing online and licensing infrastructure. These toolkits have been sold worldwide in more than 15 countries.

Company Objectives: Binary-level compilation, exploitability analysis and cyber-hardening are core competencies of BlueRISC, making this Navy effort align directly with its corporate direction. BlueRISC's expertise and relationships in these domains will ensure the success of the solution beyond this SBIR Phase II effort. BlueRISC will employ a multi-pronged strategy, via existing partnerships in the defense space, to transition the ThreatSCOPE CI toolkit to Navy programs as well as the broader DoD market. BlueRISC will also leverage existing relationships in the industrial control space (specifically the energy sector) to commercialize the tool outside of the government.

Potential Commercial Applications: ThreatSCOPE CI is expected to further the software assurance field by enabling the retrofitting of embedded firmware with cyber hardening codes at exploitability relevant locations. The project is an ideal fit for BlueRISC and will provide a strong opportunity to not only target government programs but to also transition the technology to the commercial sector, specifically targeting embedded systems. BlueRISC will target embedded systems in the commercial space (e.g. drones, Internet-of-Things - IoT, Industrial Control Systems - ICS, etc.) via a cloud-based rental model enabling broader adoption in an easy-to-use and cost-effective manner.

Contact: Kristopher Carver, Technical Director
kris@bluerisc.com (413) 359-0599