

Application of the Armament Cyber Assessment Framework

A Security Assessment Methodology for Military Systems

Aidan McCarthy

Aidan.Mccarthy@Westpoint.edu
The United States Military Academy
West Point, New York

Liam Furey

Liam.Furey@Westpoint.edu
The United States Military Academy
West Point, New York

Keagan Smith

Keagan.Smith@Westpoint.edu
The United States Military Academy
West Point, New York

Daniel Hawthorne

Daniel.Hawthorne@Westpoint.edu
The United States Military Academy
West Point, New York

Raymond Blaine

Raymond.Blaine@Westpoint.edu
The United States Military Academy
West Point, New York

ABSTRACT

As the Army modernizes, its weapon systems are becoming increasingly more cyber dependent. This increased connectivity provides incredible opportunities, but also introduces new risks. This paper introduces the Armament Cyber Assessment Framework (ACAF), a schema for creating security assessment workflows integrated into the design process. The goal of ACAF is to introduce a security oriented mindset into the solution prior to release, and to provide meaningful results at every level. This goal is accomplished through the study and incorporation of multiple industry leading frameworks into a uniquely iterative process. ACAF is implemented for testing via the Global Vulnerability Assessment and Penetration Platform (GVAPP). GVAPP works to provide automated vulnerability information during the armament design process. It offers meaningful risk calculus to armament designers without cyber security backgrounds to mitigate potential vulnerabilities prior to fielding the system. This work focuses on military applications, but is applicable to similar civilian platform technologies.

CCS CONCEPTS

• **Security and privacy** → *Distributed systems security*; **Vulnerability scanners**; **Penetration testing**; **Formal security models**.

KEYWORDS

security assessment, vulnerability scan, penetration test, red team, military

ACM Reference Format:

Aidan McCarthy, Liam Furey, Keagan Smith, Daniel Hawthorne, and Raymond Blaine. 2020. Application of the Armament Cyber Assessment Framework: A Security Assessment Methodology for Military Systems. In *Hot Topics in the Science of Security Symposium (HotSoS '20)*, April 7–8, 2020, Lawrence, KS, USA. ACM, New York, NY, USA, 2 pages. <https://doi.org/10.1145/3384217.3384222>

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
HotSoS '20, April 7–8, 2020, Lawrence, KS, USA
© 2020 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-7561-0/20/04.
<https://doi.org/10.1145/3384217.3384222>

1 INTRODUCTION

In 2017, the United States Army outlined 6 modernization priorities for the future, with number one being long range precision fires [6]. Achieving these priorities forces the Army to increasingly rely on advances in digitization from the private sector. The process involves introducing sensors, computing, and networks that were previously absent, which comprise a new source of risk [9].

The call for fire procedure (CFP) for artillery is a good example of these new challenges. In CFP, a forward observer identifies a target and transmits this information to the Fire Direction Center (FDC). The FDC then processes this information into firing data such as elevation, coordinates, and type of round [7]. The firing data is then passed to the gun line, where rounds are fired.

The CFP has several points at which vital information is vulnerable: in transit, storage, or a processing state. Manipulation of the data or these systems could result in friendly fire, civilian casualties, or disclosure of location data. As the Army continues to modernize, the number of these inter-connected systems will increase, as will the opportunities for malicious actors. It is imperative to integrate a security oriented mindset early in the weapon development process, utilizing iterative security assessments throughout.

This work seeks to fill gaps in current methodologies, which lack a standardized and iterative approach for diverse systems, by introducing the Army Cyber Assessment Framework (ACAF). ACAF is designed for continuous integration into the development process, and is capable of providing meaningful risk analysis for systems designers of various backgrounds.

2 BACKGROUND

The cyber security community has a significant number of quality frameworks. These frameworks were all developed for specific purposes, often with the idea of generalization. In most cases existing frameworks are sufficient, but they do not address the unique problem described in this paper. In developing ACAF, the existing frameworks were analyzed for advantages and disadvantages. The advantages of existing frameworks were integrated into ACAF, as well as new unique aspects to address the cumulative disadvantages.

The Lockheed Martin Cyber Kill Chain (CKC) provides analysis of the path an attacker takes during an engagement. It outlines 7 phases of an attack, covering pre-exploitation reconnaissance to post-exploitation command and control (C2) [1]. The CKC has established itself as invaluable for security researchers as a tool to

map attack signatures from an engagement, and to develop attack narratives [5]. However, it focuses too much on the decisive action surrounding an exploitation event [3]. This focus disregards unstructured movement that does not constitute decisive action, even when it may indirectly influence the end state. To create a methodology oriented around creative testing, rather than analysis, and because weapon systems are inherently unique, ACAF structures its phases in a more malleable manner.

The MITRE ATT&CK Matrix is a framework allowing security professionals to analyze attacks through the lens of known advanced persistent threats (APTs) [8]. It identifies several core components throughout the attack process, pairing each with common protocols and tools. This approach is useful from the perspective of security practitioners, enabling emulation of APTs. However, not all of the components in this framework correspond to distinct phases. The actions instead rely on real world data collection, making it difficult to generate a repetitive process. ACAF provides the necessary context behind the actions it suggests, allowing for simple yet flexible mapping to phases of the security assessment.

The Penetration Testing Execution Standard (PTES) is a collaborative standard on penetration testing. It describes a 7 step process for penetration testing from pre-engagement interactions to reporting. A technical guideline provides tools that are applicable in each step and in alternate frameworks [4]. PTES outlines concepts more closely aligned with those of ACAF, such as defining the scope and risk calculation, yet lacks a clear discussion on creating iterative processes and focuses on a business-client relationship for conducting penetration testing opposed to a holistic assessment.

0 Day Security provides an action-oriented approach, defining tools and commands to be used based on the services discovered in system scanning [2]. Using it as a reference manual requires overstepping a high technical barrier to entry, but allows security professionals to explicitly define actions taken during an engagement. ACAF targets designers with a wide range of experience; its implementation should be accessible and use automation where appropriate.

3 ARMAMENT CYBER ASSESSMENT FRAMEWORK (ACAF)

ACAF combines the ideas defined by traditional security assessment methodologies. It is built around the need for a broad application of vulnerability identification, exploitation, patching, and reporting. ACAF fundamentals rest upon the establishment of five key phases during the overall security assessment: background research, the vulnerability scan, the penetration test, the red team assessment, and analysis and reporting. One of the most important nuances of ACAF is the lack of firm sub-phases, allowing for iterative processes to be created specific to a particular assessment.

The five phases of ACAF compile the fundamentals seen throughout the CKC, ATT&CK, and PTES. Background research is built from a blend of the reconnaissance phase in the CKC and the PTES definition of the scope. The vulnerability scan moves into the later parts of reconnaissance, as well as potential weaponization and delivery. This step is crucial, setting the stage for actions conducted in both the penetration test and the red team assessment. These next two phases accomplish technical goals set during background

research, depending on whether the objective is thorough vulnerability analysis or adversary emulation. Finally, analysis and reporting ties all data collected into a plan for future improvements, giving the entirety of the assessment its driving purpose.

Unique to this framework is a design oriented around incremental testing throughout the design process as opposed to only on a final product. This allows developers and security analysts to be more efficient in their collaborative workflow, and forces a security oriented mindset from the beginning of a project's life-cycle. In order to support this feature, products utilizing ACAF should yield results capable of persisting in a database that spans multiple iterations. The periodic collection and analysis of data throughout the development and deployment cycles allows ACAF to become a living framework, providing valuable insight into the current state of system security. This allows for both pattern recognition and identification of new threats.

3.1 Application and Further Research

The Global Vulnerability Assessment and Penetration Platform (GVAPP) is our implementation of ACAF, oriented around automating security assessments for military systems. GVAPP uses a cloud database to better enable incremental testing and to provide the ability to compare against a database of previously identified vulnerabilities.

This particular implementation of ACAF benefits from a unique variant of automation that may not be applicable to other tools. The need to provide services to users without security backgrounds leads to difficulty in the automation of later phases such as penetration testing. Even with the automation of information gathering and vulnerability scanning, GVAPP's post-exploitation modules will require manual interaction.

Future implementations of ACAF should incorporate data from the MITRE ATT&CK Matrix to provide patterns of activity exhibited by APTs. The future of security testing lies with intelligent and modular algorithms to determine attack paths in the phases following the vulnerability scan.

REFERENCES

- [1] 2020. Cyber Kill Chain. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf
- [2] 0daysecurity.com. 2011. Penetration Testing Methodology - 0DAYSecurity.com. <http://www.0daysecurity.com/pentest.html>
- [3] Sean Barnum. 2012. Standardizing cyber threat intelligence information with the structured threat information expression (stix). *Mitre Corporation* 11 (2012), 1–22. http://stixproject.github.io/about/STIX_Whitepaper_v1.1.pdf
- [4] Rick Hayes. 2012. PTES Technical Guidelines - The Penetration Testing Execution Standard. http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines
- [5] J. D. Mireles, J. Cho, and S. Xu. 2016. Extracting attack narratives from traffic datasets. In *2016 International Conference on Cyber Conflict (CyCon U.S.)*. 1–6. <https://doi.org/10.1109/CYCONUS.2016.7836624>
- [6] U.S. Army Chief of Public Affairs. 2018. STAND-TO! <http://www.army.mil/standto/2018-01-16>
- [7] U.S. Department of the Army. 2016. FIELD ARTILLERY MANUAL CANNON GUNNERY. https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/tc3_09x81.pdf
- [8] Blake Strom. 2019. Getting Started with ATT&CK: Adversary Emulation and Red Teaming. <https://medium.com/mitre-attack/getting-started-with-attack-red-29f074cc7e3>
- [9] Cedric T. Wins. 2018. RDECOM's road map to modernizing the Army: Long-range precision fires. https://www.army.mil/article/211569/rdecoms_road_map_to_modernizing_the_army_long_range_precision_fires