National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

PROACTIVE VULNERABILITY MANAGEMENT - A SYSTEMS APPROACH TO MANAGING PLATFORM TECHNOLOGY VULNERABILITIES

LIEUTENANT-COMMANDER ROBIN E. MOLL

JCSP 46

Service Paper

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 46

Étude militaire

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 46 – PCEMI 46
2019 – 2020

SERVICE PAPER - ÉTUDE MILITAIRE

PROACTIVE VULNERABILITY MANAGEMENT - A SYSTEMS APPROACH TO MANAGING PLATFORM TECHNOLOGY VULNERABILITIES

Lieutenant-Commander Robin E. Moll

Word Count: 2,586

Nombre de mots : 2.586

PROACTIVE VULNERABILITY MANAGEMENT - A SYSTEMS APPROACH TO MANAGING PLATFORM TECHNOLOGY VULNERABILITIES

AIM

1. Best practices for security have been developed in the enterprise information technology (IT) domain over a period of decades. In the absence of mature cyber security practices in the military platform technology[1] (PT) domain, there is a tendency to want to apply those best practices from the enterprise without due consideration for the different requirements that may exist. This paper seeks to distinguish PT vulnerability management (VM) requirements from those of enterprise IT and further introduces a proactive vice reactive model for managing vulnerabilities through the military equipment lifecycle.

INTRODUCTION

2. In late December 2017, the very public disclosure of the Spectre and Meltdown speculative execution vulnerabilities associated with computer chips created significant turmoil across the IT industry.[2] Public Safety's response to all those affected was to recommend the application of software and firmware updates as soon as they were available.[3] Not surprisingly, within DND all eyes looked to the Assistant Deputy Minister of Information Management's (ADM(IM)) organization for impact and risk assessment relating to the vulnerabilities as well as to take the lead for reporting and patching

[1] Platform technology is defined as hardware and software on a vessel, aircraft, ground vehicle, weapon system or equipment that monitor or control data, power, command and control, surveillance, fire control, navigation, propulsion, maintenance, training or other fundamental functions (Draft DAOD 3035-0, Materiel Assurance)

[2] "Meltdown and Spectre," accessed October 23, 2019, https://spectreattack.com/.

[3] "AL18-001: Meltdown and Spectre Side-Channel Vulnerabilities," December 21, 2018, https://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2018/al18-001-en.aspx.

enterprise systems. At the same time, it was quickly realized that the scope of the vulnerabilities extended past traditional enterprise IT equipment, as it affected computer chips whose use had become ubiquitous in many different types of technologies, even those used in military applications. As a result, the Assistant Deputy Minister of Materiel (ADM(Mat)) took the unprecedented step with respect to publicly disclosed vulnerabilities and explicitly directed the Director Generals within his organization "to ensure that equipment OEMs for fleets and larger systems are engaged to determine if any vulnerabilities exist, and how they are being mitigated."[4]

3. Given the absence of an overarching PT VM program within the Materiel Group (Mat Grp), the challenge of vulnerability identification was much more difficult and labour intensive than initially anticipated. At the outset, the response was anchored in the approach used to respond and report to vulnerabilities within the enterprise IT domain. It was quickly realized however that the centralized asset management databases for platform technology did not provide the fidelity of information that would be required (i.e. computer chips and software/firmware versions are not available in the Defence Resource Management Information System).[5] After a concerted effort lasting over twelve months, the subject matter experts (SMEs) within Mat Grp concluded that the Spectre/Meltdown vulnerabilities posed minimal direct risk to the PT managed by Mat Grp, but what emerged instead was a much more pressing issue: the need for a more

[4] Assistant Deputy Minister of Materiel, Patrick Finn, "Computer Chips," (E-mail), January 8, 2018.

[5] Cmdre Simon Page, "Briefing Note to ADM(MAT) - Meltdown/Spectre Fleet Systems Reporting Proposal," (Briefing Note, Assistant Deputy Minister of Materiel, Cyber Mission Assurance), January 9, 2018.

robust VM framework within ADM(MAT) to better manage to vulnerabilities in the future.[6]

4. In order to begin to address this issue, this paper will first provide a brief overview of traditional systems security practices associated with PT. Next, this paper will propose the required essential elements of a generic VM framework and then outline how the enterprise IT approach to VM fits within it. Next, PT is differentiated from IT, and VM challenges are highlighted in the context of the same framework. Finally, an overview of a proactive model for VM of PT is presented as a consideration for future adoption within CAF.

DISCUSSION

Traditional Systems Security of PT

5. PT includes most electronics found in modern weapons platforms, including vehicles, ships and airframes. While not an exhaustive list, this can include the hardware and software that controls weapons, sensors, communications, movement, electrical power generation and distribution (EPG&D) and the heating, ventilation and cooling (HVAC) of military platforms. Traditionally, the ongoing security of platform technology in the cyber domain has been largely ignored. Many of the platform systems were built before any notion of modern cyber security threats (or requirements) were conceived. Similar to industrial control systems (ICS) used in the private sector for critical systems such as power and gas distribution, military systems were designed using proprietary

[6] Robin Moll, "BN - MEPM Cyber Vulnerability Assessment Plan," (DND 317, Assistant Deputy Minister of Materiel, Cyber Mission Assurance), February 11, 2019.

hardware and software. Security has been largely expected through obscurity[7] in addition to the notion that the systems are protected by physical security and not otherwise directly accessible by the outside world.

6. After the Stuxnet computer virus was exposed in 2010[8], the security landscape for ICS and military PT changed forever. Stuxnet was a state sponsored attack, the forensic review of which revealed that with enough resources, adversaries could breach air gapped systems on highly secure networks with targeted, precise and catastrophic effects. In the aftermath of Stuxnet, it has been recognized that principles (such as VM) once thought to only apply to securing enterprise IT networks need to also be considered in the context ICS (and by extension PT).

The Essentials of Vulnerability Management

7. VM has become a prominent concern across the technology industry and is considered one of the critical activities necessary for securing information systems.[9] The Communications Security Establishment has published IT Security Guidance to help government departments implement, operate and maintain information systems in which they specify the management of vulnerabilities as a key security control.[10] In order to

[7] "What Is Security Through Obscurity (STO)? - Definition from Techopedia," *Techopedia.Com*, accessed October 24, 2019, https://www.techopedia.com/definition/21985/security-through-obscurity-sto.

[8] Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired*, July 11, 2011, https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

[9] "Implementing and Auditing the Critical Security Controls - In-Depth | Community," accessed October 23, 2019, https://www.sans.org/community/event/sec566-ottawa-57780.

[10] "ITSG-33 - Annex 2 - Information System Security Risk Management Activities," *IT Security Risk Management*, 2012, 113. 54.

effectively manage vulnerabilities through the life cycle of a system, several complementary associated activities are required:[11,12]

a. Vulnerability discovery (VD): whereby potential vulnerabilities associated with a system are discovered and identified using appropriate tools or techniques (research, reverse engineering etc.).

b. Vulnerability scanning (VS): the process by which identified vulnerabilities are confirmed as present within a system, often using automated tools.

c. Vulnerability assessment (VA): the process by which confirmed vulnerabilities are validated and categorized in terms of severity, often utilizing penetration testing in order to determine the potential impact resulting from exploitation.

d. Vulnerability remediation (VR): this process may include updating software or replacing hardware in order to remove the vulnerability from a system. In some cases, VR can take the form of mitigations against the existence of a vulnerability such that the risk is lowered to an acceptable level.

Vulnerability Management for Enterprise IT

8. For the purpose of this paper, enterprise IT is composed of assets that connect and are connected through the national network infrastructure. While management of these assets is split between the Department of National Defence (DND) and Shared Services Canada (SSC) based on network classification, ultimately the security management practices closely map and follow best practices in other government departments (OGDs)

[11] Ibid. 99.

[12] It should be noted that the language of vulnerability management is in constant flux within the cyber security industry and continues to create much confusion. It is beyond the scope of this paper to argue the taxonomy, but for clarity within this paper terms are defined based on the author's experience and the vulnerability management context provided at the reference.

as well those of corporate networks in private industry. With this in mind, VM activities relating to enterprise IT systems are conducted as follows:

a. VD/VS/VA. These VM activities are generally combined. A commercial off the shelf (COTS) solution is utilized which performs vulnerability scanning based on a vulnerability database that is updated periodically by the COTS vendor. Typically, enterprise scanning tools use vulnerability databases that are derived from the Common Vulnerabilities and Exposures (CVE) list maintained in the open source by the Mitre Corporation.[13,14] This list represents an amalgamation of all publically disclosed vulnerabilities and provides unique identifiers and descriptions for each. Vulnerability scanners will also contextualize vulnerabilities in terms of severity by assigning them a score in accordance with the Common Vulnerability Scoring System (CVSS), which attempts to assign a severity score based on expected threat within the context of a typical enterprise network.[15]

b. VR. Normally, when vendors release security patches, they are deployed centrally when available through the national network infrastructure. When deemed sufficiently critical, in the absence of a software patch some vulnerabilities are mitigated through the introduction of signatures in the enterprise intrusion detection systems (both network and/or host based).

[13] "CVE - Common Vulnerabilities and Exposures (CVE)," accessed October 23, 2019, https://cve.mitre.org/.

[14] It should be noted that the maintenance of the CVE database by Mitre is sponsored jointly by the Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency.

[15] "NVD - Vulnerability Metrics," accessed October 23, 2019, https://nvd.nist.gov/vuln-metrics/cvss.

Vulnerability Management Challenges and Opportunities Related to PT

9. VD. In an effort to realize economies of scale, the design of modern military systems have tended towards employing standardized COTS hardware and software wherever possible. Variants of Linux and Microsoft Windows operating systems are now becoming ubiquitous within military systems, as is the presence of Intel, AMD and ARM microchips. While there is a benefit to being able to take advantage of the existing vulnerability databases for popular COTS components, it must be recognized that in many cases, proprietary military hardware and software continue to co-exist with these COTS systems and required VD activities will not otherwise occur for these systems unless resourced internally. The lack of vulnerability research on proprietary PT brings into serious question whether a net security benefit can be realized by conducting the other vulnerability activities. As an analogy, it makes little sense to lock the windows if nobody has checked to see if the front door has been left wide open. Further complicating matters, the CAF is prevented from carrying out VD activities on equipment that is controlled in accordance with International Traffic in Arms Regulations (ITAR), which only further exacerbates the VM problem by introducing the potential for additional vulnerabilities to exist that can only ever be discovered by the adversary.

10. VS. There are two primary concerns with VS with respect to PT. Firstly, the COTS vulnerability scanners employed on the enterprise IT networks were not designed to run on PT in parallel with control system hardware and software. Vulnerability scans by their very nature are invasive and running them can have unanticipated effects

including irreparably damaging equipment.[16] This is of particular concern for cyber-physical systems where the erroneous actuation of a control system could result in a weapon being fired, or fuel being dumped overboard. The second concern with VS with respect to PT is related to the security paradox introduced by interfacing a vulnerability scanner with PT. That is to say, while Stuxnet proved air-gapped systems were not infallible, isolated systems continue to provide a significant degree of protection from all but the most advanced threat actors.[17] In order to be effective, vulnerability scanners require access to an up to date vulnerability database by design. This implies that in order to conduct VS, a PT that was previously isolated would need to interface with data libraries sourced from the internet, most likely at established regular intervals (if not live). Unless mechanisms to mitigate both these concerns are deliberately built into the VM plans for these systems, the risk can only be reduced by conducting VS activities off of the "production" environment. In most cases however, offline testing facilities for PT suitable for VS simply do not currently exist and would be very costly to acquire, develop and maintain.

11. VA: Assessing the severity of vulnerabilities in the context of an isolated PT with proprietary hardware and software is much more difficult than in the enterprise context. Automated severity scores generated by scanners using the CVSS will almost necessarily be wrong as they fail to consider the impact of vulnerabilities within the context of the environment in which they are found (military PT vs. enterprise network). A reliance on

[16] Kyle Coffey et al., "Vulnerability Analysis of Network Scanning on SCADA Systems," *Security and Communication Networks* 2018 (March 13, 2018): 1–21, doi:10.1155/2018/3794603. 9.

[17] "A Look at the Threats to Air-Gapped Systems - Security News - Trend Micro USA," accessed October 25, 2019, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-look-at-the-threats-to-air-gapped-systems.

the severity assessments provided by enterprise scanning tools would lead to the misallocation of remediation resources. In the alternative however, manually contextualizing and assessing vulnerability severity requires a security analyst with a detailed understanding of the security architecture of the impacted system and few analysts currently exist with the necessary skill sets.

12. VR: The application of security patches is problematic with respect military systems that are certified for use prior to employment. Take for example the combat suite aboard a Halifax Class ship. Prior to deployment the combat system software version is fixed, and ship's crew and systems are "worked-up" over a period of months, ultimately leading to the achievement of their Weapons Systems Certification (WSC) prior to leaving on deployment. Updating any component of the software after this time would effectively void the technical component of the WSC, and would thereby necessitate recertification before weapons could be fired. Within the ICS domain (which is very similar to the PT domain), it has been shown that patching vulnerabilities can be unexpectedly disruptive to operations and often ineffective due to the overall underlying network design and implementation.[18] As a result, the urgency associated with patching an isolated system is generally very different from the urgency associated with patching a connected enterprise system and should therefore be much more carefully considered.

13. Proactive, Risk Based VM of PT. As an alternative to the reactive approach taken to the Spectre/Meltdown vulnerability disclosure, a proactive, lifecycle approach to VM has since been proposed whereby a tailored VM plan is put in place when PT is brought

[18] "Industrial Control Vulnerabilities: 2017 in Review" (Hanover, MD: Dragos, Inc., March 1, 2018), https://dragos.com/wp-content/uploads/2017-Review-Industrial-Control-Vulnerabilities.pdf.

into service.[19] In this approach, during project definition for a new military system, risk based cyber security requirements are established as a necessary deliverable which then drive the scope and scale of VM activities required through life. Upon being brought into service, similar to an equipment maintenance schedule, a VM schedule may be issued with specified intervals for VD, VS, VA and VR activities based on the priorities established by the operational authority during the requirements phase for the system.

14. This approach has particular advantages with respect to military PT as it enables whole life costs associated with vulnerability management to be identified in advance and included within the capital sustainment costs that are approved as part of new capital projects. In addition, having VM requirements determined in advance of capability acquisition ensures these activities will be scheduled and executed throughout the equipments lifecycle thus preventing the inefficient expenditure of resources when the disclosure of public vulnerabilities would otherwise demand a crisis level reaction.

CONCLUSION

15. Within an enterprise IT context, centralized control enables centralized coordination and execution of VM activities across the enterprise. Unlike this model, the Mat Grp response to the Spectre/Meltdown disclosure was decentralized, largely reactive and resulted in the expenditure of a significant amount of effort with a minimal return on investment. This type of response is neither sustainable nor scalable in the future cyber

[19] Jordan Burkhart, "System Security Engineering Guidance - Vulnerability Management Framework" (Draft System Security Engineering Guidance, Director General Maritime Equipment Program Management, July 8, 2019). 2.

security landscape where more and more critical vulnerability disclosures will drive a desire for further reactive reporting in the absence of a robust VM framework.

16. In order to achieve economies of scale, there is often a preference to reuse processes and tools to the extent possible within an organization. While mature VM practices exist within the enterprise IT domain, their wholesale application to the PT domain are not necessarily appropriate given the different challenges associated with each of the VM activities. More specifically, the lack of VD on proprietary systems and the potential consequences of conducting VS on deployed systems provide strong reasons to carefully consider the wisdom of adopting the enterprise toolset for VM. Moreover, the lack of expertise to perform VA and the different threat landscape affecting the urgency of VR activities are also good reasons to challenge the status quo with respect to the adoption of the enterprise mindset vis-a-vis VM when it comes to PT.

RECOMMENDATION

17. As detailed in the preceding, the VM approach for enterprise IT is not compatible with the operational realities of PT and as such those practices are not recommended for wholesale adoption. While it is recognized that much progress must be made with respect to improving the cyber resilience of PT, the indiscriminate adoption of enterprise IT practices will only serve to consume otherwise limited resources without achieving the strategic effect intended. The concept of taking a lifecycle, risk based and proactive approach to VM is novel and shows much promise. Given that the CAF does not have enough resources to defend all systems to the n^{th} degree in cyberspace, it only makes sense that the extent to which VM activities occur through life should be pre-determined

and accounted for as part of the requirements definition process for new systems. As a result, rather than adopt enterprise IT processes and tools, it is recommended that the project directors within the CAF and the equipment program managers within Mat Grp work together to jointly adopt a proactive, lifecycle, risk based approach to the VM of PT.

BIBLIOGRAPHY

"A Look at the Threats to Air-Gapped Systems - Security News - Trend Micro USA." Accessed October 25, 2019. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-look-at-the-threats-to-air-gapped-systems.

"AL18-001: Meltdown and Spectre Side-Channel Vulnerabilities." December 21, 2018. https://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2018/al18-001-en.aspx.

Burkhart, Jordan. "System Security Engineering Guidance - Vulnerability Management Framework." Draft System Security Engineering Guidance, Director General Maritime Equipment Program Management, July 8, 2019.

Coffey, Kyle, Richard Smith, Leandros Maglaras, and Helge Janicke. "Vulnerability Analysis of Network Scanning on SCADA Systems." *Security and Communication Networks* 2018 (March 13, 2018): 1–21. doi:10.1155/2018/3794603.

"CVE - Common Vulnerabilities and Exposures (CVE)." Accessed October 23, 2019. https://cve.mitre.org/.

Finn, Patrick. "Computer Chips." E-mail, January 8, 2018.

"Implementing and Auditing the Critical Security Controls - In-Depth | Community." Accessed October 23, 2019. https://www.sans.org/community/event/sec566-ottawa-57780.

"Industrial Control Vulnerabilities: 2017 in Review." Hanover, MD: Dragos, Inc., March 1, 2018. https://dragos.com/wp-content/uploads/2017-Review-Industrial-Control-Vulnerabilities.pdf.

"ITSG-33 - Annex 2 - Information System Security Risk Management Activities." *IT Security Risk Management*, 2012, 113.

"Meltdown and Spectre." Accessed October 23, 2019. https://spectreattack.com/.

Moll, Robin. "BN - MEPM Cyber Vulnerability Assessment Plan." DND 317, Assistant Deputy Minister of Materiel, Cyber Mission Assurance, February 11, 2019.

"NVD - Vulnerability Metrics." Accessed October 23, 2019. https://nvd.nist.gov/vuln-metrics/cvss.

Page, Cmdre Simon. "Briefing Note to ADM(MAT) - Meltdown/Spectre Fleet Systems Reporting Proposal." Assistant Deputy Minister of Materiel, Cyber Mission Assurance, January 9, 2018.

"What Is Security Through Obscurity (STO)? - Definition from Techopedia." *Techopedia.Com*. Accessed October 24, 2019. https://www.techopedia.com/definition/21985/security-through-obscurity-sto.

Zetter, Kim. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." *Wired*, July 11, 2011. https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.