Holistic Security Pattern-Based Model to Protect Network Architecture

Castro A. Yoga[a*], Anthony J. Rodrigues[a], Silvance O. Abeka[b]
[a*] cyoga@jooust.ac.ke
[a]Department Of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, Bondo, Kenya
[b]Department of Information System and Technology, Jaramogi Oginga Odinga University of Science and Technology, Bondo, Kenya

Abstract

The issue of network security holds significant importance in the contemporary interconnected global landscape, as networks encounter a wide range of both internal and external threats that can result in severe ramifications. The task of protecting networks continues to pose challenges, despite the implementation of security measures. These challenges arise from the growing complexity and rapidity of attacks, as well as misconceptions held by users. Current security solutions frequently focus on individual layers of the OSI model in isolation, resulting in potential weaknesses within the broader network. This study introduces a comprehensive conceptual model that integrates security patterns to effectively tackle network security concerns. The proposed model expands upon the OSI model by incorporating a human layer and dividing the network into three distinct layers: organization, host, and media. The systematic analysis of potential threats is facilitated through the utilization of anti-goals and attack surface identification. The retrieval of relevant attack patterns and the derivation of defensive control patterns are facilitated through the integration of the Comprehensive Attack Pattern Enumeration Classification Repository (CAPEC), enabling the performance of risk assessment. The proposed model presents a comprehensive and organized methodology for network security, offering network administrators practical recommendations for integrating security measures throughout all layers and improving overall network safeguarding.

Keywords:Network security; OSI Model; Holistic model,;Three Layer Network Security Domain (TLNSD); Comprehensive Attack Pattern Enumeration Classification Repository (CAPEC);Risk assessment; Security patterns.

1. INTRODUCTION

Networks are subjected to a plethora of internal and external attacks, the most of which have negative consequences (Ciampa, 2017)Despite the development and deployment of security measures, there are still numerous obstacles in safeguarding networks from attacks, which can be ascribed to increased attack sophistication, attack speed, and user misunderstanding amongst others (Ciampa, 2011)

The cost of correcting network vulnerabilities and the risks associated with them after installation are significant. Although numerous best practices, models and framework exist to address the problem of network security vulnerabilities, these approaches might be difficult to reuse because best practices are implementation-specific (Maher, 2016).As a result, there is a greater need to understand the fundamental causes of network security issues, where they originate, and what can be done to mitigate them. (Dougherty et al., 2009).

Securing a network can be a complex and stressful undertaking. To safeguard it, network administrators must first critically grasp how the network architecture is modelled. The Networks Architecture is described by the OSI Model divided into seven functional tiers, which outlines how networking is implemented and how data can be exchanged between computer systems via networking. Security and a methodical approach by administrators and developers to building, implementing, and administering a secure network are among the concerns that require important attention in these layers. All of these layers are vulnerable to attacks, necessitating the implementation of strong security safeguards.

According to (Szabo et al., 2015), the Network Architecture model has a fundamental design flaw in that it allows distinct layers to operate independently of one another, and information flows up and down to the next layer as data is processed. As a result, if one layer is compromised, communication can be jeopardized without the subsequent layer seeing anything wrong.

Presently, each security solution employs a unique mechanism, despite the fact that the challenges being

addressed at each level are generally the same (Small, 2012). There is rarely a comprehensive approach to the entire system. If this is attempted, it is possible that various models will be used in different areas of the network architecture. To guard against attacks, securing a network requires a holistic strategy, and the practice of relying on security components cannot secure the entire network if they do not work in concert and protect all aspects of the system It is essential to have a complete picture of the network's architecture and a unified security strategy targeting all of its layers, both of which can be attained by using security patterns(Kumar, 2014) The utilization of patterns provides a comprehensive outlook on security, which is a fundamental concept in the development of secure systems (Fernandez, 2009).

A holistic model that incorporates security throughout the network architecture is still lacking. We believe such an integrated model would facilitate the implementation of network security by providing network with guidelines for integrating security aspects across all network layers. This paper proposes a system view of the network architecture and a unified security approach targeting the network layers, leveraging security patterns to provide holistic security. In section 2 we present the literature review, while section 3 describes the theoretical assessment and development of the model. Section 4 concludes and indicated further work.

2. LITERATURE REVIEW

2.1. OSI Model Context in Network Security

Today's network and security engineers must be security-conscious and understand the networks they safeguard (Schumacher et al., 2013). Network-level safeguards such as firewalls and authentication measures may only stop a few threats. If one wants to properly secure the network, one requires a multi-tiered approach to security, and the OSI model is invaluable for this purpose (Eric, 2016). the Open Systems Interconnection (OSI) Model is a security framework that provides guidelines for ensuring application security across seven distinct layers. It is imperative that all seven layers are secured in order to establish a secure network (Solomon, 2016).

OSI Model's significance and applicability in network security have been shown by several writers. (Reed, 2003) applies the OSI Seven Layer Network Model to information security and shows that common security issues map directly to the model's logical constructs. The common information security threats and controls on each layer are examined and the Seven Layer Model's strategy for layer interaction proposed gives an insight into some of the challenges faced by concentrated, "single-layer" security solutions. This offers a holistic multi-layer approach based on network model layers rather than discrete solutions and logical or physical hardware layers to solve the problem (Reed, 2003).

(Pace, 2014) employs the seven layers of the OSI Model to present a rational, all-encompassing, and feasible strategy for safeguarding an enterprise's information assets. The authors' conclusion is that none of the layers in the model, when implemented in isolation, provides a significant level of protection. A thorough security solution entails the contemplation of all the layers of the OSI model.

(Martinović et al., 2014) proposed multiple strategies for implementing controls and safeguards across the different layers of the Open Systems Interconnection (OSI) model. The aforementioned observation highlights the attainment of granularity in network security, which progresses from general to specific security measures. This is accomplished with the aim of augmenting security through the integration of multiple layers of security, commonly referred to as "defence-in-depth". This principle posits that in the event of one security measure failing, another will assume its role.

2.2. Organization`s Context in OSI Model

While the seven-layer model is deemed sufficient for networking purposes, its application in the realm of network security necessitates the organization of certain concepts that fall beyond the purview of the conventional network model. In this regard, (Crutchley, 2002) highlights two crucial aspects that play a pivotal role in assessing a network's security posture, namely people and policy. This augments the model with two supplementary strata, whereby individuals engage with applications at layer eight, and policies govern the conduct of individuals (in principle) at layer nine.

According to (Greg, 2019) proposal, there exists an additional layer known as the human layer, where technology interacts with individuals. This stratum pertains to individuals and regulations. The rationale behind this assertion is that in addition to susceptible software and hardware serving as facilitators of attacks, individuals who lack security awareness can also be exploited as a source of vulnerability. The author suggests that there are two crucial matters that require attention at this level. Firstly, it is imperative to provide security

training to users to enable them to make informed decisions when confronted with security challenges. Secondly, it is essential to establish security policies, guidelines, and procedures to safeguard the organization against potential attacks. The conveyed information plays a crucial role in establishing the general atmosphere and shaping the perception of security within an organization. The absence of such information represents a significant vulnerability for many organizations.

According to (Gregg et al., 2006), despite the implementation of optimal security measures across the different layers of the OSI model, the susceptibility of networks to breaches through human error and employee actions underscores the significance of the "human layer" as the eighth layer in the OSI model. Therefore, a comprehensive network defence strategy must take into account this crucial layer.

2.3. Modularized, Layered Approach to Network Security

The principle of defence in depth is advocated by experts in the field of security. The principle posits that a multi-faceted approach to network security is necessary, involving the implementation of diverse techniques to safeguard the network. It is impossible to ensure that any security mechanism will be impervious to all forms of attack. Thus, it is imperative for each mechanism to possess a contingency mechanism (Richardson, 2022).

Adhering to a methodical and compartmentalized approach in the development and execution of network security measures can effectively tackle the diverse issues that are integral to security design. According to (Corgi, 2020), numerous security strategies have been devised in a disorganized manner, resulting in their inability to effectively safeguard assets and achieve the fundamental objectives of security.

The concept of modularity facilitates the maintenance of a simplistic and comprehensible nature for each constituent aspect of a design. The implementation of a design can be expedited and the need for extensive training for network operations personnel can be minimized through the utilization of simplicity. The process of evaluating a network design is facilitated by the presence of distinct and well-defined functionalities at every layer. The identification of transition points in a network facilitates the process of fault isolation, enabling network technicians to effectively identify and isolate potential points of failure.

The three-layer hierarchical model is advocated by Cisco as a modular approach. The proposed model partitions networks into distinct core, distribution, and access layers, thereby facilitating the process of devising and implementing security measures. (upravnik, 2016) suggests that organizations ought to construct network architectures that are hierarchical, modular, redundant, and secure, in accordance with their specific requirements. The utilization of hierarchy and modularity facilitates the construction of a network comprising numerous interconnected components in a structured and layered manner. The utilization of a hierarchical model has been shown to be advantageous in optimizing network performance, expediting design implementation and troubleshooting processes, minimizing expenses, and enhancing security measures (Tiso, 2011).

The comprehensive identification of potential attacks is a crucial aspect of engineering security in systems. This process enables the determination of essential security requirements and provides insights into the necessary security mechanisms and their underlying rationales. (Li, Horkoff, Paja, et al., 2015) presented a comprehensive framework for analysing attacks holistically, which examines various attack strategies from the perspective of an attacker. The framework utilizes a comprehensive system context, which is represented by a three-layer requirements model comprising of a social layer, software layer, and physical layer. This model serves as the domain model during the analysis of attacks. The framework generates a collection of diverse multistage attacks, which are subsequently mapped onto the three-layer requirements model to determine crucial security requirements

2.4. Identifying Attackers` Malicious Intentions

Thinking like an attacker constitutes an effective way to discovering attacks and attackers' malicious intentions within a network. The concept of anti-goals was initially introduced by (Lamsweerde, 2004) as a means of representing the malevolent objectives of an attacker with respect to the assets of a given system. The anti-goal model elucidates the process by which the attacker's conceptual anti-goals are transformed into concrete terminal anti-goals that can be achieved by the attacker, thereby encapsulating the attacker's tactics. Through the development of anti-goal models, analysts can proficiently recognize potential threats to a system and utilize this understanding to create secure systems.

Several papers have captured the rationale behind attacker actions using anti-goals, (Li, Horkoff, Beckers, et al., 2015)introduces a comprehensive approach for analyzing attacks. The methodology utilized in this study involves the utilization of goal modeling technique to effectively capture the malicious intentions of attackers as anti-goals. These anti-goals are then systematically refined and operationalized into concrete attack actions that are specifically targeted towards various assets such as human, software, and hardware. The integration of a Comprehensive Attack Pattern Repository (CAPEC) is a crucial aspect of the approach, as it equips analysts with practical security knowledge and enables them to identify potential attacks within specific contexts. Ultimately, a collection of security measures is furnished to alleviate detected security breaches.

The approach proposed by (Horkoff & Yu, 2016) incorporates security concerns across multiple levels of abstraction through the utilization of a three-tier, objective-driven requirements framework. Through the iterative process of refining root anti-goals into operationalizable anti-goals, it is possible to develop an attack strategy that encompasses a range of attack scenarios. This strategy can then serve as a basis for the derivation of relevant security controls. These methodologies not only encompass the potential attack surface, but also the attacker's tactics, such as contingency plans and the integration of multiple stages to accomplish a malevolent objective.

In order to address the disparity in knowledge between those who attack and those who defend, a methodical examination and enhancement of the malevolent intentions of attackers (i.e., anti-goals) should be undertaken, and a thorough collection of attack patterns known as the Comprehensive Attack Pattern Repository (CAPEC) should be utilized to translate attacker goals into tangible attack maneuvers. The selection of suitable security controls to effectively address potential attacks can be informed by the findings of the attack analysis. (Li, Horkoff, Paja, et al., 2015).

2.5. Identifying Network Attack Surface

The process of scrutinizing the attack surface is a methodical and effective approach to recognizing all plausible attack scenarios. This is a crucial step in conducting security analysis from the perspective of an adversary. The identification of operationalized attack surfaces holds significant importance in conducting focused security analysis.

The attack surface is comprised of one or more anti-goals that elucidate the malevolent intentions of attackers, thereby providing insight into the specific targets and timing of potential attacks. In order to effectively implement mitigation strategies, analysts must realistically identify potential attack vectors that malicious actors may utilize to compromise a system. (Li et al., 2016)has developed a framework that enables the generation of Comprehensive attack strategies. The framework facilitates a systematic exploration of attack strategies, resulting in more thorough and complete strategies that can enhance the overall security analysis. The researchers conducted a grounded study on three actual attack scenarios to examine the methods used by attackers to develop their malicious intentions in real-world situations. Through this analysis, they were able to identify five patterns of anti-goal refinement.

In a study conducted by Mylopous (2016), three actual attack scenarios were analysed in order to gain insight into the methods used by attackers to develop their malicious intentions. As a result of this analysis, the researchers identified five distinct refinement patterns. The authors utilize refinement patterns to propose an anti-goal refinement framework that facilitates the systematic generation of attack strategies from the perspective of an attacker. Ultimately, the individuals assess their efforts through an examination of a hypothetical situation involving the theft of a credit card.

Tong (2015) presents a comprehensive attack framework that showcases various attack strategies that can be employed by malicious actors to inflict damage on systems. The framework models an attacker's malicious intentions as structured anti-goals, which can be refined and operationalized in a manner similar to typical goals, but from the perspective of the attacker. According to their argument, the perpetrator employs distinct methods to articulate their elevated anti-goals, ultimately resulting in well-defined and precise anti-goals. Consequently, the development of anti-goals equates to the creation of their attack tactics. The authors suggest a systematic approach to examining the development of malevolent intent, wherein an anti-goal is defined as a quadruple consisting of an asset, a threat, a target, and an interval

2.6. CAPEC Repository

The Common Attack Pattern Enumeration Classification Repository (CAPEC) serves as a structured representation of the tactics, techniques, and mindset employed by network attackers. The resource in question comprises a compilation of established attack patterns utilized by malevolent actors to capitalize on identified vulnerabilities within a network configuration (capec.mitre.org, 2021). The elements provide detailed descriptions of each identified exploit, using descriptive textual fields to define and categorize each attack. The CAPEC standard is deemed essential for proficiently mitigating attacks. A security analyst who is apprehensive and aims to devise a defence mechanism or minimize vulnerability to an attack should be capable of scrutinizing an attack pattern within the CAPEC framework (CAPEC, 2021). In their study on eliciting security requirements, (Kaiya et al., 2014) suggest a technique that utilizes CAPEC, which they assert allows security experts to optimize time management. (Kanakogi et al., 2021) have proposed a methodology that employs Natural Language Processing Techniques to trace the relevant CAPEC-ID from CVE-ID by leveraging the Common Weakness Enumeration (CWE). This approach aims to address the challenge of effectively responding to security vulnerabilities.

2.7. Attack Patterns

Attack patterns are a type of software exploitation technique that is commonly described based on the concept of design patterns. According to (Zhu, 2015), the utilization of attack patterns enables the transmission and comprehension of the attacker's viewpoint, thereby facilitating network administrators to adopt an attacker's mindset.

The authors of the study (Yuan et al., 2015) present a technique for constructing abuse cases that relies on Microsoft's threat modelling and attack patterns. The Microsoft threat modelling process is employed to analyse potential threats in accordance with the methodology utilized by the user. Initial instances of abuse are generated based on the identified threats. The CAPEC attack pattern library is queried to extract attack patterns that are pertinent to the abuse cases. The data obtained from the attack patterns is utilized to expand the initial abuse cases and propose mitigation strategies during this phase of implementation. The utilization of this approach holds promise in aiding software engineers lacking advanced knowledge in computer security to create significant and valuable abuse cases, ultimately mitigating security vulnerabilities in the software systems they construct.

(Li, Paja, Mylopoulos, et al., 2015)conducted a comparative analysis of multiple attack pattern repositories and determined that CAPEC prioritizes the practical creation of security patterns through a comprehensive schema and classification taxonomy.

2.8. Network Security Risk Assessment

(Abuonji & Rodrigues, 2018) assert that adequate risk management is a fundamental and essential component of efficient security measures. This is because organizations are required to evaluate their potential risks and subsequently establish suitable security controls that can effectively counteract the risks they encounter. According to (Hewitt, 2020), the practice of risk management involves the identification and evaluation of potential risks, as well as the development of strategies to minimize their impact. The implementation of a comprehensive risk management plan can enable an organization to devise protocols aimed at pre-empting potential hazards, mitigating their consequences in the event of their occurrence, and managing the aftermath.

3. MODEL DEVELOPMENT CONSTRUCTS IN STAGES

3.1 The Extended OSI Component

We put it from literature that best security solutions can be implemented at the various layers of the OSI model and still be vulnerable through people and employees hence the eight layer “human layer” is an important consideration on the OSI Model for a holistic defence of networks. a user in a network setup should cease being something that system administrators and the top management do not know what to do with, instead becoming an important aspect that can be leveraged in the protection of networks, something that is resistant and reliable, and also demands the vision of network security professionals. Hence model adopts an enhanced OSI model with the user aspect as part of one of its constructs to assist in evaluating network security problems and solutions, see Figure 1.

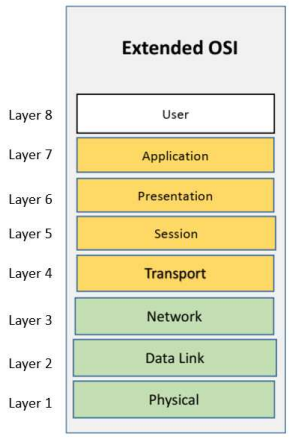

Figure 1. Extended OSI Model

3.2 Three Layer Network Security Domain (TNLSD) Component

When building and implementing network security, following a structured modular set of procedures will assist handle the many problems that play a role in security design Because of modularity, you can keep each design aspect basic and easy to grasp. Discovering possible attacks holistically is an important step in designing system security since the detected attacks will identify fundamental security needs and offer insight on what and why security measures are necessary, we modularize our extended OSI model into three layers which are the organization layer, Host Layer and Media Layer and christen them as the three-layer network security domain as shown in figure 2. The Media layer combine's the physical, data link and network layer which are in summary concerned with controlling the physical delivery of data over the network. The host layer which combines transport session presentation and application layers is concerned accurate delivery of data between computers. The organization layer is concerned with the users and how they interact with the network.

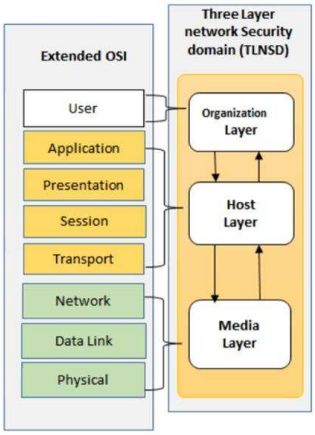

Figure 2. Three-layer network Security domain (TLNSD)

3.3 Anti Goal and Attack Surface Identification Component

As depicted in figure 3 the proposed approach involves the systematic refinement of identified root antigoals characterizes with triple construct comprising Asset, Threat, and Target, with the aim of exploring attacks across the three layers of the network security domain. The purpose of model at this instance is to examine various attack scenarios in order to gain insight into the methods used by attackers to devise strategies that enable them to carry out their nefarious objectives. Subsequent to the inquiry, we will be capable of discerning the attack aimed at the various surfaces.

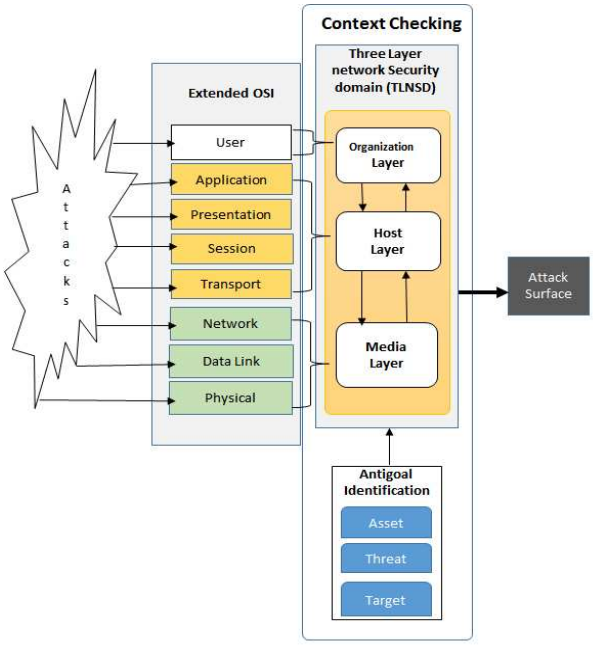

Figure 3. Anti Goal and Attack surface Identification

3.3 CAPEC Pattern Repository and Identifying Existing Attack Pattern Component

Integrating and increasing attack pattern knowledge can result in adding security by creating less exposure to identified bugs and known flaws. Attack patterns can be used to create a security checklist, which in turn can lead to a higher level of security. Since the model is about control patterns, as shown in fig 4 after identifying the attack strategy through the Antigoal process, we leverage on CAPEC repository to assist in identifying the existence of the attack pattern related to the attack strategy in order to assist in identification of mitigation strategies

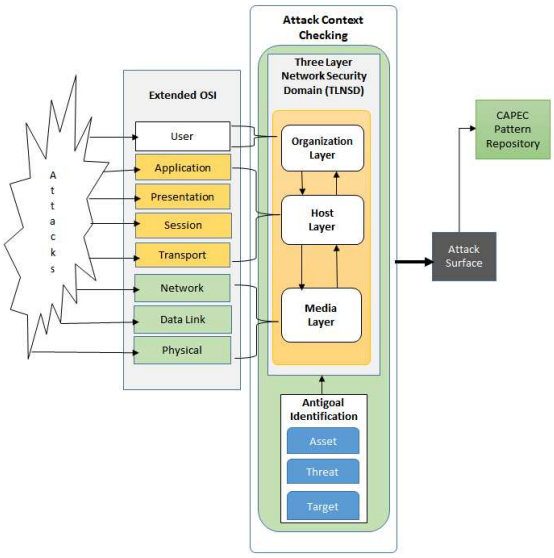

Figure 4. CAPEC Pattern Repository and Identifying existing attack pattern

3.4 Retrieving Relevant Attack Patterns Component.

Figure 5 illustrates that an attack strategy may be associated with multiple attack patterns within the CAPEC repository, resulting in a potentially cumbersome and labour-intensive analysis process. Our model suggests limiting the selection process to only those patterns that are aligned with STRIDE, a commonly utilized technique for identifying appropriate threat modelling patterns, which has been extensively researched. The identification of the Three Layer Network Security Domain (TLNSD) attack pattern would be facilitated by such action. The aforementioned model facilitates the derivation of alternative attack patterns in cases where they are not readily available within the CAPEC library. Upon deducing the patterns, it is possible to alter the CAPEC attack pattern library in order to produce novel insights. It is possible to map the same pattern using CPAEC-STRIDE.

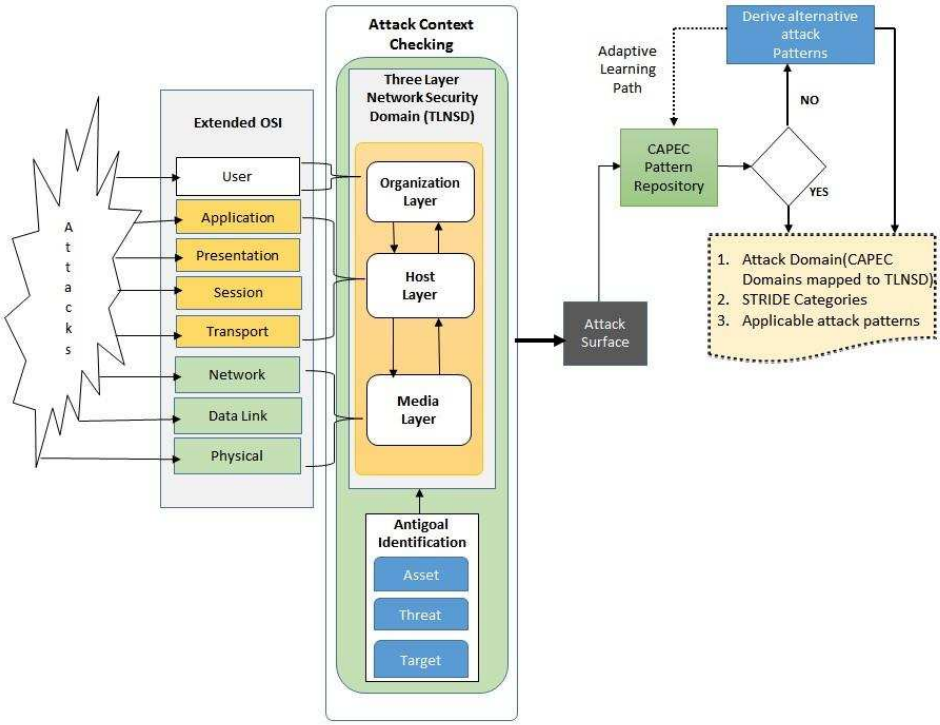

Figure 5. Retrieving Relevant Attack Pattern and Deriving Alternative Attack Pattern.

3.5 Risk Assessment Component.

Risk management identifies, estimates, and evaluates risks and delivers security requirements, which in turn lead to control mechanisms. Security risk analysis finds, evaluates, and applies important security measures; it also concentrates on preventing security flaws and vulnerabilities; and it aids in making well-informed decisions about resource allocation, tooling, and the deployment of security controls. As a result, completing an analysis is an important aspect of every company's risk management strategy. Figure 6 shows the final part of the model. Once the attack patterns are identified, they will be subjected to a risk analysis process that delivers security requirements, which in turn lead to control mechanisms. In the model, once the requirements are identified, they guide the generation of defensive control patterns that guide the network administrator to implement security measures.

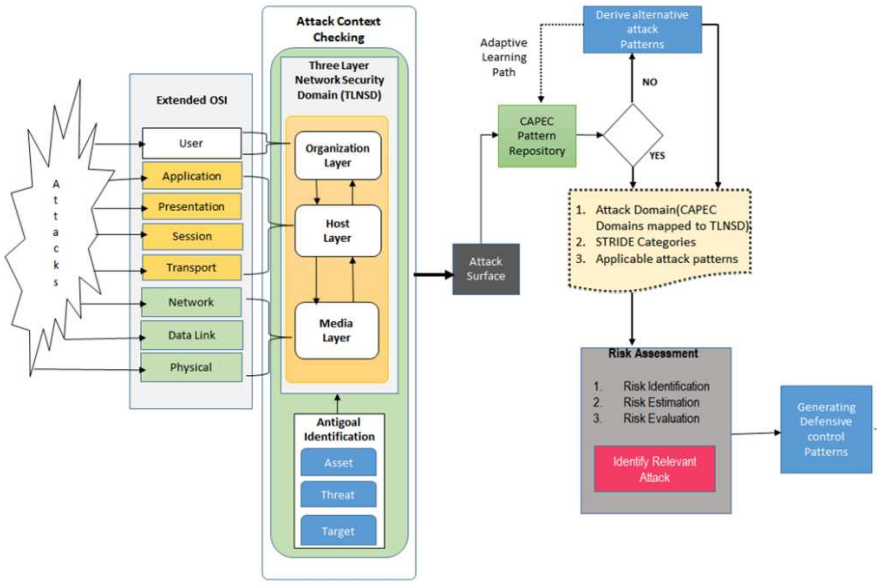

Figure 6. Risk analysis and Generation of defensive control patterns

3.6 Model Summary

From the model, figure 6. Once the network is hit by an attack, it should be categorized according to which surface it is targeting, which is either the organization, host, or media layer surfaces, which are modularized layers representing their respective layers of the OSI model. To achieve this, attack context checking is performed on the three-layer network security domain (TLNSD) by analysing the network attack traffic and identifying the targets in relation to the three layers. Once the attacks have been categorized and identified, their respective attack patterns are retrieved from the CAPEC repository. Attack strategy can be linked to several attack patterns within the CAPEC repository, which can become too many and laborious to analyse the model. Restrict, or rather, pick only those that are mapped to STRIDE since this is a technique widely used in the retrieval of suitable patterns for threat modelling based on several studies highlighted earlier. With that in mind, it would then ideally assist in identifying the applicable attack pattern per the attack domain, which is the Three Layer Network Security Domain (TLNSD). If, from the attack strategy, the model is unable to identify the applicable patterns from the CAPEC repository, it creates the option of deriving alternative attack patterns. Once the patterns are derived, they can be updated to attack the pattern library in CAPEC, generating new knowledge. The same pattern can then be subjected to the CPAEC-STRIDE mapping process. Once the relevant attack has been identified, it is subjected to the risk assessment process. Once the requirements are identified, it guides the generation of the defensive control patterns.

4 CONCLUSION AND FUTURE WORK

We have argued for the necessity of a holistic approach that incorporates security throughout the network architecture. Towards this end, we have developed an integrated holistic conceptual model that would facilitate the implementation of network security guidelines (patterns) for integrating security aspects across all network layers. The model contextualizes several security aspects and techniques (from the OSI model, the Cisco three-layer hierarchical model, the CAPEC repository, the STRIDE threat modelling framework, and the risk modelling process). As a first step towards the holistic process, we have a three-layer network security domain (aimed at specific security aspects on particular layers) that can be placed within such a model. In future work, we will show how to validate the model.

Acknowledgements

All authors would like to thank Jaramogi Oginga Odinga University of Science and Technology for the support provided to them to undertake this research project.

References

Abuonji, P., & Rodrigues, A. (2018). A Stratified Cyber Security Vigilance Model: An Augmentation of Risk-Based Information System Security. https://doi.org/10.14738/TNC.65.5166

CAPEC. (2021). CAPEC - CAPEC List Version 3.4. https://capec.mitre.org/data/index.html

capec.mitre.org. (2021). CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC). https://capec.mitre.org/

Ciampa, M. (2011). Security+ Guide to Network Security Fundamentals. Cengage Learning.

Ciampa, M. (2017). Comptia security+ guide to network security fundamentals. Cengage Learning.

Corgi. (2020). Defense in Depth and Layered Network Security \textbar Free Essay Example. In StudyCorgi.com. https://studycorgi.com/defense-in-depth-and-layered-network-security/

Crutchley, S. (2002). Information Security: Addressing the human factor. SC Infosecurity News. http://www.infosecnews.com/opinion/2002/06/19_03.htm

Dougherty, C., Sayre, K., Seacord, R., Svoboda, D., & Togashi, K. (2009). Secure Design Patterns (TECHNICAL REPORTCMU/SEI-2009-TR-010 ESC-TR-2009-010. Carnegie Mellon University.

Eric. (2016, August 23). Importance of OSI Model WALT Labs WALT Labs. WALT Labs. https://waltlabs.io/osi-model-security/

Fernandez, E. (2009). Security Patterns and A Methodology to Apply them. Advances in Information Security, 45.

Greg, M. (2019). OSI: Securing the Stack, Layer 8 – Social engineering and security policy. In SearchNetworking. https://searchnetworking.techtarget.com/tip/OSI-Securing-the-Stack-Layer-8-Social-engineering-and-security-policy

Gregg, M., Bandes, R., Franklin, B., Mays, G., Ries, C., & Watkins, S. (2006). Hack the Stack: Using Snort and Ethereal to Master the 8 Layers of an Insecure Netork. Syngress Publishing.

Hewitt, K. (2020). Importance of Network Security Risk Management l SecurityScorecard. https://securityscorecard.com/blog/importance-of-network-security-risk-management

Horkoff, J., & Yu, E. (2016). Interactive goal model analysis for early requirements engineering. Requirements Engineering, 21(1), 29–61.

Kaiya, H., Kono, S., Ogata, S., Okubo, T., Yoshioka, N., Washizaki, H., & Kaijiri, K. (2014). Security Requirements Analysis Using Knowledge in CAPEC. In W. van der Aalst, J. Mylopoulos, M. Rosemann, M. J. Shaw, C. Szyperski, L. Iliadis, M. Papazoglou, & K. Pohl (Eds.), Advanced Information Systems Engineering Workshops (Vol. 178, pp. 343–348). Springer International Publishing. https://doi.org/10.1007/978-3-319-07869-4_32

Kanakogi, K., Washizaki, H., Fukazawa, Y., Ogata, S., Okubo, T., Kato, T., Kanuka, H., Hazeyama, A., & Yoshioka, N. (2021). Tracing CAPEC Attack Patterns from CVE Vulnerability Information using Natural Language Processing Technique. https://doi.org/10.24251/HICSS.2021.841

Kumar, A. (2014). Unifying the conceptual levels of network security through the use of patterns. https://www.semanticscholar.org/paper/Unifying-the-conceptual-levels-of-network-security-Kumar/459ca9b3272a1fe731a64b842a8d994dd2911cd9

Lamsweerde, A. (2004). Elaborating security requirements by construction of intentional anti-models (Vol. 26). https://doi.org/10.1109/ICSE.2004.1317437

Li, T., Horkoff, J., Beckers, K., Paja, E., & Mylopoulos, J. (2015). A Holistic Approach to Attack Modeling and Analysis. IStar.

Li, T., Horkoff, J., Paja, E., Beckers, K., & Mylopoulos, J. (2015). Analyzing Attack Strategies Through Anti-goal Refinement. In J. Ralyté, S. España, & Ó. Pastor (Eds.), The Practice of Enterprise Modeling (pp. 75–90). Springer International Publishing. https://doi.org/10.1007/978-3-319-25897-3_6

Li, T., Paja, E., Mylopoulos, J., Horkoff, J., & Beckers, K. (2015). *Holistic Security Requirements Analysis: An Attacker's Perspective*. https://doi.org/10.1109/RE.2015.7320439

Li, T., Paja, E., Mylopoulos, J., Horkoff, J., & Beckers, K. (2016). Security attack analysis using attack patterns. 2016 IEEE Tenth International Conference on Research Challenges in Information Science (RCIS), 1–13. https://doi.org/10.1109/RCIS.2016.7549303

Maher, Z. A. (2016). A TOOL FOR MODELING SOFTWARE SECURITY REQUIREMENTS USING SECURITY PATTERNS.

Martinović, M., Lovaković, D., & Ćosić, T. (2014). Network Security Issues in Regard to OSI Reference Model Layers. 6thInternational Scientific and Expert Conference TEAM2014.

Pace, K. (2014). A Layered Security Model: OSI and Information Security. SANS Institute. https://www.giac.org/paper/gsec/3908/layered-security-model-osi-information-security/106272

Reed, D. (2003). Applying the OSI Seven Layer NetworkModel To Information Security. SANS Institute Reading Room. https://www.sans.org/reading-room/whitepapers/protocols/applying-osi-layer-network-model-information-security-1309

Richardson, S. (2022, June 3). Modularizing Security Design—Network Design. Cisco Certified Expert. https://www.ccexpert.us/network-design-2/modularizing-security-design.html

Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F., & Sommerlad, P. (2013). Security Patterns: Integrating Security and Systems Engineering. John Wiley & Sons.

Small, J. (2012). PATTERNS IN NETWORK SECURITY: AN ANALYSIS PATTERNS IN NETWORK SECURITY RECURSIVE INTER-NETWORK ARCHITECTURE NETWORKS(Doctrol Thesis. B.S., University of Massachusetts.

Solomon, S. (2016, February 4). Application Layer Security Within the OSI Model. Checkmarx. https://www.checkmarx.com/blog/application-layer-security-within-osi-model/

Szabo, R., Kind, M., Westphal, F. J., Woesner, H., Jocha, D., & Csaszar, A. (2015). Elastic network functions: Opportunities and challenges. IEEE Network, 29(3), 15–21.

Tiso, J. (2011). Designing Cisco network service architectures (ARCH): Foundation learning guide. Cisco press.

upravnik. (2016, January 26). Cisco three-layer hierarchical model. Study CCNA. https://study-ccna.com/cisco-three-layer-hierarchical-model/

Yuan, X., Nuakoh, E., Williams, I., & Yu, H. (2015). Developing Abuse Cases Based on Threat Modeling and Attack Patterns. J. Softw. https://doi.org/10.17706/jsw.10.4.491-498

Zhu, Y. (2015). Attack Pattern Ontology: A Common Language for Cyber-Security Information Sharing. TU Delft Publication, Master Thesis.