Topic: N162-073

WPL, Inc.

TEAM - Twice Encrypted and Authenticated Multicast

Twice Encrypted and Authentication Messaging (TEAM) is a device-independent software-based encryption capability supporting multi-cast that leverages approved capabilities for the protection of classified information developed by WPL, Inc. We are an engineering services and Research and Development (R&D) company founded in 1978 with extensive communications system and security engineering expertise. TEAM is targeted for the new Marine Air to Ground Task Force [MAGTF] Common Handheld (MCH) radio. TEAM's implementation adds limited overhead on multi-cast networks thereby maximizing bandwidth efficiency. A laboratory demonstration of a proof of concept was completed in Phase 2 and we are looking at future technology demonstrations with operational users through MARCORSYSCOM. Our goal is to deploy our software capability as part of new/existing platform and provide licensing/training support for its use.

Technology Category Alignment:

Trust Foundations
Networks and Communications
Scalable Teaming of Autonomous Systems
Guidance, Navigation & Control (GN&C) and Data Links

Contact:
Ryan Biondo
ryan.biondo@wpli.net
(443) 285-9874
http://wpli.net/
SYSCOM: MARCOR
Contract: M67854-18-C-6522

Room: FST at WEST 2020

Department of the Navy SBIR/STTR Transition Program

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

MCSC-PRR-3074

Topic # N162-073

TEAM: Twice Encrypted and Authentication Messaging

WPL, Inc.

WHO

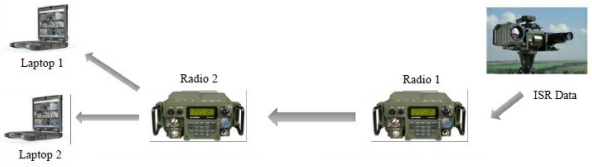
SYSCOM: MARCOR

Sponsoring Program:

Transition Target: MAGTF Common Handheld (MCH)

TPOC:
sbir.admin@usmc.mil

Other transition opportunities:
Information Assurance Specialists (IAS)
Aruba Federal
Silvus Technologies



Motivating Scenario for Deploying TEAM

Nearly any RF radio platform capability, including US Army radios and other tactical applications.

Notes: The scenario for deploying TEAM is an ad hoc, scalable network supporting many additional nodes, as required. By leveraging multicast protocols, we can provide secure transmissions with minimum bandwidth impacts due to encryption overhead.

WHAT

Operational Need and Improvement:
Develop Encryption Algorithms for Hand-held devices and Man-pack Radios. The encryption algorithm is to provide Commercial Solutions for Classified (CSfC) protection and integrity and confidentiality of transmitted information. The transmitted information will include Command and Control (C2) messages and Precision Location Information (PLI) for dismounted radios and tactical hand-held devices while providing the ability to be certified at the classified level, agnostic to the network used.

Specifications Required:
Solution must:
- provide the impact on the availability and throughput (rate of transmission) of messages
- provide integrity and confidentiality for all messages and protect classified information
- algorithms must meet the CSfC requirements for protection of classified information
- employ open architecture designs principles to protect an Internet Protocol (IP) message
- have an overhead < 6% when used in current Marine Corps systems for a 1 kilobyte message

Technology Developed:
A platform/device-independent software encryption capability supporting Multicast RF/terrestrial network communication security. Allows additional scaling of new/additional radios without adding significant overhead that would otherwise be introduced in a scaled unicast network architecture.

Warfighter Value:
- TEAM (Twice Encrypted & Authenticated Multicast) provides secure communications leveraging Suite B encryption; potential for CNSA Suite encryption support
- TEAM software encryption supports multicast network architectures
- TEAM maximizes user data throughput (6% bandwidth for encryption overhead)
- TEAM can be deployed on nearly any RF/terrestrial network
- TEAM is platform-independent (to include Android, Apple, or Linux)

WHEN

Contract Number: M67854-18-C-6522 **Ending on:** October 15, 2019

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Live demo of proof-of-concept prototype in emulated environment	Med	TEAM meets USMC overhead requirements	3	3rd QTR FY17
Beta release of scaled prototype software	Low	TEAM meets Government security requirements	4	3rd QTR FY19
Live demo of scaled prototype in Raspberry Pi network	Med	TEAM supports streaming multicast video in COTS devices	5	4th QTR FY19
Integration and demonstration in GOTS network	Med	TEAM can be integrated with MCH	6	3rd QTR FY20

HOW

Projected Business Model:
Software licensing or engineering training services support. We would like to license this capability to prime radio platform developers for integration and provide integration support, as required.

Company Objectives:
Ultimately, we are looking to deploy this capability to support MULTIPLE warfighter capability gaps when it comes to provided simplified encryption and handling on ad-hoc and multi-cast network architectures.

Potential Commercial Applications:
This technology could provide Communications Security (COMSEC) for radio frequency (RF) and terrestrial networks without relying on the handling and logistics of NSA Type-1 secure capabilities. This includes commercial or coalition users for which these capabilities are otherwise not available.

Contact: Ryan Biondo, Principal Engineer
ryan.biondo@wpli.net (443) 285-9874