IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cyber Threat Map: Detection and Analysis of Threats

Pranav V Kini *1, Mrs. Jismy Joseph *2

*1Department of MCA,SCMS School Of Technology And Management, Ernakulam, Kerala, India

*2Associate Professor, Department of MCA,SCMS School Of Technology And Management, Ernakulam, Kerala, India.

Abstract

When a network safety occasion happens, an individual needs to address the accompanying inquiries: what occasions are going on, where are the occasions happening, and how much harm has happened or will happen. This paper strongly prescribed to a network protection observing framework that gives connection of time-series occasion information, a visual portrayal of the security occasions, and gives a prescient figure of potential occasions dependent on known natural states. The reasoning for this comes from the need to have a general perspective on security occasions or tempests that are happening on an organization while giving data regarding seriousness and a spread example. In this manner, it can conceivably give an early admonition so occasions or tempests can be proactively moderated. In addition, it can help in making typical business decisions by determining or understanding the relationship between the computing devices and the business/information technology services they make up.

Keywords: Cyber security, Networking, Intel, Zero day attack, Vulnerabilities, SVM, RPL, Ransomware, Intrusion, Detection, Raspberry Pi, SRPL, Crypto.

I. INTRODUCTION

In recent years, cyber attacks such as Internet worms or DDoS (Distributed Denial of Service) attacks are serious concerns in our society. To monitor and analyze these attacks, a variety of cyber threat monitoring systems are in use (DShield , SANS Internet Storm Center). These systems utilize traditional visualization methods, such as geographical visualization and temporal visualization, to show the result of its analysis. These visualizations are independent and it is difficult to know the relation between them. For example, the temporal visualization shows us transition of the number of attacks. On the other hand, the geographical visualization shows us the number of attacks of different locations at a particular moment. Even if we click on the geographical visualization, it does not reflect to the temporal visualization. In practical cyber threat monitoring, it is important to analyze all the information from different viewpoints and to make a right decision. It would be helpful for the administrators that these different views are integrated and synchronized

Efficient visualization of Cyber incidents is the key on securing increasingly complex Intel infrastructure. Extrapolating security related data from multiple sources can be daunting task for organization to maintain safe and secure operating environment. However , meaningful visualizations can significantly improve decision making quality and help security administrators in taking rapid response. This application allows users to monitor Cyber threat in real time. It supports to kind of virtualization regional and notional. Each one of them has got it's own advantage and disadvantage.

II. LITERATURE REVIEW

The rapid growth of the Internet of Things (IoT) and the massive propagation of wireless technologies has revealed recent opportunities for development in various domains of real life, such as smart cities and E-Health applications. A slight defense against different forms of attack is offered for the current secure and lightweight Routing Protocol for Low Power and Lossy Networks (RPL) of IoT resource-constrained devices. Data packets are highly likely to be exposed in transmission during data packet routing. The RPL rank and version number attacks, which are two forms of RPL attacks, can have critical consequences for RPL networks. The studies conducted on these attacks have several security defects and performance shortcomings. In this research, we propose a Secure RPL Routing Protocol (SRPL-RP) for rank and version number attacks. This mainly detects, mitigates, and isolates attacks in RPL networks. The detection is based on a comparison of the rank strategy. The mitigation uses threshold and attack status tables, and the isolation adds them to a blacklist table and alerts nodes to skip them. SRPL-RP supports diverse types of network topologies and is comprehensively analyzed with multiple studies, such as Standard RPL with Attacks, Sink-Based Intrusion Detection Systems (SBIDS), and RPL+Shield. The analysis results showed that the SRPL-RP achieved significant improvements with a Packet Delivery Ratio (PDR) of 98.48%, a control message value of 991 packets/s, and an average energy consumption of 1231.75 joules. SRPL-RP provided a better accuracy rate of 98.30% under the attacks.[1]

Real-time Ethernet has been applied to train control and management system (TCMS) of 250km/h Fuxing Electric Multiple Units (EMUs) and some urban rail vehicles. The openness of the Ethernet communication protocol poses a risk of intrusion attacks on the train communication network. It is, therefore, necessary that a safety protection technology is introduced to the train communication network based on real-time Ethernet. In this paper, a train communication network intrusion detection system based on anomaly detection and attack classification is proposed. Firstly, the paper built an anomaly detection model based on support vector machines (SVM). The particle swarm optimization-support vector machines (PSO-SVM), and genetic algorithm-support vector machines (GA-SVM) optimization algorithms are used to optimize the kernel function parameters of SVM. Secondly, the paper built two attack classification models based on random forest. They are iterative dichotomiser3 (ID3) and classification and regression tree (CART). And then, the built intrusion detection and attack classification model is tested by using the public data set knowledge discovery and data mining-99(KDD-99) and the data set of the simulation train real-time Ethernet test bench. PSO-SVM improves the intrusion detection accuracy from 90.3% to 95.75%, GA-SVM improves the detection accuracy from 90.3% to 95.85%. The training time of the PSO-SVM algorithm was higher than that of the GA-SVM algorithm, and much higher than that of the SVM, without optimization. Both ID3 and CART models are verified valid in the attack classification, while the ID3 algorithm obtained 100% accuracy on the training set, and only 32.89% accuracy on the test set, ID3 has a poor classification accuracy of the data outside of the training set. Also, the classification time is very long for ID3 compared with CART. So the comprehensive experimental results show that the intrusion detection system of train real-time Ethernet can use the GA-SVM model for detection of abnormal data. After passing the normal data, the CART model can be used to distinguish between the types of attacks to better complete subsequent responses and operations. Compared with the anomaly detection model based on SVM, the proposed model improves intrusion detection accuracy. And the proposed attack classification algorithm based on CART can improve the computing speed while ensuring the precision of classification.[2]

Crypto ransomware is a type of malware that locks its victim's file for ransom using an encryption algorithm. Its popularity has risen at an alarming rate among the cyber security community due to several successful worldwide attacks. The encryption employed had caused irreversible damage to the victim's digital files, even when the victim chooses to pay the ransom. Therefore, this research proposes the Pre-Encryption Detection Algorithm (PEDA) that can detect crypto-ransomware at the pre-encryption stage, when no encryption has been done. PEDA provides two levels of detection; the first level of detection was before the ransomware can be activated using a signature comparison with a known crypto-ransomware's signature. The signature was generated using SHA-256 (Secure Hashing Algorithm) that allowed fast and accurate comparison of the file content. The second level of detection used Learning Algorithm (LA) that can detect crypto-ransomware based on pre-encryption application program interface (API). The LA produced a 100% recall rate based on 80:20 ratios of training and testing, and 99.9% recall rate with a 10-fold cross-verification test. In addition, this research had also successfully identified fourteen important APIs that can differentiate between ransomware and goodware. Three APIs were present in most ransomware, but less in goodware; these APIs were NtProtectVirtualMemory, NtResumeThread, and NtTerminateProcess. Eleven APIs, on the other hand, were mostly present in goodware, but less in ransomware; these APIs were NtWriteVirtualMemory, UuidCreate, NtDelayExecution, NtSetInformationFile, NtWriteFile, CreateThread, NtReadVirtualMemory, VirtualFreeEx, CreateDirectoryW, VirtualProtectEx, and SetFilePointer.[3]

Information protection is becoming a focal point for designing, creating and implementing software applications within highly integrated technology environments. The use of a safe coding technique in the software development process is required by many industrial IT security standards and policies. Despite current cyber protection measures and best practices, vulnerabilities still remain strong and become a huge threat to every developed software. It is crucial to understand the position of secure software development for security management, which is affected by causes such as human security-related factors. Although developers are often held accountable for security vulnerabilities, in reality, many problems often grow from a lack of organizational support during development tasks to handle security. While abstract safe coding guidelines are generally recognized, there are limited low-level secure coding guidelines for various programming languages. A good technique is required to standardize these guidelines for software developers. The goal of this paper is to address this gap by providing software designers and developers with direction by identifying a set of secure software development guidelines. Additionally, an overview of criteria for selection of safe coding guidelines is performed along with investigation of appropriate awareness methods for secure coding.[4]

Information security is the most critical component of the information system. It is also a challenge of the organizations to build a secure network. Every organization that developed its organizational network has faced security attacks, security risks, and vulnerabilities. Internet of things (IoT) is based on smart devices that connect with each other to formulate a complex network. Therefore, in order to build a secure traditional network and IoT network, understanding the basics of the network layers, network security, and different types of network attacks is essential for network security beginners who are interested in working in the field of information security. In this chapter, the authors reviewed the essential and most important concepts of information security, IoT, and explained these topics in an easy-to-understand way. Furthermore, the chapter discussed the basic level of information security challenges to familiarize the undergraduates and postgraduate students and IoT information security practitioners about it.[5]

In this paper, we provide a systematic review of the growing body of literature exploring the issues related to pervasive effects of cybersecurity risk on the financial system. As the cybersecurity risk has appeared as a significant threat to the financial sector, researchers and analysts are trying to understand this problem from different perspectives. There are plenty of documents providing conceptual discussions, technical analysis, and survey results, but empirical studies based on real data are yet limited. Besides, the international and national regulatory bodies suggest guidelines to help banks and financial institutions managing cyber risk exposure. In this paper, we synthesize relevant articles and policy documents on cybersecurity risk, focusing on the dimensions detrimental to the banking system's vulnerability. Finally, we propose five new research avenues for consideration that may enhance our knowledge of cybersecurity risk and help practitioners develop a better cyber risk management framework.[6]

The rapid growth of network services, Internet of Things devices and online users on the Internet have led to an increase in the amount of data transmitted daily. As more and more information is stored and transmitted on the Internet, cybercriminals are trying to gain access to the information to achieve their goals, whether it is to sell it on the dark web or for other malicious intent. Through thorough literature study relating to the causes and issues that are brought from the security and privacy segment of wireless networks, it is observed that there are various factors that can cause the networks to be an insecure; especially factors that revolve around cybercriminals with their growing expertise and the lack of preparation and efforts to combat them by relevant bodies. The aim of this paper is to showcase major and frequent security as well as privacy issues in wireless networks along with specialized solutions that can assist the related organizations or the public to fathom how great of an impact these challenges can bring if every related stakeholder took a step in reducing them. Through this paper it is discovered that there are many ways these challenges can be mitigated, however, the lack of implementation of privacy and security solutions is still largely present due to the absence of practical application of these solutions by responsible parties in real world scenarios.[7]

The paper aims to raise awareness in the domain of security and privacy concerns in network communication that takes place among machines. Knowing that there are lots of possibilities that an attacker or hacker may get a slight chance of causing exploits from network vulnerabilities leads to threats at personal and organizational level. In this paper, research has been carried out using survey methodology to gather user viewpoints on general awareness and importance of network security and privacy. The results will be used to support the overall significance of how a network should behave and work on behalf of the users. The main goal as developers and engineers is to prioritize and improve user satisfaction and data protection standard. Therefore, this paper will also discuss the methodologies and possible ways to offer the best strategies for protection against security and privacy attacks.[8]

Vulnerabilities in software systems exist since the birth of computer systems. Along with the development and revolution in technology the risks and vulnerabilities also increased which is a great threat to the security of software systems. Hence, the security of software systems is an important issue even in today's world. Software could have vulnerabilities like an error, mistake, or flaw which can be accessible to hackers; allows them to violate the confidentiality and integrity of the software system and thus are dangerous and harmful for the system. Monitoring these vulnerabilities is very important so they need to be detected and removed completely from the system to protect it from attacks. However, it is challenging to do so. The goal of this study is to identify and predict the security vulnerabilities in software systems.[9]

In this COVID-19 pandemic, the use and dependency on Internet has grown exponentially. The number of people doing online activities such as e-learning, remote working, online shopping and others have increased. This has also led to increased vulnerability to cyber crimes. Cyber security attacks have become a serious problem. The common types of cyber security attacks are phishing, malware, ransomware, social engineering, identity theft and denial-of-service. The attackers target the victims in order to get their credential information or financial benefits. Those people who are doing online activities are vulnerable to cyber threats. This is because the network is not safe. The attackers are able to code according to the weaknesses of the Internet. Once the attackers hack into the devices, they have the root access and can do whatever they want to do with the device. In this research paper, the concept of cyber security attack and detailed research about real attacks are discussed. This is followed by detailed review about the recent cyber security attacks with a critical analysis. Moreover, the research paper will be proposing the latest research contribution of cyber security during COVID-19 and the implementation scenario which will give the examples about how the companies maintain privacy as well as the limitations. Then, the paper will be discussing the reasons that people are vulnerable to cyber security and the unique solution to the problems stated. Finally, this paper will conclude with an in-depth analysis and future direction for cyber security research.[10]

III. LIST OF FRAMEWORKS USED

1. Metasploit framework:

   The Metasploit Project is a PC security project that gives data about security weaknesses and helps in infiltration testing and IDS signature advancement. It is claimed by Boston, Massachusetts-based security organization Rapid7.

2. Armitage:

   Armitage is an incredible Java-based GUI front-end for the Metasploit Framework created by Raphael Mudge. Its will probably help security experts better comprehend hacking and assist them with understanding the force and capability of Metasploit.

IV. LIST OF TOOLS USED

1. Packer:

   Packer is an open source tool for creating identical machine images for multiple platforms from a single source configuration. Packer is lightweight, runs on every major operating system, and is highly performant, creating machine images for multiple platforms in parallel.

2. Vagrant:

   Vagrant is an open-source software product for building and maintaining portable virtual software development environments; e.g., for VirtualBox, KVM, Hyper-V, Docker containers, VMware, and AWS. It tries to simplify the software configuration management of virtualization in order to increase development productivity.

3. Vagrant Reloaded:

   The equivalent of running a halt followed by an up. This command is usually required for changes made in the Vagrantfile to take effect. After making any modifications to the Vagrantfile, a reload should be called. The configured provisioners will not run again, by default.

4. Git:

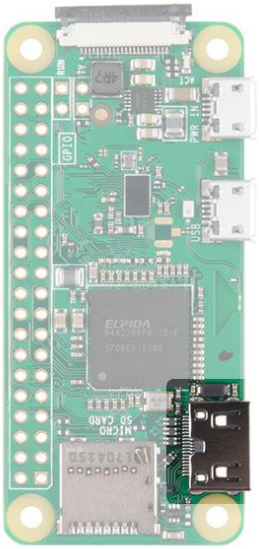
   Git tool is for tracking changes in any set of files, usually used for coordinating work among programmers collaboratively developing source code during software development. Its goals include speed, data integrity, and support for distributed, non-linear workflows.

V. SETTING UP RASPBERRY PI

a. **HARDWARE SETUP:**

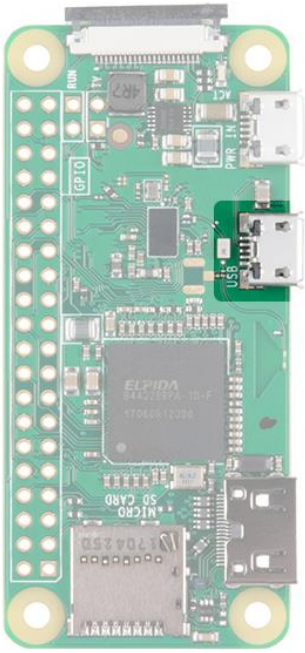
1. MINI HDMI :-

   Dissimilar to the past models of the Raspberry Pi which utilize a standard HDMI connector, the Zero uses a small scale HDMI connector to save space. To interface the Zero to a screen or TV, user will require a little HDMI to HDMI connector or cable.



2. USB ON THE-G0:

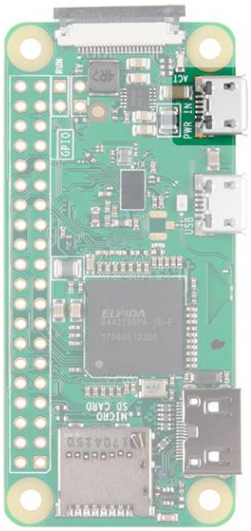
The Raspberry Pi 3 and different models have customarily had 2-4 standard size female USB connectors, which took into consideration all assortment of gadgets to associate including mice, consoles, and WiFi dongles. Again to save space, the Zero has selected a USB On-the-Go (OTG) connection. The Pi Zero uses the very Broadcom IC that controlled the first Raspberry Pi An and A+ models. This IC interfaces straightforwardly to the USB port taking into consideration OTG usefulness, in contrast to the Pi B, B+, 2 and 3 models, which utilize a locally available USB center point to consider different USB associations.



User is given alternative option to use the USB to micro-b adapter if required to access the USB port on the Pi Zero.

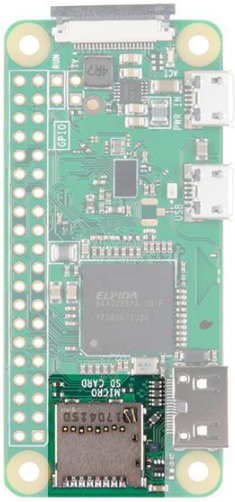
3. POWER:

Like other Pis, power is provided through a microUSB connector. Voltage supplied to the power USB should be in the range of **5-5.25V**.



4. MicroSD CARD SLOT:

Like different Pis, power is given through a microUSB connector. Voltage provided to the force USB ought to be in the reach of 5-5.25V.



5. WiFi AND BLUETOOTH:

Likewise with the Raspberry PI 3, the Zero W offers both 802.11n remote LAN and Bluetooth 4.0 network. This opens up large numbers of the associations that would have been made over USB, like a WiFi dongle and a USB console and mouse if subbing a Bluetooth console/mouse.

b. **HARDWARE ASSEMBLY:**

1. 1.To join the Pi Zero to a Monitor or TV that has a HDMI input, append a miniHDMI to HDMI link or connector to the miniHDMI connector on the Pi Zero. Associate the opposite finish to the HDMI port on your screen or TV.
2. Connect the USB OTG link to the Pi Zero through the microUSB connector. On the off chance that you have a console/mouse combe, append your dongle to the standard female USB end. In the event that where user have a different mouse and console, In such case user will require a USB center to append both tto the USB OTG link.
3. Make sure that the user is having a substantial Raspberry Pi picture on your microSD card (more on this later). Addition the microSD card into the microSd space.
4. Power the Pi Zero through the microUSB power input.

There are a few other connectors to point out but we won't be using. The Pi Zero has a 40 pin GPIO connector on the board that matches the pinout of the standard Pi 3. You can solder wires, headers or Pi Hats to this connector to access the GPIO pins or even power. The camera connector will allow you to connect the Raspberry Pi camera although it is worth noting that the connector is a 22pin 0.5mm and different than the standard Pi and will need a different cable to connect the camera to the Pi.

VI. MODELLING AND ANALYSIS

Upon the onset of the project, the working hypothesis of the research was that such aggregated picture would uncover key and critical points in the IT infrastructure. To be able to test this hypothesis in practice, we realized an experimental database with more than 55 domains. We further entered metrics and reference values for several domain groups including, but not limited to – hospitals and dispensaries, IT sector, banks, insurance companies, small and large administrative institutions, pharmaceutical companies, schools, kindergartens and a few others. Passive tests were carried out on different domains and domain groups and several mechanisms allowing information filtration and sorting based on different technical metrics were created.

Figure 1: The screenshot represents originating traffic

VII. RESULT AND DISCUSSION

This paper examined the cybersecurity problem of early warning, prognosis, vulnerability analysis and threat prevention and informed on the development and functionalities of an instrument providing an aggregated picture of the technical profile, standard behavior and vulnerabilities of a large number of independent systems that maintain services within the cyberspace. The development of the CyberMap and the ongoing larger project, embeds multiple research methods to develop a series of interconnected instruments that work together to provide a working product, that aims at allowing an end client to use tools, means and methods for the dynamic monitoring and analysis of the behavior of the web systems of specific target groups, by adding mechanisms for monitoring, historical retrospective and identification of symptomatic behavior models, which will allow for the early warning for mass cyberattacks and crisis threats. Our belief is that with such instruments and services we will be able to improve the efficacy of predicting, preventing and handling cybersecurity incidents and improve the overall cybersecurity posture.

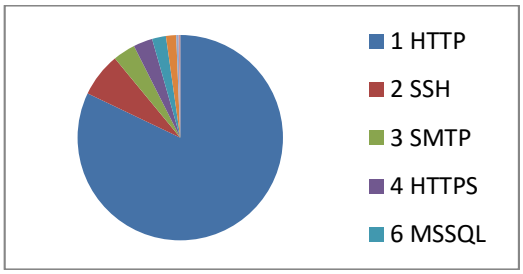


Figure 2: Top targeted services

Figure 3: Attack Success rate and Zero-day time frame

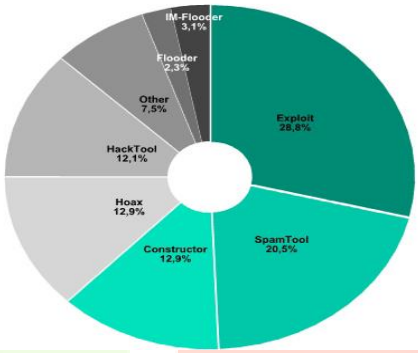


Figure 4: Breakdown of malware behaviour

REFERENCES

[1] Noor Zaman (Oct.2020) Detection and Mitigation of RPL Rank and Version Number Attacks in the Internet of Things: SRPL-RP

[2] Ruifeng Duo(Jan 2021) Anomaly Detection and Attack Classification for Train Real-Time Ethernet

[3] Sim Hoong Kok (July 2020) Early Detection of Crypto-Ransomware Using Pre-Encryption Detection Algorithm

[4] Isaac Chin Eian (Dec 2020) Integration of Security Modules in Software Development Lifecycle Phases

[5] Engr. Dr. Shahzadi Tayyaba (Jan 2020) Network Security and Internet of Things

[6]Md Hamid Uddin (Dec 2020) Cybersecurity hazards and financial system vulnerability: a synthesis of literature

[7] Alya Hannah Ahmad Kamal (Sept 2020) Security and Privacy Issues in Wireless Networks and Mitigation Methods

[8] Yong Weixiong(May 2020) Security and Privacy Concerns in Wireless Networks - A Survey

[9] Ahsen Ilyas (Oct 2020) Identifying and Predicting Security Vulnerabilities in Software Systems

[10] Isaac Chin Eian (Sept 2020) Cyber Attacks in the Era of COVID-19 and Possible Solution Domains