RISK ASSESSMENT IN TELEMETRY NETWORKS: ACADEMIC NETWORK ENVIRONMENT CASE STUDY

Authors: Moses Odejobi, Wondimu Zegeye, Ronald King

Advisors: Dr. Farzad Moazzami, Dr. Richard Dean, Dr. Adebisi Oladiputo

Morgan State University, Electrical and Computer Engineering Department

ABSTRACT

This paper develops and utilizes a method for analyzing, modeling and simulating cyber risks in a networked environment as part of a risk management model by incorporating an approach that will be used for the development of attacks, detection, controls from real data or assumptions. The risk assessment considers Morgan State University's network as a case study, which can be migrated to a networked telemetry system. Recent attacks on more than 300 U.S. universities targeting university professors, students, and faculty to collect credentials of the victims' university library accounts have been identified by the PhishLabs. This research work develops a model for cyber-attack risk assessment and countermeasures for the security of distributed and decentralized Servers resource in academic and other environments.

Key words: *Risk Assessment, Cyber Security, Telemetry Networks*

1. INTRODUCTION

One of the significant purposes of Risk Assessment is to have measurable and verified Information Security. We need our personal and sensitive information to have high Confidentiality, Integrity, and Availability (CIA Triad) to authorized persons only. This paper adopts an analytical model [7] and provides a worked example with a normalized MSU's IT system while under attack and shows the results (risk reduction estimates) from simulations that reflect the analytical model. To achieve this, a process model that was based on MSU's normalized design of the old (CISCO), and new (NGN-using ALE) network security infrastructure was being used.

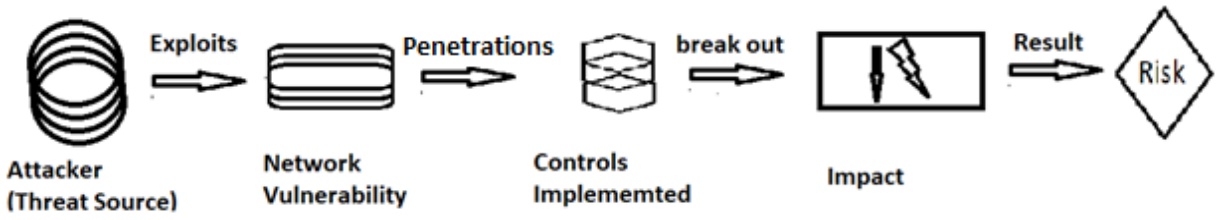

Figure 1: Risk Model for a Cyber System

The proposed methodology is based on the assumption that risk is related to the elapsed time required for a successful attack. This general risk model developed from the NIST model [1], describes how attackers, also known as the threat sources, launch various attacks whose purpose is to exploit any known vulnerabilities in a network. While some controls are in place, we found out that there are still some loopholes (residual risks) in the system which could allow the attacker to gain unauthorized access to personal information or data intended only for authorized users. This could adversely impact the network and could result in different levels of risks depending on the mission of the attacker. This same model is applied to both Morgan State University's normalized old and new (Improved-NGN) network. Comparisons were made, and the resulting impact and risks (monetarily, i.e. $$ and non-monetarily, i.e. reputation/prestige) were assessed for different attack mechanisms.

2. BACKGROUND

The methodology described below depends on the process model which came from NIST/ISACA [2-3], and the analytical model which is from MSU [7] is used to get the network's reaction to various attacks, and this was eventually used to compute the impact and risk of these attacks on the network.

Attack: A cyber-attack could be any passive or active threat actions taken to gain unauthorized access to any information that is considered confidential, by exploiting the vulnerabilities of the network. The probability that an attack is present, Pa, can be expressed as the probability of one or more attacks

$$Pa = \sum_{i=1}^{\infty} 1 - \Pi_i((1-Pa_i(k=0))) \quad (1)$$

The probability of k occurrences of attack (i) during any specified interval of time with a Poisson pdf as:

$$Pa_i(k) = \lambda_i^k e^{\lambda i}/k! \quad (2)$$

λ_i = average arrival rate of k attacks, for attack (i) with i = 0, 1, 2, 3… ∞ in some interval T.

Residual risk = Likelihood of Vulnerability * Value – "% controlled" + Uncertainty) [4], while Risk can also be simplified to equal Vulnerability * Threat.

Vulnerability:

"A Vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source" [1].

Vulnerabilities could be classified but not limited to any of the following categories: Policy flaws, Design errors, Protocol weaknesses, Software vulnerabilities, Misconfiguration, Hostile code, or Human factor [5].

The number of successful attacks determines how vulnerable a network security system is. Therefore, to account for the network's vulnerability, we first account for the probability of a successful attack over a period T and with an exponential probability of detection with parameter λ2. This can be represented as [7]

$$\mathbf{Psa = 1\text{-}Pd = 1\text{-}e^{-\lambda 2T}} \quad (3)$$

The probability of detecting an attack, **Pd**, is a critical factor in determining how vulnerable the system. The system's vulnerability is high with a low probability of attack detection, and vice versa if the probability of detection is high. We can also say that the shorter the detection time, the less vulnerable the network is, and if it takes a longer time to detect the attacks, then the vulnerability of the system can be said to be high. The likelihood of detection is mathematically represented as

$$\mathbf{Pd = \lambda_2 e^{-\lambda 2T}} \quad (4)$$

Where λ_2 represents the average time for detection, and T is the time it takes (attack or detection)

Controls: Security controls against successful attacks against the network are a crucial factor to be considered while trying to reduce the impacts of attacks on your network. If the controls in place can detect infiltrations on time, the impact and hence their risks on the network would not exist

The probability of penetration detection (Ppd) was used to model the network security control, and it could be represented with an exponential pdf as:

$$\mathbf{Ppd = \lambda_3 e^{-\lambda 3T}} \quad (5)$$

Where λ_3 is the average time it takes to control penetration and T is the period.

Impact:

Attacks cause two major categories of harm, regardless of the source: data breaches and loss of service. Data breaches could cause a situation whereby your confidential information is captured, secretly removed, and transferred to criminals. Data breaches could cause damaging impacts by tarnishing the organization's reputation, thereby causing customers to lose trust in the company, and this could eventually lead to business shutdown due to be financial losses accrued from compensating attack victims, legal charges etc. Companies who fall victim to network attacks spend a lot of time and money detection and technical remediation [6].

How does a targeted attack affect the victims?

Business upheaval, i.e. system downtime, loss of intellectual property or personally identifiable information (PII), tarnished reputation, and financial loss, are some of the negative impacts that could be felt if your network is under attack [5].

The magnitude of the loss of an attack (i) is assumed to be proportional to the total penetration time Tp which exponentially approaches your net worth ($NW) as:

$$\mathbf{Loss_i(T) = (1 - e^{-\lambda 4 Tp})\$NW} \quad (6)$$

Where λ_4 represents the time constant for dissipation of assets from the enterprise network.

Risk:

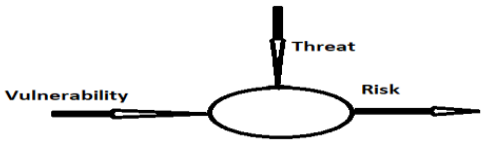

Figure 2: Risk Illustration

Risk can be computed as an accumulation of costs and their associated probabilities. In a multi-attack environment the aggregate risk can be expressed as:

$$\mathbf{Risk = \sum_i Psp(i)\ Loss_i\ (T)} \quad (7)$$

Risk can be express from equations 1 to 7 above as[7]:

$$\mathbf{Risk = \sum_i \left(\sum_i \left(\lambda_i^k e^{\lambda i}/k!\right)\right)\ (1 - e^{-\lambda 2T})(1 - e^{-\lambda 3T})(1 - e^{-\lambda 4Tp})\$NW} \quad (8)$$

3. RISK ASSESSMENT

Figure 3 describes normalized MSU's old network security architecture; this contains two redundant firewall service modules (FWSM), and operating in a failover configuration modes which were located at the outer edge of the network to help safeguard information technology (IT) resources from security risks. The network also includes two operational but redundant core

switches/routers, which are capable of segregating the un-trusted wireless and students computer lab network segments from the administrative users. Server farm (servers that houses banner application for Students, Human Resource, and Financial Information Systems) was positioned behind one of the Cisco Firewall Service Module (FWSM), operating on a Cisco 6509 switch/router positioned within the MSU network.

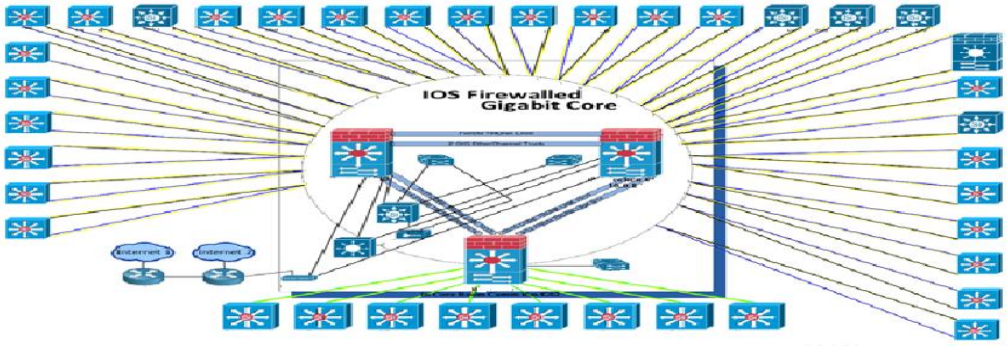

Figure 3: Old Network Diagram

Each switch block that surrounds the core represents each building of the school. Some of the attacks experienced include but not limited to phishing, SQL injection, and WordPress Attacks. Assaults on most educational institutions includes, but is not limited to: Eavesdropping, Data Modification, Identity Spoofing (IP Address Spoofing), Password-Based Attacks, Man-in-the-Middle Attack, Compromised-Key Attack, Sniffer Attack, Application-Layer Attack etc. while some of these attacks were detected and removed, others had negative impact on the school's network, but not to the extent of costing the university loss of reputation.

3.1 MONTE-CARLO SIMULATION OF THE RISK MODEL

The Monte-Carlo model simulation of the cyber security model in Section 2 was simulated for different scenarios considering a single attack type and $\boldsymbol{\lambda_i}$ fixed for attack arrival and cost, λ_2 and λ_3 are varied for the 4 different scenarios. These scenarios are as follows:

- Small emphasis (10%) on both detection (λ_2) and control(λ_3)
- High emphasis (50%) on detection only.
- High emphasis (50%) on control only.
- Balanced emphasis (35%) each on detection and control.

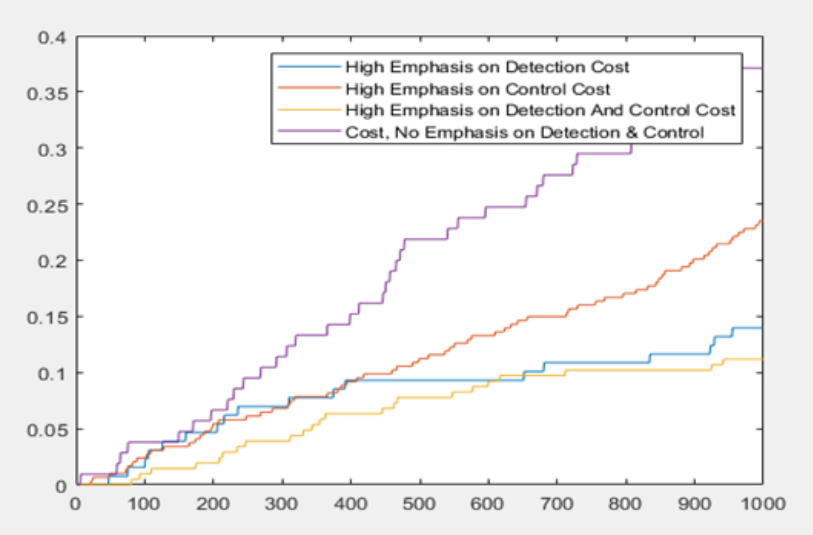

Figure 4: Comparing cost for all four cases

The results of the risk (cost) of the four scenarios are plotted in Figure 4. It depicts the balanced approach to detection and control is the lowest risk and most effective strategy. This confirms what many security experts predict in the risk management of systems. The next sections of this paper apply this theoretical simulation in a practical approach.

3.2 NEW NETWORK SECURITY INFRASTRUCTURE

The network diagram (normalized) in Figure 5 shows what the new network (NGN) security infrastructure; the security method used can combat most Attacks. Some of the attacks experienced include but not limited to all that was stated in the old network and more. NEW Components of the New Network Security Architecture

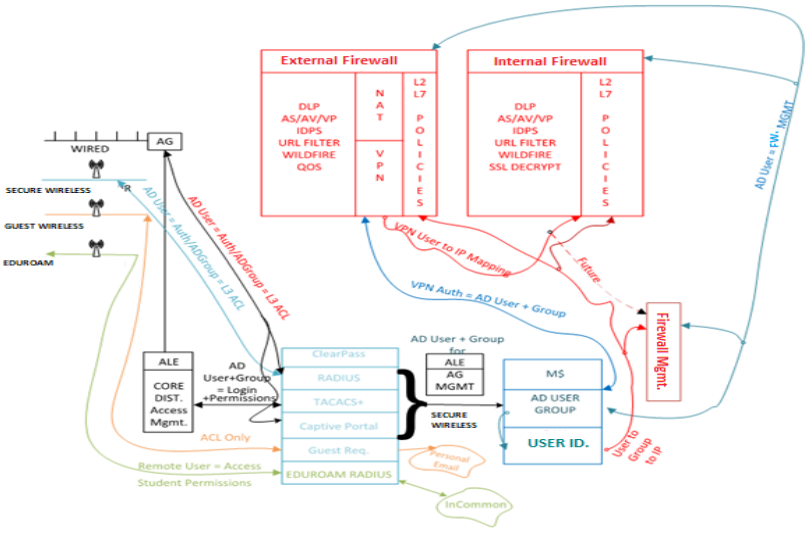

Figure 5: New Network Security Architecture

3.2.1 Wired Users

Wired users are connected to the network via cables (RJ-45 CAT6), as soon as a user logs into his/her PC by typing his/her username, the user will immediately be directed to its portal based on the user group classification he/she belongs, the user's classification also determines the level of privileges the user will have on the network. Access guardian is what makes this possible.(a)

(a) Access Guardian

Access Guardian requires a combination of 802.1x configuration, AAA authentication, and QoS ACL to identify the user network profile (UNP) to configure the individual users into an assigned group to provide a dynamic, proactive network security solution.

Authentication and Classification—Access control is configured on 802.1X-enabled ports using device classification policies. A policy can specify the use of one or more types of authentication methods (802.1X, MAC-based, or Web-based Captive Portal) for the same port. For each type of authentication, the policy also specifies the classification method (RADIUS, Group Mobility, default VLAN, or block device access)

User Network Profiles (UNP)—one of the configurable options of a device classification policy is to classify a device with a UNP. When the policy applies the UNP to one or more devices, the UNP determines the VLAN assignment for the device, and if any QoS access control list (ACL) policies are applied to the device, which will be based on MSU's existing and future Active Directory structure.

(b) Policy Configuration for Access Guardian

Policy network group provides the access list, which identifies the permissible IP address or IP network; furthermore, the policies correlate to policy condition that is tied to the policy rule and policy list. The configuration is standard across all access switches accordingly.

3.2.2 Wireless Users

Wireless Users (secure wireless, guest wireless, eduroam), unlike wired users, they are connected wirelessly and without wires. Wireless devices initially locate the nearest access points, and the access points routes the data's through the switch and to the wireless controllers where policies are being setup (looks just like access lists). For the wireless devices, the wireless controllers check the policies in place for each user based on the group they belong by checking and authenticating via ClearPass policy manager.

The ClearPass Network Access Controllers provides Radius Authentication Services for wired, wireless, and Palo Alto VPN clients. It also provides wireless guest access. It operates by matching the user to their AD group membership, and returns the necessary role to Access Guardian and the Wireless Access Controllers, for assigning the proper network access to the user.

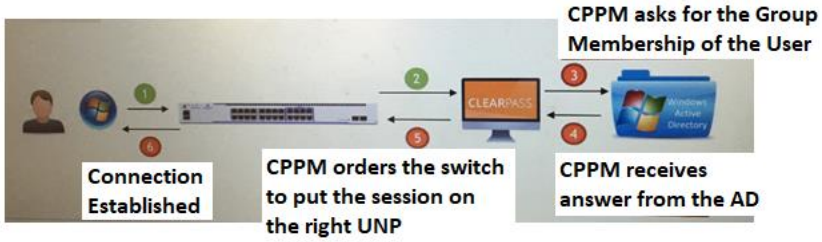

Figure 6: Communication between Clearpass and Active Directory

The Active Directory structure has direct ties to the security architecture of ClearPass as well as Access Guardian and Firewalls. Given proper consideration, Active Directory can provide granular security permission through Access Guardian and ClearPass for wired and wireless users. Others include but not limited to lldp security, learned port security and more.

3.3 Vulnerabilities in the Old Network and Solutions from New Network Security

The Security vulnerabilities identified in the old network are balanced by placing security controls in the new network. Table 1 shows these network vulnerability and their countermeasures in the new network.

Vulnerabilities of old Network Security	**Solutions from the New Network Security**
IDPS systems - Device Hardening 1. Significant portions of MSU's network traffic were not subject to IDPS coverage 2. IDPS signatures were not updated on the ISDM for about 20 months 3. The ISDM modules were not being backed up.	MSU implement IDPS coverage for all critical portions of its network MSU also continually maintain active licenses for its ISDM modules and update the signatures on the modules as the vendor releases them. Periodically, MSU backup the ISDM modules' configuration files and store them offsite in a secure environmentally controlled location.

Control over administrative access to its two IDSM modules is not good enough 1.The User Account on the IPSs modules configurations each contained one locally defined user account for accessing the device which was not renamed or deleted 2.User Authentication - several user authentication control settings were not enabled.	Limited administrative access to IPS1 to only IP addresses of network administrators and network management servers that require access. Default user account was deleted. Authentication control settings for user accounts and passwords comply with DoIT requirements.
OLD Network Security Architecture (Host-based IDPS) IDPS coverage for encrypted traffic entering the MSU network from un-trusted sources did not exist.	Complete IDPS coverage was introduced which includes the use of network-based IDPS.
Old Network Security – Firewall (Outdated and Unsupported Software) Data center Firewall Service Module software was susceptible to known vulnerabilities, and the manufacturer no longer supported the FWSM software	Enables constant firewalls updates.
Old Network Antivirus/ Anti-malware 1. Inadequate procedures or policy to install, monitor MSU workstations and server 2. Lack centralized management of monitoring Antivirus and Antimalware	Provision of adequate policy for the installation and monitoring antivirus and antimalware. MSU acquire and utilize a centralized management console to monitor.
Old network's Administrator Privileges: *User Access Control (UAC*) was not enforced	*User Access Control (UAC*) was enforced

Table 1: Vulnerabilities in the Old Network and Solutions from the New Network

4. CONCLUSIONS AND FUTURE WORK

To implement a very good security system in a networked environment, you have to do a thorough risk assessment, and make sure to put into account every known attack while also making considerations for attacks that may occur in the future. The simulation which contains an analytical model from prior work shows that if you place a balanced emphasis on attack detection and control, you have far lesser risk than when you only place much emphasis on either attack detection or controls. A worked example of the previous model is used to compare Morgan State University old and new IT network to migrate to an

improved security system by placing balanced emphasis on attacks prevention/detection, and control to reduce the total risk of the old system to the bearable minimum.

5. ACKNOWLEDGEMENTS

The authors would like to express appreciation to Mr. Gilbert Morgan, Alexandre Adao, and James Clark for their support for this effort and heartfelt gratitude to our advisors, Dr. Dean, Dr. Moazzami and Dr. Adebisi Oladipupo and our colleagues, Samuel Akinola and Tobiloba Komolafe for providing such fruitful discussions, comments and support. Finally the authors also would like to express their appreciation to Mr. Ronald King (CISO) of MSU DIT for constantly reviewing the paper to make sure confidential information is not included in the paper and his constant suggestions.

6. REFERENCES

[1] Guide for Conducting Risk Assessments, NIST Special Publication 800-30 Revision 1.

[2] Process Models ICASA, "The Risk IT Framework", Rolling Meadow, IL, May 2009

[3] Managing Information Security Risk -Organization, Mission, and Information System View, NIST Special Publication 800-39, March 2011.

[4] Michael E. Whitman, Herbert J. Mattord, "Management of Information Security", Cengage Learning, 2014. Print.

[5] Understanding Targeted Attacks: The Impact of Targeted Attacks. (2015, October 8), Retrieved from, https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/the-impact-of-targeted-attacks, March 14, 2018

[6] Sweeney, P. (2013, August 13). Network-based attacks: How much can they cost you?, Retrieved from https://www.scmagazine.com/network-based-attacks-how-much-can-they-cost-you/article/541922/ , April 23, 2018.

[7] Shourabi B. , "A Model For Cyber Attack Risks In Telemetry Networks" , *in proceedings of the 51st International Telemetry Conference (ITC 2015)*, Oct. 2015, Las Vegas, NV.

[8] W.H.Baker et al, 2009 Data Breach Investigation, Verizon Report, 2009.

[9] W.H.Baker et al, 2008 Data Breach Investigation, Verizon Report, 2008.

[10] W.H.Baker et al, 2010 Data Breach Investigation, Verizon Report, 2010.

[11] W.H.Baker et al, 2011 Data Breach Investigation, Verizon Report, 2011.

[12] Data Breach Investigation, Verizon Report, 2016.