Cyber Defense Matrix – A New Model for Optimal Composition of Cybersecurity Controls to Construct Resilient Risk Mitigation

Ashutosh Dutta, Ehab Al-Shaer
University of North Carolina at Charlotte
Charlotte, North Carolina
{adutta6,ealshaer}@uncc.edu

ABSTRACT

Most enterprises aiming to deploy cost-effective security configuration follow information security standards and guidelines to adopt cybersecurity controls such as CIS Critical Security Controls (CIS CSC) [2]. With the increased dependency over cyber, the landscape of cyber attacks is escalating quickly, and as a consequence, hundreds of cybersecurity controls have to be delineated to implement NIST Cybersecurity Framework (i.e., identify, protect, detect, respond and recover) [6]. The security configuration comprised of the appropriate set of security controls requires not only to be optimized regarding *Return on Investment (RoI)* but also to be resilient in order to tackle the failures against diversified cyber attacks. However, the composition of such optimal and resilient cybersecurity portfolio (security configuration) is a highly complex and error-prone task as there are exponential numbers of ways to construct a portfolio due to a large number of security controls, threats, resource, and usability constraints.

The objective of this research is to develop a novel and an automated approach to compose the optimal and resilient risk mitigation planning by selecting the most critical security controls (CSC) considering affordable residual risk (risk appetite), budget, resiliency, and enterprise-oriented usability constraints. We developed a model named *"Cyber Defense Matrix (CDM)"* that resemblances the deployed cyber defense strategy. The structure of CDM incorporating three dimensions: Security Function (what), Enforcement Level (where), and Kill Chain Phase (why) enables the composition of multi-layer and multi-stage resilient defense configuration. Our approach leverages CDM to determine which security controls are needed for "what" security function (Identify, Protect, Detect, Respond, and Recover), "where" each security control should be enforced in the cyber systems (Network, Device, People, Application, and Data), and "why" they are effective (i.e., against what attack and wherein the kill chain). We formulate the approach to compute the resilient cybersecurity planning as CDM using SMT constraints.

1 INTRODUCTION

Institutions such as academia, industries, and government agencies have made efforts over the years to create guidelines for security controls. These guidelines highlight the de facto standard approaches for risk measurements and risk mitigation against sophisticated and evolving cyber attacks. One example of such effort is CSC [2] that recommends the set of actions to provide an effective defense against pervasive and advanced attacks. However, it is practically and economically infeasible to deploy all the security controls due to resource and diversified usability constraints. Therefore, besides ensuring resiliency as per enterprise requirements, the risk mitigation planning must also be able to select the appropriate set of countermeasures which guarantees the optimized cost-effectiveness concerning RoI. However, to compose such a resilient and cost-effective security portfolio, an exponential number of control compositions need to be explored. Moreover, the situation exacerbates because of the heterogenous resiliency policies across the enterprises.

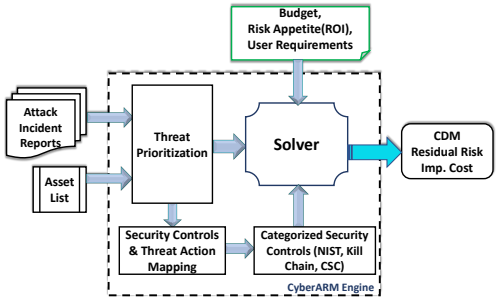


Figure 1: Decision-making Framework

Decision-making to discover proactive and resilient risk mitigation is a highly complex and error-prone for the following reasons. First, it is necessarily a multi-dimensional decision-making process that must consider multiple factors including attack incidents, mission-based risk appetite, and budget constraints. Second, the computational complexity required for such risk planning grows non-linearly with the increase of the asset size, especially with the increase of the types of the assets. Third, the semantic gap between the descriptions of the security control guidelines and threat actions enabled by the vulnerabilities and weakness hinder the automated mapping of applicable security controls with the relevant set of threat actions. Fourth, there exists a lack of mechanisms to cope with the inevitable failures of security controls against the broad threat landscape. As a consequence, the current ad hoc and manual techniques adopted by the enterprises for selecting the most critical security controls cannot systematically yield to measurable values of risk mitigation (i.e., RoI) and resiliency.

The three key decision-making elements that each cybersecurity analyst seeks to determine is "what" security controls (and security functions), "where" to deploy effectively, and "why" or for what purpose. Cyber Defense Matrix (CDM) is a multi-dimensional

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.
https://doi.org/10.1145/3314058.3317725

model that integrates these questions as three dimensions: (1) security function based on NIST Cybersecurity Framework [6], (2) enforcement level (network, devices, people, application and data), (3) attack Kill Chain. Moreover, it segregates the cyber defense into many phases to enforce the divide and conquer strategy against the continuum of sophisticated cyber attacks, while enabling the satisfaction of the resiliency requirements such as defense-in-depth, multi-layer, and multi-control k-resiliency. The CDM model and formal techniques developed in this project provide a new groundbreaking solution for automated risk mitigation decision-making that guarantees the satisfaction of mission-based risk appetite, RoI, and resiliency requirements.

We formulate the problem of finding the cost-effective and the resilient CDM as a Constraint Satisfaction Problems, where all the requirements regarding budget, affordable residual risk, minimum RoI, resiliency policies, and other user requirements are introduced as constraints. Besides, our developed algorithm decomposes this computationally complex problem into multiple similar sub-problems to improve the scalability of decision making for enterprises with a large number of distinct cyber assets. We compute and verify the generated planning to check its compliance with the constraints using an SMT verification solver, Z3Prover/z3 [1].

The project presented in this paper contains the following novel capabilities:

- The main contribution is the development of an automated decision-making approach to compute a resilient set of security controls and the corresponding countermeasures (cybersecurity products), which is also cost-effective and multi-dimensionl.
- Another contribution is the development of a pragmatic data-driven threat prioritization framework by quantifying the risks imposed by threat actions based on the probabilistic model developed using threat incident reports.

The previous researches on optimizing the decision-making to eliminate the cybersecurity risks are too general [3, 4, 7, 8]. Moreover, no previous work addresses the problem of risk mitigation through selecting the optimal set of security controls and also considering the correlations among threat actions.

2 TECHNICAL APPROACH

Fig. 1 shows the architecture and the workflow of our decision-making framework. Our framework executes the following steps sequentially to compute the resilient and the cost-effective CDM with its residual risk and the implementation cost if deployed:

- **Threat Prioritization:** In this step, the framework calculates the probabilities of exerting the combinations of threat and threat action pairs against the assets of user-given "Asset List" using "Attack Incident Reports", where a threat may use one or more threat actions and vice versa. The output of this step is the prioritized set of threat actions.
- **Identifying Candidate-set of Security Controls:** We require the mapping between security controls and threat actions to determine the candidate-set of security controls for the prioritized set of threat and threat actions. In order to do so, we apply text mining to categorize the descriptions of security controls into one or more threat actions using word2vec (to bring semantic features)[5]. Besides, these security controls are categorized

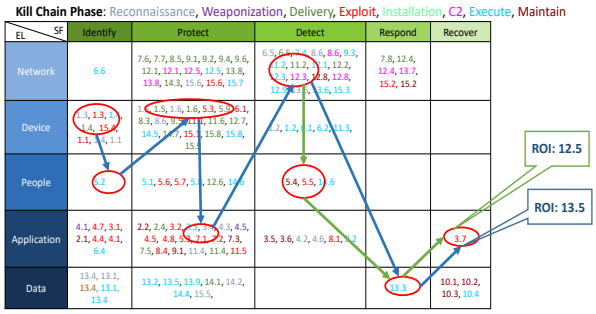


Figure 2: Cyber Defense Matrix in Action - An Example

based on three fundamental properties of security controls: Security Function (SF), Enforcement Level (EL), and Kill Chain Phase (KC phase), which are three dimensions of CDM.

- **Finding optimized CDM:** We apply Z3Prover [1] as SMT-Solver to choose the subset of the candidate-set of security controls to fill each phase of CDM structure, while ensuring the orchestration of security controls among the phases of CDM concerning cost-effective risk mitigation and resiliency.

In Fig. 2, rows and columns represent EL dimension and SF dimension of CDM, whereas Kill Chain Phase represents the third dimension of CDM. Our framework recommends patterns like in Fig. 2 as CDM to its users. The blue pattern shows the most cost-effective portfolio, whereas the green pattern deviates in the "Detect" column as the user wants more resiliency in detecting the threat actions.

3 PRELIMINARY FINDINGS

Based on the preliminary experiments, we discover two findings. First, a model reduction approach based on the cost-effectiveness of products can improve RoI while reducing the complexity significantly. Second, the complexity of a problem largely depends on the number of assets, risk tolerance (the difference rate between the risk appetite and the achievable minimum residual risk), and budget gap (the difference rate between the maximum cost to implement all products of candidate-set and the given budget).

REFERENCES

[1] *The Z3 Theorem Prover.* https://github.com/Z3Prover/z3.
[2] Center for Internet Security 2018. *CIS Controls Version 7.* Center for Internet Security. https://www.cisecurity.org/controls/.
[3] Andrew Fielder, Emmanouil Panaousis, Pasquale Malacaria, Chris Hankin, and Fabrizio Smeraldi. 2016. Decision support approaches for cyber security investment. *Decision Support Systems* 86 (2016), 13–23.
[4] Robert J Kauffman and Ryan Sougstad. 2008. Risk management of contract portfolios in IT services: The profit-at-risk approach. *Journal of Management Information Systems* 25, 1 (2008), 17–48.
[5] Tomas Mikolov, Kai Chen, Greg Corrado, and Jeffrey Dean. 2013. Efficient estimation of word representations in vector space. *arXiv preprint arXiv:1301.3781* (2013).
[6] National Institue of Standards and Technology. *Framework for Improving Critical Infrastructure Security.* National Institue of Standards and Technology. https: https://www.nist.gov/sites/.
[7] Loren Paul Rees, Jason K Deane, Terry R Rakes, and Wade H Baker. 2011. Decision support for cybersecurity risk planning. *Decision Support Systems* 51, 3 (2011), 493–505.
[8] Valentina Viduto, Carsten Maple, Wei Huang, and David LóPez-PeréZ. 2012. A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem. *Decision Support Systems* 53, 3 (2012), 599–610.