2019 NDIA GROUND VEHICLE SYSTEMS ENGINEERING AND TECHNOLOGY SYMPOSIUM
GROUND SYSTEMS CYBER ENGINEERING TECHNICAL SESSION
AUGUST 13-15, 2019 - NOVI, MICHIGAN

Implementing Cybersecurity Risk Management Framework for the MAPS Base Kit

Matt Nowc[1], Andrey Shvartsman [2], Ed Moon [3], Lucas Tucker [4]

[1]MAPS Chief Engineer, CCDC-GVSC, Warren, MI
[2]MAPS Controller Lead, CCDC-GVSC, Warren, MI
[3]AVDS Chief Engineer, LM MFC, Orlando, FL
[4]AVDS Cyber Lead, LM MFC, Orlando, FL

ABSTRACT

The Modular Active Protection System (MAPS) Science and Technology Objective (STO) program led by the CCDC- Ground Vehicle Systems Center (CCDC-GVSC) has undertaken and committed to delivering a product baseline that can readily support performance requirements for Vehicle Protection System (VPS) capabilities while meeting cybersecurity requirements. DoD investments in a cyber-secure common kit can provide many benefits to the DoD as each program (i.e., Abrams, Bradley, Stryker, AMPV) will be able to leverage the initial investments without having to create their own technical solution per platform. It is broadly acknowledged that implementing security controls early in the product's life cycle provides better capabilities, reduces vulnerabilities, reduces program schedule, and reduces program cost compared to attempting to add cybersecurity later in the production and test phases. As the MAPS open-architecture enables programs to leverage occupant and vehicle protection capabilities from other current programs, exemplifying Horizontal Technology Insertion (HTI), it will also support effective and efficient reuse for cyber-security required by the Risk Management Framework (RMF) to protect the VPS itself, in turn enhancing overall vehicle protection.

1. INTRODUCTION

The U.S. Army is developing a common hardware and software kit to enable advanced vehicle protection capabilities for combat and tactical vehicles. The kit will provide required interfaces and functions to rapidly integrate with advanced sensors and countermeasures delivered from a wide variety of suppliers, both domestic and foreign. DoD acquisition decision-makers have mandated cybersecurity requirements for current and future programs in policy documents such as DoD 5000.02 and DODI 8500.01. The policy requires DoD program managers to plan and implement cybersecurity requirements prescribed in the Risk Management Framework (RMF). The resulting program's plan will include the many technical solutions and their associated testing to determine the level of compliance. To receive a positive decision to move a program forward, program managers must allocate funding and schedule to be successful during the DoD acquisition decision processes. The first decision point is at Milestone A where mission critical systems, functions and components will require a plan (i.e., tasks, funding allocation and schedule) to conduct penetration testing during operational test and evaluation.

The Modular Active Protection System (MAPS) Science and Technology program led by the CCDC-Ground Vehicle Systems Center (CCDC-GVSC), has undertaken and committed to delivering a product baseline which can readily support projected performance requirements for Vehicle Protection System capabilities while meeting cybersecurity requirements. DoD investments in a cybersecure common kit can provide many benefits to the DoD as each program (i.e., Abrams, Bradley, Stryker, AMPV) will be able to leverage the initial investment without having to create their own technical solution. It is readily acknowledged that implementing security protocols early in the product's life cycle provides better capabilities, reduces vulnerabilities, reduces program schedule and reduces program cost compared to attempting to add cybersecurity later in the production and test phases. Cybersecurity on the MAPS programs has leveraged capabilities from other current programs and is a good example of Horizontal Technology Insertion (HTI).

This paper will describe U.S. Army efforts and industry's support to make this concept of reusable cyber hardening of vehicle protection systems a reality. The audience (especially, DoD program managers, requirements owners and S&T leaders) will benefit from an understanding of the requirements, the process and status of technical solutions to provide a robust, cyber secure capability for U.S. Army and potentially U.S. Marine Corps ground combat vehicles for vehicle protection. There is application of this approach to other vehicle functions such as fire control solutions, communications, situational awareness, vehicle mobility controls and even unmanned ground vehicles.

Cybersecurity in a ground vehicle environment includes eliminating the ability for an adversary to modify, disrupt, defeat or disable any capability. All methods of access must be considered, beginning with procurement of manufacturing materials and continuing throughout the entire life-cycle including maintenance actions and upgrades. Controls must be in place to address each of these vulnerabilities. These features, practices, controls and methods will be directly transferable to additional platforms as they are enhanced with MAPS-compliant capabilities.

The challenge for the DoD is to develop a solution set which can be leveraged/re-used across many platforms rather than to re-invent a unique solution for each platform. The Army and the Marine Corps simply don't have the time nor the funding to allow inefficiencies to occur while allocating limited resources across their portfolios. The payoff is to accelerate the capabilities to the maximum number of warfighters by adopting the Better Buying Power 3.0 construct. The intent of this paper is to help the Army and Marine Corps ground vehicle community better understand the cyber requirement, its synergistic relation with MAPS, and the associated enabling technologies and processes for both.

MAPS has defined and developed a formal architecture that clearly communicates the system and subsystem security requirements. Making security a requirement for becoming MAPS compliant ensures that vendors bring a hardened and tested solution to the MAPS environment. Ensuring a cohesive security solution, no matter the instantiation. This allows platforms to have confidence that the introduction of MAPS into their networks does not present a cybersecurity risk.

2. RMF PROCESS

There are six (6) steps in the RMF process listed below with a brief implantation description of each task. MAPS has been designated as a Platform Information Technology (PIT) System. This requires the system to go through an Assess & Authorize process for an Authority to Operate (ATO) decision. Long-term, this postures programs to be able to reuse T&E results, enabling easier transition for multi-platform use through the reciprocity process.

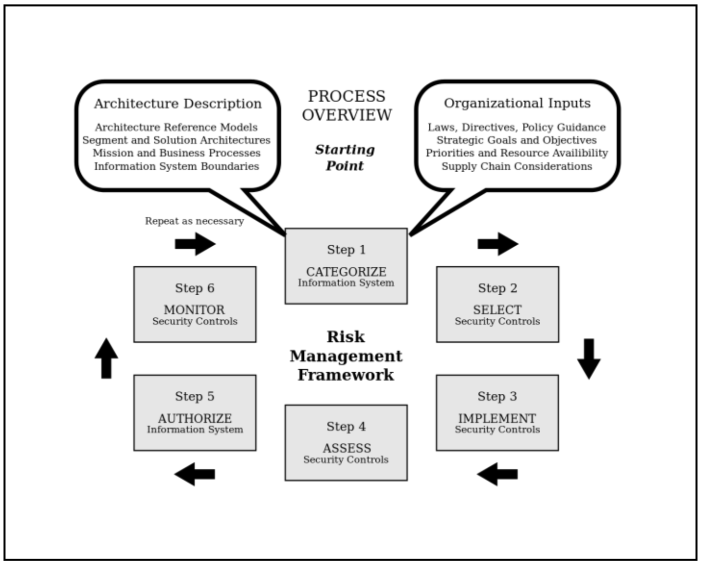

Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries
PROCESS OVERVIEW
Starting Point
Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availibility
Supply Chain Considerations
Repeat as necessary
Step 1 CATEGORIZE Information System
Step 2 SELECT Security Controls
Step 3 IMPLEMENT Security Controls
Step 4 ASSESS Security Controls
Step 5 AUTHORIZE Information System
Step 6 MONITOR Security Controls
Risk Management Framework

Figure 1: The Risk Management Framework (RMF) Process Overview [1]

1-**Categorize** the information system and the information processed, stored, and transmitted by that system based on an impact analysis. Vested party is identified.

The determination of system categorization impact levels for the Confidentiality, Integrity, and Availability (C-I-A) security objectives is described in Committee on National Security Systems Instruction (CNSSI) 1253, Security Categorization and Control Selection for National Security Systems [2]. There are three security objectives, and each has three possible values (Low, Moderate, or High). The impact of the security objectives are determined using the criteria set forth by FIPS 199 [3]. MAPS engineers used a threat-based risk assessment to assist in the system categorization.

2-**Select** an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions. If any overlays apply to the system, it will be added in this step.

MAPS has implemented additional overlays on top of a determined baseline set of security controls. In addition to the RMF security control, system design and architecture is derived from a multitude of sources. These sources can include the PPP, ICD, Survivability KPPs, CONOPS, and threat assessments.

The open-systems concept directly violates the principals of security. Knowing this, it was important to analyze how the security requirements could be used as enhancements to the MAF messages while allowing modularity. This involved identifying common messages that must be implemented in each subsystem in order to assure security for every MAPS instantiation.

3-**Implement** the security controls identified in the RMF Step 2 are applied in this step.

MAPS system security architecture is a combination of RMF security controls and unique system security requirements which can be mapped to RMF controls. System security design is influenced by the technical controls of the RMF which primarily reside in the Access Control (AC), Audit (AU), Configuration Management (CM), Authentication (IA), System and Communication Protection (SC), and System and Integrity Protections (SI) families. The MAPS controller provides the security management functionality. Applicable Security Technical Implementation Guidance (STIG) is used for COTS components in the MAPS environment.

4-**Assess** third party entity assess the controls and verifies that the controls are properly applied to the system.

The assessment and controls must include the entire access chain as shown in the Context Diagram below.

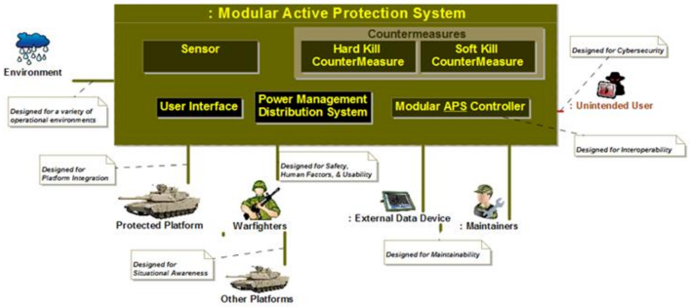
5-**Authorize** the information system is granted or denied an Authority to Operate (ATO), in some cases it may be postponed while certain items are fixed. The ATO is based off the report from the Assessment phase.

The MAPS ATO data package continues to be assembled and will be submitted for each configuration to be fielded.

6-**Monitor** the security controls in MAPS are continuously monitored in a pre-planned fashion documented earlier in the process. Continuous monitoring must be considered in Step 2 of the RMF process to ensure that appropriate data is collected. This allows the MAPS PM to assess the effectiveness of security controls over time. ATO is good for 3 years, every 3 years the process needs to be repeated.

3. MAPS CONTEXT DIAGRAM

The current scope of the Assessment step is encapsulated as the hardware defined as the Modular APS Controller (MAC), the Power Management Distribution System (PMDS), the MAPS Network Switch and User Interface Control Panel (UICP) shown in the context diagram below. The following are known access points into the system that must be assessed and controlled.


: Modular Active Protection System
Countermeasures
Sensor
Hard Kill CounterMeasure
Soft Kill CounterMeasure
User Interface
Power Management Distribution System
Modular APS Controller
Environment
Designed for a variety of operational environments
Designed for Cybersecurity
: Unintended User
Designed for Interoperability
Designed for Platform Integration
Designed for Safety, Human Factors, & Usability
Protected Platform
Warfighters
: External Data Device
: Maintainers
Designed for Maintainability
Designed for Situational Awareness
Other Platforms

Munition Threats

The threats interface defines the type of munitions the MAPS is required to encounter. The primary threats that MAPS seeks to engage and protect against are the Anti-Tank Guided Missile (ATGM), the Rocket Propelled Grenade (RPG), Recoilless Rifle, and tank fired rounds.

A MAPS instantiated Vehicle Protection System (VPS) protects the vehicle from munitions. Cyber controls for physical protection from destruction, as well as electronic, should be intrinsic to each MAPS VPS open-module, to protect itself so it can protect the vehicle.

Environment

The environmental interface defines the operating and non-operating conditions that the MAPS system will be subjected to. This includes items such as thermal, electromagnetic, atmospheric, vibration, shock, etc.

Control systems in MAPS are used to mitigate the impacts of environmental conditions. Subsequently, the logic used to control these devices (i.e thermometers, fans, etc.) can be influenced by cyber. MAPS utilizes information integrity controls to ensure the environment surrounding it is correct.

Protected Platform

The protected platform interface defines the parameters associated with the installation of the MAPS onto the vehicle platform. These parameters include mechanical installation, power requirements, and data interfaces required by the MAPS and platform.

MAPS must assure information received and transmitted is correct and allowed. Access controls have been defined to protect these interfaces.

Other Platforms

Most protected platforms are networked with other platforms to provide situational awareness and share threat data. These parameters include the data interfaces such as Blue Force Tracker.

Threat data is to be protected using data at rest requirements and complying with the National Security Agency's guidance on protecting classified information. MAPS integrates a certified storage solution for this information that protects data confidentiality and integrity at rest.

Warfighters/Operator

The warfighter interface defines the parameters related to the controllability and status of MAPS. It also includes the safety aspects of dismount and secondary vehicles about the MAPS employed vehicle.

MAPS must present only the functionality required for the warfighter to operate the system and nothing more. MAPS secures the operator interface by employment of the principle of least privilege. System status and logging is provided to the warfighter as an indicator of the system state. Operators can use this information to quickly remediate system malfunctions.

External Data Device\External Maintenance Device (EMD)

The External Data Device interface provides for an external device to be able to maintain the MAPS system. The external device may permit the querying of failure data, reprogramming of system software, loading or modifying mission data, and configuring installed subsystems.

It is important that this device is an integrated product of the security environment. Controlling this interface requires multiple levels of authentication and verification of installed packages.

Maintainers

The maintainers interface relates to the aspects of the system required for the diagnosis of failure states, removal and replacement of system components, handling aspects, markings, and the logistic supply of spare equipment.

The maintainer interface is protected by physically and logically controlling access to the EMD. Additionally, ensuring that the EMD inherits appropriate security controls from the baseline provides a hardened system configuration.

Unintended User

Unintended users indicate the potential for unauthorized access to MAPS and defines the control boundaries required for cybersecurity.

Unintended access to MAPS could allow information to be disclosed to an unauthorized individual. This access is controlled on MAPS by maintaining an active list of authorized ports, protocols, and services. Assuring that only the approved interfaces, specifically externally facing, are authenticated and access controlled.

4. CONSIDERATIONS OF A SECURE SYSTEM

A secure system is more than just developing a fully functional and compliant system. A system can function error free but still contain multiple vulnerabilities. System security should be treated as 'ility and managed throughout the entire lifecycle of the program. Whether it is from initial program inception, where security is considered in Hardware and Software selection, all the way to sustainment to ensure appropriate maintenance procedures and functions are in place to protect the program's investments.

The system (Hardware and Software) should continuously be tested against 'rainy day' scenarios, as the cybersecurity landscape changes rapidly. This allows changes to be incorporated into system upgrades.

No one likes to hear a system is full of "bad software" after passing a Formal Qualification Test (FQT). This this is not a description of a systems functionally, but the lack of security. A list of common remaining vulnerabilities in a fully functioning system include improper exception handling, back doors through an incomplete system, untested fault conditions, processor overflow, developer access, basic passwords (admin, password,), development ports and instrumentation ports.

Cybersecurity does not end at system delivery. The maintenance of a system is also prone to attacks. New threats are also discovered over time. Spectre & Meltdown are examples of system vulnerabilities that were discovered years after Intel processors effected were delivered.

Thus, programs must follow Step 6 of the RMF process, which calls for monitoring and re-evaluating which circles back to step 1 and repeats the steps to ensure the lowest risk to fielded systems throughout the operation and sustainment phase of the lifecycle, and eventually through decommissioning and disposal.

5. CONCLUSION

To establish an effective cybersecurity strategy and solution there must be investment from the beginning of the system concept. RMF is not a 'silver bullet', however it does provide a mechanism to define system requirements. This contributes to the HW and SW selection, reducing the risk of redesign. Ultimately, this approach has allowed MAPS to "bake-in" security features that contribute to easily integrating new requirements against the ever-evolving threat landscape. Additionally, getting cybersecurity involved in planning allows the program to appropriately staff the cybersecurity programs leading to on-time system delivery.

6. REFERENCES

[1] National Institute of Standards and Technology Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems," current edition

[2] Committee on National Security Systems Instruction 1253, "Security Categorization and Control Selection for National Security Systems," March 15, 2012, as amended

[3] Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems