Measures and Metrics for the Enforcement of Critical Security Controls: A Case Study of Boundary Defense

Mohiuddin Ahmed, Ehab Al-Shaer
University of North Carolina at Charlotte
Charlotte, NC, USA
{mahmed27,ealshaer}@uncc.edu

ABSTRACT

The center for internet security (CIS) publishes a set of defense actions which forms a set of defense in depth best practices known as critical security control (CSC) to detect, prevent, respond, and mitigate the cyber attacks against cyber systems and networks. However, no well defined automated measures and metrics are developed to validate the enforcement of these CSCs. Additionally, it is infeasible to directly analyze the implementation of security products to verify and validate the enforcement of CSCs in those security products. In this poster, we are going to present our preliminary analysis to develop automated measures and metrics for CSC based on threat model each CSC is targeting, measurable features, and cyber artifacts which can be used to create metrics for key enforcement indicators. We also present a case study to develop measures and metrics for a CIS CSC called boundary defense.

ACM Reference Format:
Mohiuddin Ahmed, Ehab Al-Shaer. 2019. Measures and Metrics for the Enforcement of Critical Security Controls: A Case Study of Boundary Defense . In *Hot Topics in the Science of Security Symposium (HotSoS), April 1–3, 2019, Nashville, TN, USA.* ACM, New York, NY, USA, 3 pages.

1 INTRODUCTION

The center for internet security (CIS) [3] publishes 20 critical security controls which contain in total 171 sub-controls. According to CIS, these CSCs provide guidelines not only to block the initial compromise of the cyber systems but also to detect already compromised systems and prevent or block post-compromise adversaries' actions. These guidelines also provide ways to reduce the attack surface by hardening device configurations, identifying compromised systems, and disrupting attackers' command and control communications. These CSCs are now widely used in both industry and government organizations to enhance and enforce cybersecurity. There are many solution providers who claim to implement these top 20 critical security controls. For instance- Rapid7 global service [5] implements top 20 critical security controls and verified by SANS [5] as a top solution provider. AlienVault [2] is also known as a top solution provider for top 20 critical security controls. Moreover, a genuine effort has been made by NSA, NIST and other cybersecurity counsels to establish these CSCs as a standard or best practices to enforce cybersecurity.

However, CIS critical security controls (CSC) provide only guidelines to enforce cybersecurity. No automated enforcement or measurability mechanisms for these CSCs has yet been developed. Additionally, analyzing the implementations of security products to validate the enforcement of CSC is infeasible. Thus, it is quintessential to develop formal- and data-driven approaches and automated tools to measure effectiveness and validate the enforcement of CSC deployment. We can formulate the problem in the following way- if a company X has invested in Y products to implement Z CSCs, our goal is to identify metrics and measurement procedures to test and evaluate the quality of CSC enforcement by these products quantitatively.

2 OBJECTIVE AND TECHNICAL APPROACH

In this poster, we will present our preliminary work to identify metrics and measurement procedures for each CSC subcontrol to validate the enforcement of CSC deployment. Specifically, this poster will address the following objectives to identify metrics and measurements to validate CSC enforcement in security product under test (PUT)-

- Identify what threat actions each CSC subcontrol are targeting.
- Determine key measurement indicators (KMI) or cyber measurable features that can be computed for each CSC subcontrol.
- Determine the cyber observables of each CSC subcontrol that can be used to identify KMI.
- How to compose KMI to develop metrics for the key enforcement indicators (KMI) which will quantitatively assess quality attributes of each CSC subcontrol enforcement.
- Determine the measurement category and the measurement approach for each CSC subcontrol.
- Develop active and passive measurement methodologies and techniques to measure the enforcement of each CSC subcontrol.

To develop the measures and metrics for the validation of CSC enforcement, the first step is to identify the threat model of each CSC subcontrol that determines what the adversary can do in the absence of this specific CSC subcontrol. For instance- the absence of CSC 13 (Data Protection) implies the lateral movement of the attacker and exfiltration of sensitive data. Next, *Key Measurement indicators (KMI)* will be determined based on the identified cyber observables or artifacts of each CSC subcontrol. Each *KMI* is a concrete and objective attribute for the corresponding CSC subcontrol,

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, April 1–3, 2019, Nashville, TN, USA
© 2019 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-7147-6/19/04.

such as- the number of detected malicious IP address, the number of the unused IP address in the target organization. The next step is to compose different *KMIs* to develop metrics for *KEI* which will be used to assess the quality of the CSC enforcement. Each *KEI* is an abstract and subjective attribute, such as- Coverage or percentage of malicious IP that can be detected, Freshness or how fast a new asset is discovered by the PUT.

Moreover, four categories for CSC has been identified by analyzing all subcontrol based on their measurability or verifiability. One such type is *General* which indicates that the subcontrol in this category offers high-level guidelines and it is needed to be more specific. The next category is *Checklist* which indicates that the subcontrol under this category can be verified by using scripting such as CIS CSC subcontrol 6.1 [3]. A CIS CSC subcontrol is considered in the category of *Verifiable Properties* if we can verify it using configuration and vulnerability analytic such as subcontrol 12.1 where we have to analyze the network configurations to find out reachable hosts. The final category is *Measurable* which indicates that subcontrol under this category can be verified by using data-driven analysis based on logs, network traffic. For instance- we can verify usage of time server in subcontrol 6.1 by analyzing network traffic logs directed towards known time servers.

Additionally, four types of CSC enforcement measurement approaches are identified by analyzing the CSCs. One such approach is *Vulnerability Analytic* which will use intended services' vulnerability score (CVSS) to measure the deployed CSCs' effectiveness. *Data-Driven Approach* will use network traffic statistics such as NetFlow data, DNS traffic, and web traffic data to measure the effectiveness of the candidate subcontrol. The next approach is *Model-Based Approach* which will use configuration of the system and network to validate the enforcement of the corresponding subcontrol. The *Active testing* approach will be used to validate a subcontrol if it is necessary to send probe for measurement. The *Cyber Threat Intelligence* based approach will use indicators of compromise(IOCs), threat feeds, and malicious actor intents, opportunities, and capabilities from CTI reports to develop CSC effectiveness measurement. Finally, active and passive measurement methodologies will be developed based on the identified CSC category(*General, Checklist, Verifiable Properties, and Measurable*) and measurement approach(*Data-Driven, Model-Based, Active testing, Vulnerability analytic, and Cyber Threat Intelligence*).

3 CASE STUDY OF BOUNDARY DEFENSE

In this section, we are going to present a case study of CSC 12 called *Boundary defense* to demonstrate the steps to develop measures and metrics to validate the enforcement of this CSC. According to CIS [3], enforcement of CSC 12 will enable detection, protection, and correction of flow of information transferring network by focusing on security damaging data. It recommends that boundary defense should be multi-layered and relied on firewalls, proxies, DMZ, and network-based IDS and IPS. Thus, the absence of this CSC will provide ways to bypass boundary defense, launch denial of service attack and exfiltrate data. This CSC contains 12 subcontrols from which we are going to analyze one to develop measures and metrics for the validation of this subcontrol enforcement.

The subcontrol 12.2 of boundary defense CSC states that perform *regular scans* from outside of each trusted network boundary to detect any *unauthorized connections* which are accessible across the boundary. The observables or cyber artifacts of this subcontrol is the configuration of the networks and network traffic directed towards the unauthorized hosts or dark spaces. The quality attributes we have to calculate for this subcontrol are the detection rate of unauthorized connections and whether PUT is performing the regular scan or not. Therefore, the KMI will be the *total address space (m), total host (t), number of unauthorized hosts from outside (n), average number of used port (p)*. Since we have to use the configuration of network and network traffic logs for this subcontrol, the category of this subcontrol is *Verifiable and Measurable*. For the same reason, the evaluation method will be *Data-Driven and Model-based*. Since we have to send active scanning probe to outside, another evaluation method will be *Active Testing*. Moreover, the passive monitoring of the network traffic can be used to measure following KMI- *number of detected connections to dark spaces (M_3) and the number of connections to unauthorized servers (M_4)*. The number of scanning probe sent by PUT (M_1) and number of total possible combination of destination (M_2) will be calculated using traffic logs and configuration where $M_2 = t \times \#ports \times 2 + t \times \#ICMPType$. The identified KMIs will be composed together to develop following KEIs-

Scan Coverage (SC) defines the ratio of the scanned address space by the product under test (PUT) to the total address space where $SC = \frac{M_1}{M_2}$.

Scan Efficiency (SE) denotes the ratio of the detected unauthorized connections to the total scanning probes sent, $SE = \frac{M_3}{M_4}$. We will also measure the scan efficiency by measuring the actual host distribution (p) and the scan distribution (q) for a feature i using Kullback-Leibler divergence, $D_{KL}(p||q) = -\sum_i p(i) \log \frac{p(i)}{q(i)}$ where i is the distance between every two consecutive IP address in the network.

Detection Efficiency of the Unauthorized Connections defines the probability that unauthorized connections will be detected. Following three metrics will be used to determine the detection efficiency-

- Probability that a scan will hit unauthorized host= $\frac{d}{m} \times \frac{n}{m}$.
- Probability that a scan will hit unused address= $\frac{d}{m-t}$.
- Probability that a scan will hit unused port= $\frac{d}{t \times (2^{16}-p)}$.

where d is the number of distinct scanning probes sent.

To measure the Key measurement indicators, we will use passive monitoring of network traffic, statistical testing based on probabilistic scanning, and active testing by performing exhaustive scanning.

4 FUTURE WORKS

This preliminary analysis of CIS critical security controls reveals that every CSC enforcement can be validated by developing metrics for key enforcement indicators based on threat model each CSC targetting, cyber artifacts, and key measurement indicators for each CSC. In the future, we are going to analyze all of the CIS CSC to develop metrics for KEI calculation which will validate enforcement of each CSC. We are also going to develop automated tools [1, 4] to

measure the KMI which will be used to calculate the KEI to validate the enforcement of the CIS critical security control.

REFERENCES

[1] E. Al-Shaer, W. Marrero, A. El-Atawy, and K. ElBadawi. 2009. Network configuration in a box: towards end-to-end verification of network reachability and security. In *2009 17th IEEE International Conference on Network Protocols*. 123–132. https://doi.org/10.1109/ICNP.2009.5339690

[2] AlienVault 2019. AlienVault OSSIM. Retrieved March 1, 2019 from https://www.alienvault.com/products/ossim

[3] CIS 2019. Center for Internet Security. Retrieved March 1, 2019 from https://www.cisecurity.org/controls/

[4] M. A. Rahman and E. Al-Shaer. 2013. A Formal Framework for Network Security Design Synthesis. In *2013 IEEE 33rd International Conference on Distributed Computing Systems*. 560–570. https://doi.org/10.1109/ICDCS.2013.70

[5] Rapid7 2019. Rapid7 Global service. Retrieved March 1, 2019 from https://www.rapid7.com/solutions/compliance/critical-controls/