Innovations in Computing Technology and Applications
Volume 2 | Year: 2017 | ISBN: 978-967-0194-95-0

Cyber Attack Profiling Towards Critical Inftastructures Using Modified System Fault Risk Framework

Amirul Aslam Ahmed[1], Anazida Zainal[2]

[1,2]Faculty of Computing, Universiti Teknologi Malaysia (UTM),
81310 Johor Bharu, Johor, Malaysia

amirulaslam@live.com[1], anazida@utm.my[2]

Abstract. Critical infrastructure is defined as those real and virtual assets, systems and functions that are highly important to the nation. In which any of destruction of those assets would give a huge impact to the economy, image and government function of a nation. As most of the critical infrastructure use internet as a medium to communicate, dealing with clients, store data and even manage their resources, it is important for us to protect the critical infrastructure from any kind of cyber-attack. As to take a preventive and proactive approach on handling cyber-attack, this research studied the essential step on protecting the critical infrastructure from cyber-attack which is cyber-attack profiling. The system fault risk framework which have been introduced by [1] will be modify accordingly to make sure that the profile of the attacks is good and suit the needs of critical infrastructure.

Keywords: Cyber-attack; Profiling; Critical infrastructure.

1 Introduction

Internet has become one of the most important things in our life. From ordering food to meet and discuss with potential clients, all we can do via internet. Internet has change the landscape of how the information been spread, the data been stored and also change the method for government to provide services for the peoples.

While internet has become very important to us, it also attract criminals to exploit the weaknesses of it for their own gain. As reported in 2015 Data Breach Investigation Report lead by Verizon, the estimated financial loss from 700 million compromised records is USD 400 million [2]. There are 79790 cyber security incidents reported, 2122 confirmed data breaches from 61 countries in 12 industries in which seven from them are industries categorized as critical infrastructure in Malaysia [2].

There is an absence of suitable cyber-attack profiling for critical infrastructure. The current framework which have been used such as System Fault Risk framework are not being updated for several years and thus it cannot suit the needs of profiling a cyber-attack on critical infrastructures. The impact of the absence of cyber-attacks profiling for critical infrastructure might exposed a nation to multiple kind of cyber threats or attacks from various criminals which later may lead to a serious problem.

Cyber-attacks on critical infrastructure will give a bad impact to the country. In this study, rough set technique will be used to determine another attribute to be used in SFR framework. Several frameworks and modelling concepts which have been used to classify attacks, vulnerabilities and exposure will be assessed. After the modification of SFR framework have been made, a profiling of cyber-attacks in several critical infrastructures using that modified framework will be done. The research will provide a graphical view of

the cyber-attacks profiles so that people who see it can easily interpret the research results. Thus, authority can make a precautionary step before the attacks happen and avoiding harmful disruptions to the critical infrastructure itself [3].

2 Literature Review

Several modelling techniques on characterizing cyber-attack which have been established from previous research will be discussed in this section.

2.1 System Fault Risk Framework

The development of SFR framework is based on the concepts of system modelling, fault modelling and risk assessment theories [1]. System modelling concept are often used for attack detection which include resource-process interactions and activity-state-performance interaction in which we can use to model the computer and network systems [1]

In fault modelling concept, the essential part is to capture the cause-effect chain of changes in a system [1]. A fault in a system will affect activity-state-performance interactions. The last component in building SFR framework is risk assessment theories. There are three factors that we consider in order to assess the system risk of a fault (such as, one caused by a cyber-attack) which are asset, vulnerability and threat [1]

2.2 System Fault Risk Framework

Attack graphs are conceptual diagrams which visualize the analysis of how organization can be attacked. It is a preventive mechanism to prevent the network from being intruded by the attackers. The attack graph is one of the traditional method in finding vulnerability of network of an organization which have been suggested by many researchers [4]. Attack graphs used by the network administrators to find the vulnerability of their system, the possibility of how an attack can happen and a set of preventive actions to obstruct the attacker from compromising their network.

2.3 Diamond Model

Four main components in Diamond Model are adversary, capability, infrastructure and the victim. Adversary is the attacker who attacks a victim after finding out their capability compared to the security level of the victim's infrastructure. This kind of model is useful and important when the organization are dealing with more advanced attacker [4]. This model have been chose to be included in this study because of the simplicity of the implementation of the models.

2.4 Kill Chain Model

In the Kill Chain model, it is used to describe an attack based on the steps taken. The kill chain model has seven steps of attack which are reconnaissance, weaponization, delivery, exploitation, installation, command and control and action on objectives [4]. The Kill Chain model has been used by many organization and authorities for many years including US Department of Defense.

2.5 National Vulnerability Database

National Vulnerability Database (NVD) is a superset of CVE. NVD is extended of CVE by providing additional analysis, a database and a fine-grained search engine (National Institute of Standards and Technology, 2017). The NVD is particularly and perfectly synchronized

with CVE in which any updates happen to CVE databases, it will immediately appear on the NVD.

3 Research Methodology

In order to guide the progress of this research, a framework has been created to achieve the objective as stated in Chapter 1. The framework for this research will consist of three phases.

3.1 Obtaining Attributes from Literature Review and CVE Details

Initially, the study focused on obtaining suitable attributes which have been used by other cyber-attack modelling technique and cyber-attack profiling framework including SFR framework. There are three steps involved in this process which are, 1) Find sources from internet, books, journals, conference paper, and thesis; 2) Study the previous researches done by many researches; 3) For all the techniques and frameworks, list down all the attributes which is suitable to considered to be implemented.

For the attributes obtained from CVE Details by implementing rough set theories, there are several steps should be taken in this process which are, 1) Extracting data of Common Vulnerabilities and Exposures and National Vulnerability Database from CVE Details; 2) Change the data structure and file type from comma-separated value to information system file; 3) Change the format of the data from characters to numerical dataset.; 4) Filtering out the non-related attributes; 5) Reduction process; 6) Obtain rules from the datasets.

3.2 Designing Framework

After obtaining attributes from research and machine learning process done in the previous phase, the data will be placed accordingly by adopting the design of SFR framework.

In SFR framework, there are four parts in profiling an attack which are threat, attack, cause (activity) and effects. All the new attributes will be classified as these four classifications before it been implemented in the framework.

3.3 Visualization

The last output is to display the cyber-attack profiles for critical infrastructure graphically by using network graph in R. This phase needed to be done as when the result is shown graphically, it will attract more people and they can understand better as well as helping the authorities in making a decision [5].

4 Attrıbutes Selectıon For Cyber Attack Profılıng

In this section, the complete process of obtaining suitable attributes to be implemented in the modified System Fault Risk (SFR) framework for critical infrastructure will be discussed. These suitable attributes were extracted from the literature and from National Vulnerability Database. For the purpose of this research three modelling concepts which are Attack Graph, Kill Chain Model and Diamond Model will be covered. These concepts have been chose based on the simplicity shown, the implementation of the modelling concept by the higher authority and how old the modelling technique have been established [4].

In attack graph each type of attacks is dependent to three things which are attack rule, vulnerability and reachability. As for the needs of this study, the reachability attributes have been dismissed as this research are not focusing on connecting the nodes in the network. Thus there are four attributes obtained from this model which are: 1) Attack type; 2)

Prerequisite; 3) Consequence; 4) Vulnerability. The kill chain model use the same concept as attack graph which defines attack as a chain of action. This model has been adopting by US Department of Defence, and they have defined this model with some stages such as find, fix, target, engage and assess. There are seven steps of attacks as describe by this model which are: 1) Reconnaissance; 2) Weaponization; 3) Delivery; 4) Exploitation; 5) Installation; 6) Command and control; 7) Action on objectives. For this study, The command and control attribute has been dismissed as this study are not focusing on evaluating and describing the command and control activity performed by the attackers.

There are four main components in describing diamond model which are adversary, capability, infrastructure and the victim [4] as shown in Figure 1. Each of the main components in this model are linked using edges to show the fundamental relationships between the features. The core features of an intrusion event as described in this model are: 1) Adversary; 2) Capability; 3) Infrastructure; 4) Victim. All the attributes listed as core features in this model are being considered to be implemented in the modified SFR framework.

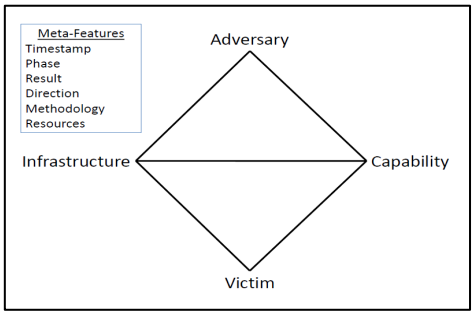

Figure 3: Diamond Model of Intrusion Analysis

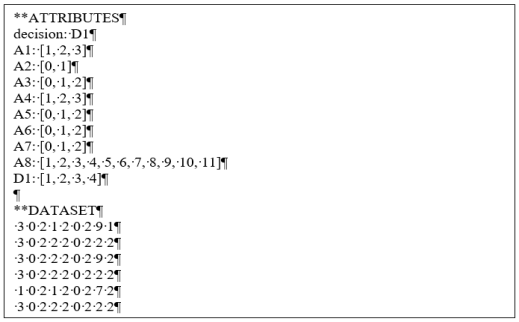

Figure 2: Example of Dataset in Information System File Format

For the purpose of this study, 2739 rows of data with 16 attributes has been collected from CVE Details website which provide datasets from CVE and NVD. After the process of collecting data has been done, the data needs to be formatted into a new format before the suitable attributes can be extracted from it. There are two things have been done to format the data. First, the name of information in the vulnerability type attribute has been change to its real name as certain data in the dataset are using special character, which are not suitable to be used in the next process. The example of the result is shown in Table 1.

Table 1. Data Conversion for Vulnerability Type Attribute Attribute

Before	After
+Priv	Gain.Privileges
+Info	Gain.Info
Exec Code Bypass	Code.Execution Bypass
+Priv	Gain.Privileges
+Priv	Gain.Privileges
XSS	XSS
Exec Code Overflow	Code.Execution Overflow
+Priv	Gain.Privileges
DoS Exec Code Overflow Mem. Corr.	DoS Code.Execution Overflow Memory.Corruption

Table 2. Number of Occurrence for Each

Attribute	Number of Occurrences
Access	38
Authentication	21
Confidentiality	21
Complexity	44
Integrity	33
Gain Access	2
Availability	30
Vulnerability Types	61

The null value in the dataset then being specified as NA as it has been leave blank before. From 16 attributes, 7 of them have been drop as they does not give any significant effect on impact metrics [6]. The drop attributes are: 1) ID; 2) CVE ID; 3) CWE ID; 4) Number of exploits; 5) Publish date; 6) Update date; 7) Description. All the attributes that being removed would not give significant insight on the visualizing the behavior of an attack. The remaining attributes then being converted from enumerated type and floating point to the integer type. As the data collected is in the form of comma- separated value, the dataset need to be converted into information system file. The example of dataset is shown in Figure 2.

Then the process to determine and removing insignificant attributes by using reducts has been done. The result is no insignificant attributes, which means all attributes are important in classifying the severity of a vulnerability to an organization and infrastructure. Then, the process of finding suitable attributes has been continued with the rule induction process. LERS algorithm has been chosen as the dataset used in this study is not consistent because of the conflicting objects in the dataset. There are 76 rules have been generated from this dataset. Occurrence of each attribute in each rule have been counted, and the result is shown in Table 2. Based on the result, seven from eight attributes listed will be included in the modified framework which are Access, Authentication, Confidentiality, Complexity, Integrity, Gain Access, Availability and Vulnerability Types.

5 Modıfıed System Fault Rısk Framework

The design of the new framework is still based on the current framework which have four parts in classifying the attributes which are threat, attack, cause (activity) and effect. Each attribute should include two categories whether it is threat or attack and whether it is cause or effect. Before the attributes being classified, the attributes will be listed and the redundant attributes will be removed, and only the remaining attributes will be implemented in the new framework.

After removing all the redundant attributes, the final attributes that will be adopted in the modified SFR framework are: 1) Objective; 2) Propagation; 3) Attack Origin; 4) Action; 5) Vulnerability; 6) Asset; 7) Performance Effects; 8) Confidentiality; 9) Integrity; 10) Availability; 11) Authentication; 12) Complexity; 13) Adversary; 14) Sector. As this study is focusing on building a suitable framework for cyber-attack profiling towards critical infrastructure, one attribute that describe the sector in which the attack happen has been added. The framework then re-design by adding all the attributes that have been listed and classified accordingly into their respective classes. The example of the modified framework which profile the attack during cyber-attack on Estonia in 2007 is shown in Figure 3.

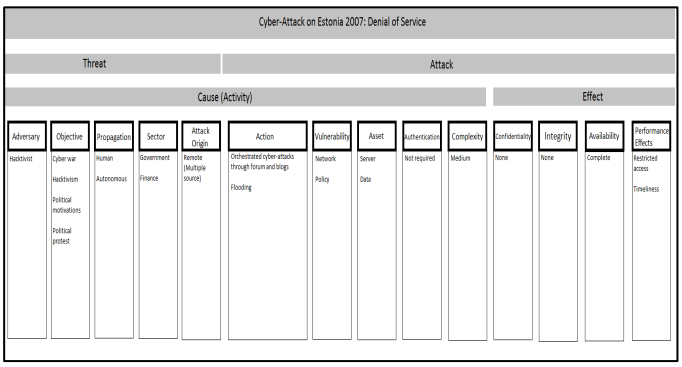

Figure 3: Cyber Attack on Estonia in 2007

Several cyber-attacks data on critical infrastructure then being collected to produce network graph. The network graph produce could give an insight on the typical behavior of an attack. The network graph which show the behavior of attack and sector in critical infrastructure is shown in Figure 4. Based on the network graph in Figure 4, malware, distributed denial of service and defacement are among the top attacks used by the attacker. Malware has a strong relationship with information and communication sector and national defence and security, while for distributed denial of service it is always being used to banking and government sectors.

6 Conclusion

This research studied about the cyber-attack profiling towards critical infrastructures using modified System Fault Risk framework which is vital to take a preventive approach to protect the critical infrastructures. All the objectives in this study has been achieved. First, the additional attributes used to modify SFR framework has been determined. Based on the attributes collected, a new framework has been established by adopting the design of SFR framework. Several attacks then being profiled and the visualization of the profiles will give us an insight on the behaviour of an attack.

References

1. Ye, N., Newman, C. and Farley, T., A system-fault-risk framework for cyber attack classification. Information Knowledge Systems Management, 5(2), 2005, pp.135-151.
2. Team, V.R., 2015. 2015 Data Breach Investigations Report.
3. Cornish, P., Livingstone, D., Clemente, D. and Yorke, C., Cyber security and the uk's critical national infrastructure, 2011.
4. Al-Mohannadi H, Mirza Q, Namanya A, Awan I, Cullen A, Disso J. Cyber-Attack Modeling Analysis Techniques: An Overview. InFuture Internet of Things and Cloud Workshops (FiCloudW), IEEE International Conference on 2016 Aug 22 (pp. 69-76).
5. Crossman, A.R. and Neary, D., Neuroanatomy: an illustrated colour text. Elsevier Health Sciences, 2014.
6. National Institute of Standards and Technology. "The Common Vulnerability Scoring System." NVD - CVSS. N.p., n.d. Web. 16 Mar. 2017.