Department of the Navy SBIR/STTR Transition Program

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

ONR Approval #43-8627-21

Topic # N18A-T018

Protocol Feature Identification and Removal

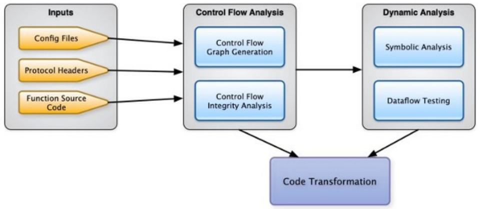
P&J Robinson Corporation

WHO

SYSCOM: ONR

Sponsoring Program: Total Platform Cyber Protection (TPCP) Innovative Naval Prototype (INP)

Transition Target: Endor Future Naval Capability (FNC) & Avalanche FNC. Additional transition opportunities with all Navy Government Off-The-Shelf (GOTS) and Commercial Off-The-Shelf (COTS) stand alone and enterprise software applications when security, efficiency and performance are key factors. Legacy systems are high value targets due to the difficulty in safely and effectively removing the features from the source code of the target protocol. These protocol features that are not enabled in a configuration need to be identified as potential targets and be disabled or removed.



Graphics Copyright 2021, P&J Robinson Corporation

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

Other transition opportunities: FNC Avalanche

Notes: Artus is Latin for "compaction" or "to make smaller" ArtusProtocol is part of a suite of products to remove bloat and unwanted features from software and protocols.

WHAT

Operational Need and Improvement: The Navy extensively leverages and adopts communication protocols and standards developed for commercial and public sectors. These standard, feature-rich protocols are often implemented as a one-size-fits-all library and are generally deployed as a whole. It is extremely rare that an application or even a set of applications within the computing system requires and invokes the entire feature set supported by a standard protocol. In most deployments, many features are not needed and are never invoked by the application(s). However, these extraneous, unnecessary features are invoke-able by an external party and represent an attack surface and risks that need not be incurred. The Navy would like to acquire the capability for modifying standard protocols it deploys for reducing the attack surface and limiting the risk exposure to only that of the protocol features that are essential to its application(s).

Specifications Required: Support protocol features necessary for correct communication of Navy application(s) and nothing else. All other protocol features should be removed from the protocol code/library. The core functionality of the protocol remains intact. The resulting protocol is still compatible with an external party communicating via the standard protocol. Software toolset does not require access to source code. Consultation with original software developers not required.

Technology Developed: ArtusProtocol, a fully functioning software toolset for identifying and tagging protocol features, allowing end users to selectively remove unwanted features and their corresponding code.

Warfighter Value: Warfighter's rely upon the accuracy and availability of information. Compromised software and data can be adversely affect outcome and even cost lives. Removing unwanted features, dead code and Cyber Vulnerabilities and Exposures (CVEs) can reduce the available attack surface while improving the simplicity, reliability and efficacy of software systems used by warfighters.

WHEN

Contract Number: N68335-19-C-0633 **Ending on:** August 19, 2021

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Phase II Base: Research & developement to show development progress towards successful prototype demo.	Med	Verified the Protocol Feature Identification tool, to include the Source Code Mapping as well as the transformation of Source Code.	4	4th QTR FY21
Phase II Option: Generalize and mature tools (not awarded yet)	Low	Continuation of Feature Identification and Source Code Mapping, integrate and test functions. Generate Control-Flow Graph of Modified and/or Removed Features	5/6	2nd QTR FY22
Phase III: Transition to Navy Command (not awarded yet)	Med	Provide Beta version of tool for use by Navy personnel and refine product for integration with exisitng orchestration and deployment tools	9	2nd QTR FY24

HOW

Projected Business Model: ArtusProtocol will be open source and PJR will offer a fully a supported version and services to facilitate integration with customer Continuous Integration and Continuous Development (CICD) models. PJR plans to leverage current existing Navy customers/contracts as well as developing new customer relationships. PJR will also reach out to existing partnerships with Large Systems Integrators (LSIs) to deliver on major programs. Since the relocation of corporate headquarters (HQ) to Boerne, Texas we will be targeting the Army Futures Command in Austin, TX in developing a new customer relationship. PJR also plans to develop delivery partners to rebadge/resell software licenses, and support agreements to their commercial and Government customers. PJR plans to offer Artus Protocol licenses for sale or software as a service along with installation and configuration services to ensure customer success. Customers can purchase a license outright or hire PJR or a delivery partner to use Artus Protocol on new versions and releases of the software.

Company Objectives: Objectives for the FST event include: lead generation, competitive research and partner development. The longer term goals for the Artus Protocol is to continue to build the Artus product suite including the ArtusJava. Artus will help PJR grow through additional revenue generated by support agreements and services. Indirectly, PJR will benefit from the competitive differentiation and "street-cred" gained as customers adopt and deploy software and protocols transformed via Artus tools.

Potential Commercial Applications: PJR is building the "To The Power of 5" suite to optimize customer software and networks thus providing the cyber security so necessary in securing their assets. PJR will offer these software and protocol transformation tools to commercial customers special focus on healthcare industry as well as the critical infrastructure of muncipalities and/or government-specifically the Supervisory Control and Data Acquisition (SCADA) systems.

Contact: Cindy McClister, Business Development Manager
cmcclister@pjrcorp.com 830-400-4133 ext 105