2018 NDIA GROUND VEHICLE SYSTEMS ENGINEERING AND TECHNOLOGY SYMPOSIUM
Vehicle Electronics and Architecture (VEA) & Ground Systems Cyber Engineering (GSCE)
TECHNICAL SESSION
AUGUST 7-9, 2018 - NOVI, MICHIGAN

MICROTOKEN EXCHANGE (MTE) FOR SECURING DIGITAL DATA FROM CYBER WARFARE ATTACKS

Dariusz Mikulski, Ph.D.
CIV USARMY TARDEC (US)
Ground Vehicle Robotics (GVR)
Warren, Michigan
dariusz.g.mikulski.civ@mail.mil

Steven R. Russo
Executive Vice President
Eclypses Inc.
Colorado Springs, CO 80919
steven.russo@Eclypses.com

Abstract

New technological advancements call for innovative cybersecurity assurance measures in preventing increased vulnerabilities through cyber-attacks and cyber warfare. Current encryption processes are no longer failsafe in secure data management architectures, especially with accessibility to Advanced Encryption Algorithms (AES). Through new technological advancements, including informational technology architectures and autonomous vehicle implementation, it is imperative to provide new paradigms of security against cybersecurity breaches. In all realms of data usage, including the development of the Next Generation of military vehicles, the demand for significant preventative measures in cybersecurity assurance has dramatically increased. The matter of advanced need in cybersecurity can be established through the use of MicroToken Exchange™ (MTE). By way of MicroToken Exchange, it is possible to provide an additional robust layer of security that allows the right data, as well as ultra-secure command and control actions, to get to the right device, endpoint or End User Device (EUD), at the right time. Through MicroToken Exchange (MTE), operational changes are made to a sequence of digital data, which replaces the original data with new data or MicroTokens, prior to the streaming process; this process protects the data by replacing the real data with MicroTokens. By changing the data through the streaming process to MicroTokens rather than real data, the real data is then rendered inaccessible during the streaming process. When the MicroTokens reach their destination, they are then transformed for the device-- endpoint or EUD that the information was intended for--to execute a command. This added transformation layer inhibits non-authorized users to affect unauthorized actions to any paired End User Devices (EUDs). This process would provide the U.S. Army and U.S. Marine Corps with optimized effectiveness, efficiency and security in systems processing with MTE. MTE can be deployed on a one-to-one, one-to-many, and/or many-to-many ecosystem. Compatibility of this process is compliant with C, C++, and Java platforms, with possibilities of translation for multiple languages. MTE makes command data exploitation unassailable, as systems and connected devices remain unscathed, fully operational, stable, and secure by preventing these vulnerabilities. It is both unique and unparalleled in its design architecture. This paper provides more details on the process and the possibilities aligned with MTE's applications. In providing these details, this paper further converses how MTE can provide cybersecurity assurance to informational technology aspects of the military. Also, how to integrate into the Next Generation vehicles for protection against cyber-attacks and cyber warfare in autonomous systems. By providing these additional layers of security, MicroToken Exchange would support the mission of the U.S. Army and the U.S. Marine Corps. This would prevent unauthorized user access to all information and all autonomous controls, by removing the real data that typically passes through the streaming process. Utilization of MTE would also coincide with the military goal of using more Unified Capabilities (UC). By preventing data collection from unauthorized users, vulnerabilities decrease dramatically, security increases exponentially, mission effectiveness increases dramatically, and safety of this nation's business and warfighter communities are preserved in the cyber realm.

Introduction

In a world of interconnectivity comes the new responsibility of safeguarding our information. Technology, the need for speed, as well as, the vulnerabilities within networks, continue to grow exponentially. The development of a new platform for cyber-attacks and cyber warfare has complicated the dynamic of using these data networks in business and in warfighter communities. The typical solution for this thus far has been use of encryption and red-black engineering, which is traditionally followed by government and military information architect intervention. Due to the increased rates of speed and the multiplications of vulnerabilities these typical solutions are becoming less effective and less practical. These situations coupled with the ability to employ super computers on Advanced Encryption Algorithms (AES) and the perfect storm for cyber warfare suddenly exists.

Combat vehicle prototypes are focused on leap ahead technologies to support the mission. Ground Vehicle Robotic mid-term capabilities are set to improve the cybersecurity of unmanned systems. TARDEC Value Stream 1 Autonomy is one program that warrants 100% security need in its technological architecture. In this growth of technology, also comes the growth of responsible protection against cyber warfare attacks. Current data environments require data yet using the “real” data is no longer a secure option.

Through MicroToken Exchange (MTE), Secure Data Management Architecture is protected from cyber activity. This process makes it possible to secure data-in-transit, changing the technological aspect of where vulnerabilities exist in information technology and autonomous systems.

MicroToken Exchange™ (MTE)

MicroToken Exchange, (MTE) is a process for information security that consists of replacing a sequence of digital data from a data stream with a different sequence of digital data that has no relationship to the data that is replaced. In the case of data that is already encrypted, the process of MTE can still be applied as an additional layer of protection.

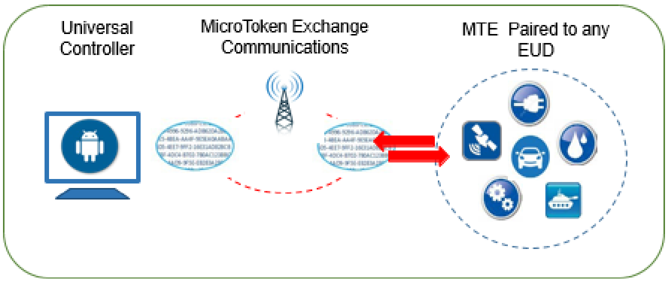


Figure 1: The use of MicroToken Exchange communications between the Universal Controller and the paired EUD. Process is shown prior to the MicroToken Exchange from both end nodes.

The following is an overview regarding its operation and how it works:

- Every send/receive command is authenticated and obfuscated, (No Encryption Req.)
- MicroTokens execute preprogrammed commands, these commands are stored in paired libraries.
- MicroTokens can only be interpreted by paired devices.
- MicroTokens are instantly obsolete. Each time a command is execute the entire library of commands is re-generated.
- Valid MicroTokens are hidden within complex digital chaff. The amount of chaff changes with each command so every packet has a different size.
- Pattern-recognition is not possible due to its design.

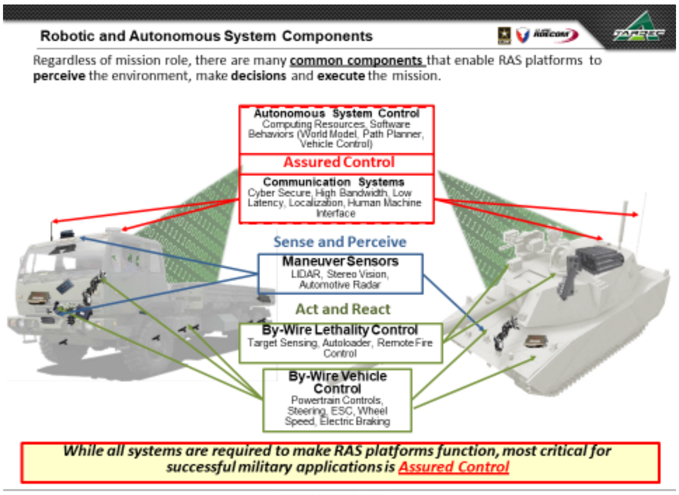
While there are additional layers within MTE, the solution makes sensitive command data invisible to hackers and cyberterrorists. MTE for data-in-motion began with the securing of commands to both connected and intelligent devices, including IoT devices.

With the use of MTE, it is possible to secure data-in-transit, through enhanced capabilities that are agnostic to the type of Communication Protocol that is used to transmit information. By processing data through the MTE process, a new paradigm is created by removing the vulnerability that exists today with data in motion. These capabilities are eligible for use in transferring data commands and communications This process secures the commands, providing the user with an unequivocal layer of protection against cybersecurity breaches, including unauthorized actions.

Operational Challenge

Vehicle to Infrastructure (V2I) communication is a critical component of a connected vehicle environment—a system of hardware, software, firmware and wireless communication that enables the dynamic transfer of data between vehicles as well as between vehicles and elements of the Joint Information Environment, (JIE). The greatest threat facing autonomy-enable military vehicles is cybersecurity.

TACOM-TARDEC is developing Squad Maneuver Equipment Transport, (SMET) systems.
Securing commands from the control device to the SMET over a wireless network is required for operational success. Current cybersecurity capabilities are at “fail safe” level. TARDEC is seeking enhanced security capabilities to achieve “full/fail mission capable” systems. By continuing to use typical cybersecurity options, there continues to be security risks and concerns for Automated Driving and Advanced Driver Assisted Systems, (ADAS). Through experimentation, it has been demonstrated that there are consequences of jamming and spoofing, exploiting underlying sensing principles. With very little effort, using simplistic tactics, bad actors can cause a great deal of harm and or destruction.



Robotic and Autonomous System Components

Regardless of mission role, there are many **common components** that enable RAS platforms to **perceive** the environment, make **decisions** and **execute** the mission.

Autonomous System Control
Computing Resources, Software Behaviors (World Model, Path Planner, Vehicle Control)

Assured Control

Communication Systems
Cyber Secure, High Bandwidth, Low Latency, Localization, Human Machine Interface

Sense and Perceive

Maneuver Sensors
LIDAR, Stereo Vision, Automotive Radar

Act and React

By-Wire Lethality Control
Target Sensing, Autoloader, Remote Fire Control

By-Wire Vehicle Control
Powertrain Controls, Steering, ESC, Wheel Speed, Electric Braking

While all systems are required to make RAS platforms function, most critical for successful military applications is Assured Control

Fig 2. Shows the Robotic and Autonomous system and their need for assured control.

MTE and Army Digital Devices

Military vehicles receive command inputs from many devices that need to control them, including satellites, handheld devices, other vehicles, thumb drives, and ground-based installations. These command inputs need to be secured. The purpose of this Technical Paper is to present a Proof-of-Principle encompassing physical devices, software, protocol rules, and MTE proprietary software “methods” that provide significantly stronger cybersecurity to protect commands over existing communication networks. The systems viewpoint below presents the envisioned integration of MTE for test and evaluation at TRL 4 and rapidly maturing to TRL 6.

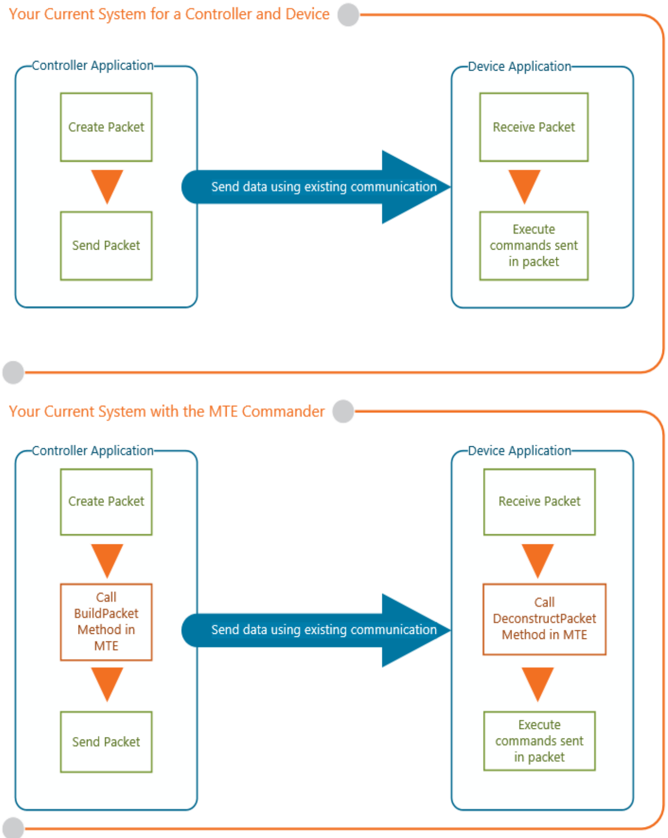

Your Current System for a Controller and Device
Controller Application
Create Packet
Send Packet
Send data using existing communication
Device Application
Receive Packet
Execute commands sent in packet
Your Current System with the MTE Commander
Controller Application
Create Packet
Call BuildPacket Method in MTE
Send Packet
Send data using existing communication
Device Application
Receive Packet
Call DeconstructPacket Method in MTE
Execute commands sent in packet

Fig 3. High-level pictorial of a system without MTE versus that of a system with MTE.

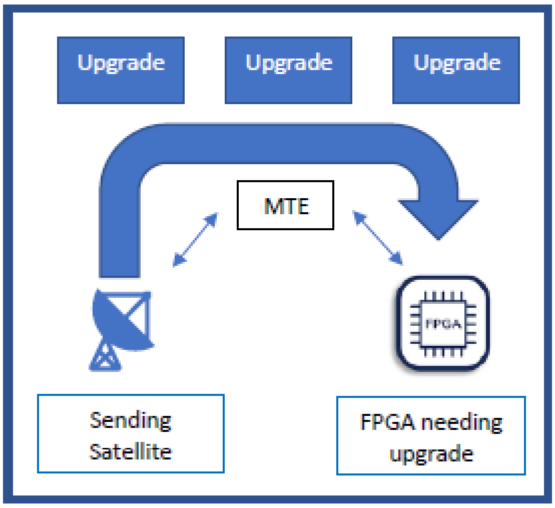
EUDS

Recent trends in military communications are driving the Army toward more diverse end-user devices (EUDs) to perform more activities via Unified Capabilities (UC). UC are a suite of integrated voice, video and/or data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to increase mission effectiveness for the warfighter and business communities.1 Concurrently, Army commanders are requesting EUDs based on their assessments of mission requirements, raising demand for the devices themselves as well as the connectivity necessary to enable their use. Meeting the demand comes at a cost. For the purposes of this Technical Paper TARDEC identifies all nodes within a network as a EUD, whether it is a point of origination or point of use.

FPGA

A field-programmable gate array (*FPGA*) typically has requirements to receive firmware upgrades from many devices, including satellites, handheld devices, thumb drives and ground-based installations. It is imperative for these upgrades to be secured. By pairing MTE with system encompassing physical devices, an unassailable security system is created.

FPGA have been included in missile command systems in defense efforts. By using MTE within an FPGA, the command and control of that missile system is unassailable to hackers, providing assured controls for the U.S. Military operating that missile system.



. **Fig 4.** Depicts a high-level visual of MTE on an FPGA during upgrade from satellite.

Operational Needs for Implementation of MTE

Eclypses MTE is a modified Commercial-off-the-Shelf, (COTS) software that can integrate into Army End-User Device, (EUD) operating systems, such as Robotic Operating Systems, (ROS) and others. Common EUD's include Control Devices and SMET autonomy kits. The Eclypses MTE is a small footprint software solution that requires as little as 700KB of RAM and 1.4 MB of non-volatile storage or less of FPGA resources for integration and operation. MTE is available in multiple languages and can be translated to C, C++ and Java platforms, additional languages are also possible with some additional development effort. MTE is optimal for use within embedded systems. By using MTE, a secure command environment within a bitstream from C5 to EUD is created. Use of MTE eliminates exploitable data from the communication network that delivers commands to EUD's creating "full/fail mission capable" systems.

Eclypses Components

The Eclypses MTE transmission is comprised of an Eclypses Controller Command Sender (ECCS) and an Eclypses Device Command Receiver (EDCR). Through these components, MTE can be deployed on a one-to-one, one-to-many, and/or many-to-many ecosystem. Communication utilizing MTE is two-way. The control command sender (ECCS) is a software component that receives an external input from an application and then builds a transmission packet. The packet is then sent through the clearing house where it is directed to the specific device. The communication protocol is not important, as long as, the route can be established. This component is delivered as a set of libraries that the specific sender applications interacts with. The device command receiver (EDCR) is a software component that receives transmission packets and based on the security profile, parses them into internal command tokens which it then uses to relay the specific command instructions to the underlying device. This component is responsible for accepting the communication, processing it and then calling a device adapter passing it the actual command sequence. The device then receives the instruction and executes it. Through this process the consumer does not manage or control the underlying cloud infrastructure, but has control over the operating system, storage, and deployed applications; and possibly limited control of selected networking components (e.g., host firewalls).

Risk Mitigation

Risk mitigation is a value add in order to comprehend the possible risks within new programs, providing additional insight into program cost, scheduling and performance objectives. For the purpose of this White Paper the implementation of a modified commercial-off-the-shelf, (COTS) protocol has been discussed for the securing of commands and controls. The capabilities within this COTS package is estimated at a Technical Readiness Level 9 (TRL 9) in commercial applications in the financial and healthcare industries. MicroToken Exchange is currently estimated at a TRL 4/5 initially and is believed to result in a TRL 6/7 in a military environment, prior to the end of the year.

Known Programmatic Risks are as follows:

- MTE deployment in Army Systems Integration Lab (SIL) has not been done before but is in process through current OTA.
- MTE integration with Controller and Combat Vehicle Robots has been done in our lab and is code complete and working as expected. However, it has not yet been field tested.
- Red team could find vulnerability and assail the technology, though we believe this will not occur.

Intellectual Property

MicroToken Exchange, (MTE) technology is protected by the following patent pending U.S. Patent Applications:

• U.S. Issued Patent No. 9,921,561 directed to "Real Time Control of a Remote Device"
• U.S. Patent Application No. 14,644,815, Filed 03/11/2015, Encrypted Data Storage And Retrieval System
• U.S. Provisional Patent Application No. 62/134,182, Filed 03/27/2015, Real Time Controlled Access to Preloaded Data
• U.S. Provisional Patent Application No. 62/237,487, Filed 10/21/2015, Real Time Control of a Remote Device.

Conclusion

In this paper, a MicroToken Exchange explains how it defends against cyber threats against end points, including but not limited to during data transfer. With increased technology throughout all defense systems, including autonomous vehicles, it is imperative to protect these systems as they mature. This defense should provide security against a cybersecurity breach. This new paradigm must ensure that only the right people get access to the right endpoints at the right time. Current use of encryption assists in preventing some cyber-attacks; however, MTE secures the data during transmission preventing the attacks occurrence. While it is not the intent for MTE to be a replacement to current encryption, it absolutely can, as MTE acts as an enhanced cybersecurity capability for all data outlets, including autonomous vehicles Command and Control. As the DoD continues to move forward on the path of autonomous vehicles, data security is a need in this sector. With MicroToken Exchange, there is a future in providing sustainable and responsible security measures against cybersecurity attacks. In a world where cyber atmospheres have higher prominence of warfare, MicroToken Exchange is a practical and compatible solution for ultra-secure Command/EUD security management.

Reference

Secure Cloud Systems, (2015). *U.S. Issued Patent No. 9,921,561.* Washington, DC: U.S. Patent and Trademark Office.

Secure Cloud Systems, (2016) U.S. *Patent Application No. 15/921,829.* Washington, DC: U.S. Patent and Trademark Office.

Secure Cloud Systems, (2015) *Patent Application No. 62/134,182 U.S.* Washington, DC: U.S. Patent and Trademark Office.