World Journal of Advanced Engineering Technology and Sciences

eISSN: 2582-8266

Cross Ref DOI: 10.30574/wjaets

Journal homepage: https://wjaets.com/

(Review Article)

Evaluation of the cyber security models implemented across common attack vectors: A review of literature

Afra Ansaria *

SIGMOID, San Francisco, California, U.S.A.

World Journal of Advanced Engineering Technology and Sciences, 2024, 11(01), 064–068

Publication history: Received on 06 December 2023; revised on 19 January 2024; accepted on 22 January 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.11.1.0023

Abstract

Cybersecurity is an organizational issue that should be looked at through the lens of various stakeholders. However, it is often treated as a siloed issue in which more is always seen as better. The CISOs, CIOs, and the key decision-makers struggle to understand how much security is enough. Cybersecurity solutions, referred to as controls, more often than not result in a residual risk. To assess this risk better, the security controls should be studied in further detail. The objective of this paper is to educate the audience with the various cyber security controls being used in the academia and in the industry. In order to circumvent the security issues faced by large organization, the tradeoffs of each controls should be studied further. The paper is meant to provide a balanced view providing the positive and the critical aspect of implementing some of the known security solutions. There is no one perfect formula when it comes to selecting security controls. However, picking a security control that are in line with the users' needs will help reduce some of the risks associated with implementing the controls. An optimal solution requires a balanced approach towards the risk, cost, and benefit of the solution. The aim of the paper is to help the reader assess some of risks and the tradeoff associated with the security controls being practiced in the industry today.

Keywords: Cybersecurity; Zero-Day Attacks; Attack Planner; MulVal; Attack Capability Graph

1. Introduction

Cybersecurity is an organizational issue. In reality, however, the issues related to cybersecurity are more often than not treated in siloes. Managed by the security experts and the risk teams, the cybersecurity solutions are often endless, where more is always seen as better. It is no surprise that the cybersecurity industry is filled with varied solutions, paving the way for a long list of vendors. The Chief Information Security Officers (CISOs) [1], who are responsible for the security of the organization, are often faced with challenges in choosing the right solutions that can make their organization more secure. While the common wisdom might support the idea that adopting more solutions should result in better security, there is a lack of understanding of the methods available to curb the security risks. This paper provides a literature overview on some of the advanced methods proposed across the academia and the industry, thus helping the reader understand the landscape of the security controls better.

Cybersecurity solutions, termed as controls, are often looked at through the lens of various stakeholders. Each of these stakeholders demands a different priority. Organizations end up optimizing the cybersecurity risk at the loss of overall benefit to the company, resulting in high investment toward potentially redundant resources.

In most cases, each of the controls results in a tradeoff between the cost and the overall benefit of implementing the controls. To optimize the security measures, there is a need to balance between the cost, the benefit, and the risk associated with the implementation of such security controls.

* Corresponding author: Afra Ansaria

2. Literature Review

Security measures matter to every stakeholder in an organization. A good security measure considers various factors that play a key role in the life cycle of the organization's development. In [6] Lihua Yin et al. considered the security measurements for unknown threats based on the attack preferences. In the paper, zero-day attacks are considered long-term processes. They presented a long-term game theory to predict the behavior of the attacker and then proposed a security metric based on the prediction. Factors that affect the attack and defense mechanisms were investigated and the prediction of the attacker's behavior was fine-tuned based on observation and information sharing. Each attack and defense move was divided into a subgame and Nash equilibria were used to calculate the attacker's next possible move. In [7], Wang et al. proposed ways of representing the measurements of zero-day attacks. The paper used attack graphs to analyze the minimal number of vulnerabilities needed to achieve a specific goal, assuming there are unforeseen vulnerabilities on any of the nodes. This number was used as a reference for security measures. The paper measured the security from the dimension of complexity of the attack and does not consider the defender's preference.

In [8] Hardy et al. proposed a targeted threat index that combined the sophistication of social engineering and technical attacks. In [9] Thakore proposed a set of metrics that included redundancy, confidence, coverage, and the cost to quantitatively evaluate deployments. In [10], Ekelhart et al. looked at the attackers' behaviors and the attackers' strategies with a simulation-driven approach. In [11] Jarrah and Arafat used a time-delay neural network that considered the temporal behavior of the attackers. In [12] the strength of the IDS and the strength of the password were evaluated. In [13] Mitchell and Chen looked at ways different attack types such as random or opportunistic attackers can be treated. In [14], Allodi et al. showed that not all vulnerabilities are equally exploited by the attacker and proposed the possible choice of the attacker. Dumitras [15] proposed a more accurate assessment of the risk of cyberattacks using a novel metric. In [16] Bozorgi et al. represented ways of using machine learning to predict the vulnerabilities which are more likely to be exploited by the attacker.

The security of the deployed and active systems is often a moving target that requires more thorough security metrics. Such security metrics are difficult to assess. In [18] code-based metrics were shown to exhibit a significant correlation with security vulnerabilities. Calculating the attack surface metrics can require access to the source code of the product and the composition of its deployment. Kartik Nayak et al., in [18], sought to solve this problem by looking at empirically validated metrics. In the paper, several security metrics derived from the field data were explored to get a better picture. Metrics such as the total count of vulnerabilities exploited and the size of the attack surface exercised in the real-world attack were analyzed. By examining these metrics, the author showed that more than 35% of the disclosed vulnerabilities exploited in the wild did not show in any of the products in the study. They suggested metrics such as the exploitation ratio and the exercised attack surface. They found that with the upgrade to newer product releases, the exercised surface attacks decreased. In similar works, Ozment et al. [17] studied the rate of vulnerability disclosure in OpenBSD and proposed a vulnerability growth model that could discover the number of vulnerabilities left undiscovered. In [19] Shin et al. studied metrics such as code complexity, code churn, and the developers' activity to predict the vulnerable code location. In [20], Howard proposed the attack surface metric as a weighted combination of communication channels, protocols, targets, and enables.

Manadhata et al. [21] investigated the attack surface as a combination of entry and exit points, the channels, and the untrusted data items. In [22], Kurmus defined the attack surface using a call graph, a set of entry functions, and a set of barrier functions.

Zero-day Attacks are one of the most notorious exploits that are hard to measure. The security risks of unknown vulnerabilities are unmeasurable since they are less predictable.

Several works have attempted to define the network security metrics for such zero-day vulnerabilities. In [23] Lingyu Wang et al. proposed a novel security metric called k-zero- day safety. Instead of ranking unknown vulnerabilities, they proposed a metric that counted the number of vulnerabilities that would be required to compromise the network. The larger count implied higher security since the probability of having more unknown vulnerabilities that can be exploitable all at the same time will be significantly lower. In their paper, the new metric was defined and analyzed and a heuristic algorithm was devised for intractable cases and finally applied to the existing network practices. In [24], Leyla Bilge et al. proposed a method for identifying zero-day attacks based on field-gathered data. This data represented all the benign and malicious binaries that were downloaded on more than 11 million real hosts across the globe.

The data set was used to identify the malicious files that were exploited before the corresponding vulnerabilities were disclosed. The paper suggested that a typical zero-day attack lasts 312 days on average after the vulnerabilities are disclosed publicly. Meanwhile, the number of attacks exploiting such vulnerabilities increases by a magnitude of more than 5.

Studies that look at benchmarks focus on performance and reliability evaluations, however, some benchmarks consider the sensitive code and data for computer security. Based on this, Tudor et al [25] proposed the Worldwide Intelligence Network Environment (WINE), a security benchmarking approach based on experimental methods. WINE allows researchers to gather insights on the security arms race.

In the arms race between the attacker and the defender, new defenses are built to stop a specific attack vector but sophisticated attackers are likely to bypass such defenses. A strategic reason for the protection offered by the defenses, the coverage of the defenses, and the possible new vectors of attacks should be looked at further to keep up with the attackers. In [26] a framework called QUASAR, Quantitative Attack Space Analysis and Reasoning was proposed. The framework was used to systematically analyze the attacks and the defenses at the granularity of the technicalities necessary to execute the attack. The paper presented attack models in the memory corruption domain and represented the prominent defenses in the domain. The framework was used to compare defenses at the fundamental level, reason about the coverage of the new defenses, and also to hypothesize about the new attack strategies that are possible. The defense coverage was represented as the difference between the number of attack methods available when a defense was deployed, to the number of attack methods available when no defenses were deployed. This is further normalized on [0, 1] intervals, in which a higher value corresponds to higher coverage, i.e. lower number of successful attacks. QUASAR proposed each attack class with a set of fundamental capabilities that are required to be present for an attacker to be successful in carrying out the attack. These capabilities may further be composed of finer-grained capabilities and combined with AND/OR operations in a graph-like structure, called the Attack Capability Graph (ACG). A defense is represented as a set of constraints on the ACG which disables a few of the branches (capabilities) in the Attack Capability Graph. The ACGs are then used to specify the impact of each defense and compare the defenses that shed light on how the defenses can be done instead of what the defenses do.

The severity of an attack can also be realized using an attacker score and the corresponding defense measures can be looked at using probabilistic methods. In [27], Raydon et al. proposed a SPAR framework that used a Probabilistic Attack Graph to reason about the security methods of the network. Using the MulVal attack planner and the CVSS metrics, a probabilistic attack graph was formed. A network reachability graph was also computed using the SDN controllers. A security analyzer was then used to generate near-optimal countermeasures for the attacks. At first, the attacker score was calculated using the probability of risk across each of the attack nodes. The best sequence of attack was then picked as the best possible attack chosen by the attacker under a given set of conditions. The security controls were given a Boolean variable to denote if the control had been deployed against the exploit or not. Later a security objective was defined that considered the best attack sequence expected to be used by an attacker and the respective controls that were required to be placed. The output of the framework included routing decisions for the SDN devices as well as the mitigation strategies required by it. In [28], Vaibhav et al. looked for ways to score the attack graphs and thus proposed a ranking scheme for the states of an attack graph. The rank of a graph showed the importance based on factors like the probability of an intruder reaching the stage. Given a ranked attack graph, the decision-maker could focus on the relevant subgraphs to deploy the mitigation strategies. The paper also defined a metric of security based on the ranks the system administrator used to compare the attack graphs and determine the effectiveness of the mitigation strategies. Two algorithms were presented to rank the stakes of the attack graph. The first algorithm was inspired by the Page Rank algorithm used by Google to measure the importance of web pages. The second algorithm is used to rank individual states based on the probability of the reachability of the attacker.

Nayot et al. in [29] formulated a framework for the risk management of the organization using a Bayesian network that allowed the decision-maker to quantify the factors of network attacks at various levels. The paper showed ways to use such information to develop a security mitigation and management plan that would provide the decision-maker with all the trade-offs required to make decisions in a resource-constrained environment.

3. Conclusion

Deploying cybersecurity controls is a complicated problem. Not just in terms of execution but also in terms of picking the right control to mitigate any possible attack. For a given attack scenario, there may be multiple ways of combating the attacker. It is the choice of the security experts, the defenders, to pick controls that can prevent the attacker from inflicting further damage to the organization. The security experts, in most cases, hardly have insight into the overall effect of such choices and thus their decisions are limited by the technical biases that exist in their eco system. With a wide range of available controls available, it is important to select those that are aligned with the business goals of the organization. A high-cost control, technical or financial, doesn't necessarily imply that it is the best option available to circumvent the attack. Similarly, the common industry-standard controls might not imply that it is the best approach to improve the defenses of the organization.

As is the case in reality, there is no such thing as perfect security. Every security measure comes with a probability of success. In a given range of security choices, considering the probability of success would help improve the decision-making of selecting security controls. The objective of the paper is to study the various literature on cyber security controls. The methods proposed by various authors are studied providing the reader an insight into the risks and benefits of each security controls and perhaps leaving the reader with a better understanding of the current landscape of cybersecurity solutions.

Compliance with ethical standards

Acknowledgement

I am grateful to my mentor Dr. Howard Shrobe who helped guide me through the entire research

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Optimize Risk, Value and Cost in Cybersecurity and Technology Risk, https://www.gartner.com/document/code/466056

[2] National vulnerability database. available at: https://nvd.nist.gov/, May 9, 2021

[3] 2021 Cyber Security Statistics, https://purplesec.us/resources/cyber-security-statistics/

[4] Outcome-Driven Metrics for Cybersecurity in the Digital Era, https://www.gartner.com/document/3980892

[5] Michael McGeachie, Utility Functions for Ceteris Paribus Preferences, 2002

[6] Lihua Yin, Yanwei Sun , Zhen Wang: Security Measurement for Unknown Threats Based on Attack Preferences

[7] L. Wang, S. Jajodia, A. Singhal, P. Cheng, and S. Noel, K-zero day safety: a network security metric for measuring the risk of unknown vulnerabilities, IEEE Transactions on Dependable and Secure Computing, vol. 11, no. 1, pp. 30–44, 2014.

[8] S. Hardy, M. Crete-Nishihata, K. Kleemola et al., Targeted threat index: Characterizing and quantifying politically-motivated targeted malware, in Proceedings of the in USENIX Security Symposium, pp. 527–541, 2014.

[9] U. Thakore, A quantitative methodology for evaluating and deploying security monitors [Ph.D. thesis], 2015.

[10] A. Ekelhart, E. Kiesling, B. Grill, C. Strauss, and C. Stummer, Integrating attacker behavior in IT security analysis: a discrete- event simulation approach, Information Technology and Management, vol. 16, no. 3, pp. 221–233, 2015.

[11] O. Al-Jarrah and A. Arafat, Network intrusion detection system using attack behavior classification, in Proceedings of the 5th International Conference on Information and Communication Systems, ICICS 2014, pp. 1–6, April 2014.

[12] A. Milenkoski, M. Vieira, S. Kounev, A. Avritzer, and B. D. Payne, Evaluating computer intrusion detection systems: a survey of common practices, ACM Computing

[13] Surveys, vol. 48, no. 1, pp. 1–41, 2015. R. Mitchell and I.-R. Chen, Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications, IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 44, no. 5, pp. 593–604, 2014.

[14] L. Allodi and F. Massacci, Comparing vulnerability severity and exploits using casecontrol studies, ACM Transactions on Information and System Security, vol. 17, no. 1, article no. 1, 2014.

[15] T. Dumitras,, Understanding the vulnerability lifecycle for risk assessment and defense against sophisticated cyber-attacks, in Cyber Warfare, pp. 265–285, Springer, 2015.

[16] M. Bozorgi, L. K. Saul, S. Savage, and G. M. Voelker, Beyond heuristics: Learning to classify vulnerabilities and predict exploits, in Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD- 2010, pp. 105–113, ACM, July 2010.

[17] Ozment, A., Schechter, S.E.: Milk or wine: Does software security improve with age? In: Proceedings of the 15th Conference on USENIX Security Symposium - Volume 15. USENIX-SS'06, Berkeley, CA, USA, USENIX Association (2006)

[18] Kartik Nayak*, Daniel Marino†, Petros Efstathopoulos†, Some Vulnerabilities Are Different Than Others Studying Vulnerabilities and Attack Surfaces in the Wild

[19] Shin, Y., Meneely, A., Williams, L., Osborne, J.A.: Evaluating complexity, code churn, and developer activity metrics as indicators of software vulnerabilities. IEEE Trans. Software Eng. 37(6) (2011) 772–787

[20] Howard, M., Pincus, J., Wing, J.M.: Measuring relative attack surfaces. In: Workshop on Advanced Developments in Software and Systems Security, Taipei, Taiwan (Dec 2003)

[21] Manadhata, P.K., Wing, J.M.: An attack surface metric. IEEE Trans. Software Eng. 37(3) (2011) 371–386

[22] Kurmus, A., Tartler, R., Dorneanu, D., Heinloth, B., Rothberg, V., Ruprecht, A., Schr¨oder-Preikschat, W., Lohmann, D., Kapitza, R.: Attack surface metrics and automated compile-time os kernel tailoring. In: Network and Distributed System Security (NDSS) Symposium, San Diego, CA (Feb 2013)

[23] Lingyu Wang, Sushil Jajodia, Anoop Singhal, Pengsu Cheng, and Steven Noel k-Zero Day Safety: A Network Security Metric for Measuring the Risk of Unknown Vulnerabilities

[24] Leyla Bilge, Tudor Dumitras Before We Knew It An Empirical Study of Zero-Day Attacks In The Real World

[25] Tudor Dumitras, Darren Shou, Toward a Standard Benchmark for Computer Security Research

[26] Richard Skowyra, Steven R. Gomez, David Bigelow, QUASAR: Quantitative Attack Space Analysis and Reasoning 103

[27] Rayden Yongxiang CHIA, SPAR: An Autonomous SDN Intrusion Response Framework using Combinatorial Optimization over a Probabilistic Attack Graph

[28] Vaibhav Mehta, Jeannette M. Wing, Ranking Attack Graphs

[29] Nayot Poolsappasit, Indrakshi Ray, Dynamic Security Risk Management Using Bayesian Attack Graphs