International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 11 Issue 8, August-2022, Impact Factor: 7.957

Making a Solution for the Horrible Problems Experienced by Indian Smartphone Owners

G Prasad Babu[1], Dr. Ashish Chandra Swami[2], Dr. Sikhakolli Gopi Krishna[3]

[1]Research Scholar, Department of Computer Science & Engineering, JS University, Shikohabad, Uttar Pradesh
[2]Associate Professor, Supervisor, Department of Computer Science & Engineering, JS University, Shikohabad, Uttar Pradesh
[3]Professor, Co-Supervisor & Professor Sri Mittapalli College of Engineering, Guntur, Andhra Pradesh.

ABSTRACT

Criminals represent a substantial danger to people, corporations, and society as a whole by exploiting holes in the security layers of the internet and the programs that function on it via social engineering. There are many different types of attacks that have made it simpler to break into a number of online services and applications. Some of these attacks include Denial of Service (DoS), Distributed Denial of Service (DDoS), Probe, Remote to Local (R2L), User to Root (U2R), HeartBleed, Exploits, Malware, Botnet, and Worms.

One of the most significant problems with the Internet is that criminals may falsify their Internet Protocol (IP) address and then use it to download dangerous information in an anonymous manner. The Internet Protocol (IP) brings forth the possibility of this happening. When it comes to intellectual property, it is possible. These vulnerabilities have been exploited by hackers on several occasions in their attacks, causing disruptions to a variety of online services and activities and causing irreversible damage to the targets of their attacks. Ever since the dawn of time, people have been trying to figure out a means to stop cyberattacks like this one from happening.

Many people have thought about potential remedies that may either lessen the frequency of attacks or put an end to the growing number of assaults. Components of this category of security technology include the ability to identify and prevent attacks, routers, security software, encryption, decoding, and IP traceback. Additionally, this category includes the ability to trace IP addresses. IP traceback and intrusion detection are two technologies that have been researched in the past, and the purpose of this thesis is to integrate them in order to better identify and mitigate potential risks in software-defined networking (SDN). It is common practice to install an intrusion detection system, also known as an IDS, in order to keep an eye on the network for any suspicious behavior or violations of the relevant policies. Because of this, any problems that may occur in the future may be resolved in a timely manner. There is a possibility that this approach may be used in the future to handle any problems that may occur. In the event that you are aware of the origin of the malicious assault packets, you have the ability to delete them by using an IP traceback algorithm.

The "SDN and MPLS Integrated Traceback Mechanism (SMITE)" is the name of the IP traceback system that will be included into an AS that is based on SDN when it is implemented. Right now, I am the one who will narrate the first story. While data bits are moving across an AS, the SMITE protocol makes use of MPLS labels to ensure that the original source IP addresses of the data bits are maintained. We are able to achieve a low false positive rate by using the benefits of MPLS and SDN. Additionally, we are able to track packets after they have been broadcast, identify and delete a single fraudulent attack packet, and do all of this with minimal expenditures on both data and hardware. I-SMITE is the best choice for those who are looking for an alternative to Inter-AS SMITE that they may use. As an example, OpenFlow incorporates software- defined networking (SDN), the border gateway protocol (BGP), and multiprotocol labeling (MPLS), which is sometimes referred to as "protocol labels," in order to accomplish this result. Due to the fact that ASes often share traceback information with one another via BGP Update Messages, IP traceback may be compatible with other ASes. Consequently, IP traceback may continue to work even in the presence of a large number of ASes. One of the many appealing characteristics of I-SMITE is its BGP support.

One other benefit that SMITE provides is this, which is only one of many advantages that it provides. The third argument is that there is continuous development of Intrusion Detection Systems (IDS) that make use of Support Vector Machines (SVM) to detect intrusions and selectively record IP addresses for the purpose of IP traceback. This is the third point. This brand-new intrusion detection system (IDS) makes use of both a portion of the NSL-KDD dataset as well as the whole dataset. Consequently, the chance of uncovering an attack is significantly increased as a result. With the help of the PACKET_IN event, it is possible to identify people who

have acquired access to the community network as well as data that does not belong there. OpenFlow switches are currently considered to be the standard method for collecting flow data on a regular basis. You are able to selectively collect suspicious packets or flows by using the PACKET_IN event functionality. By doing so, you will be able to determine the identity of the person who launched an assault on your network by using their IP address. In order to do this, one method is to monitor the happenings of the CPU while it is operating.

INTRODUCTION

In possession of a computer, a device that is capable of connecting to the internet, or another method of connecting to the internet. These technologies are used on a daily basis by individuals all over the world, and they have a tremendous influence on our behavior within the context of both our professional and personal lives. Its use in business environments is also growing at a rapid pace. A rising number of transactions are being recorded on the internet. Participating in these conversations are a diverse range of individuals hailing from a number of walks of life. Employment opportunities for these persons may be found in fields such as manufacturing, healthcare, banking, and social services. The challenge of preserving digital data, which was previously believed to be impossible, has become viable as a result of the introduction of new technologies such as cloud storage. An important step forward has been taken in this regard. This part includes a broad range of papers, such as corporate files, health data, and financial information, among other types of documents. The management of infrastructure activities, such as the collection of trash and the production of power, is increasingly being handled by software-driven systems. The amount of individuals who depend on the Internet and the improvements in technology are both contributing factors that are driving an increase in the interest of hackers in getting into systems.

The "Global Economic Crime Survey 2016" found that at least one- third of the companies that were surveyed have experienced some kind of cybercrime themselves. In light of the fact that these breaches take place on a regular basis, individuals who deal with foreign cash are intrigued by them. It is possible for hacking to result in a variety of unfavorable results; nevertheless, according to the findings of the study, hurting someone's reputation is the most detrimental of these outcomes. A total of five million rupees (PS3.5 million) in losses were recorded by the enterprises that responded to the survey, with one-third of those businesses claiming losses that were more than one hundred million rupees (PS69 million). It may be deduced from this that at least fifty percent of the businesses that took part in the poll reported suffering a loss. In recent years, there has been a rise in both the number and severity of hacking attacks, according to the findings of the "Cyber Security Breaches Survey 2020" conducted by the government of the United Kingdom. Based on the findings of the survey, around 26% of non-governmental organizations (NGOs) and 46% of businesses had a data theft or hacking event over the last year. Based on the information provided by the company, Kaspersky Lab discovered an extra 360,000 harmful files every single day in the year 2020. In comparison to this time last year, there have been almost 18,000 new members that have joined up. Furthermore, there is a further rise of 5.2% that is seen. Object-finding sensors in the laboratory were able to locate the malicious software for tracking.

Criminals are responsible for the creation and dissemination of new forms of malware on a regular basis, as shown by the frequency with which new kinds of harmful files are detected everyday. Despite the major developments in technology, criminals may still use the Internet to prey on people, businesses, or even the state or military. This is the case even if the Internet has not disappeared. Due to the fact that denial of service (DoS) assaults have been carried out, a number of internet services have become less reliable. At the time of its debut, a firm need to be aware of these common risks and make efforts to reduce them at the same time. Hacking and data breaches are risks that are always changing and growing, and the tools that are used to perpetrate these types of crimes are becoming more readily available.

When you hear the term "malware," you certainly think of a wide variety of apps that are damaging to your computer. The goal of these programs is to steal data or cause damage to computer systems and networks using malicious software. Malware refers to a broad category of harmful software that includes a wide range of applications. Computer viruses, Trojan horses, worms, spyware, and ransomware are all included in this category. Adware, malware, and rubbish are all included in a single handy package at your disposal. Whenever the receiver reads the email or clicks on a link included within it, the message is sent to the machine that has been selected to receive it. When users attempt to access crucial portions of a network, they may be prevented from doing so by viruses and other types of malicious software. Not just humans, but also a wide variety of other animals and organisms are vulnerable to viral infection. Not only does it take critical data from the computer of the victim, but it also has the potential to ruin or damage gadgets, rendering them without value.

In order to achieve their goals, hackers may sometimes make use of phishing emails that seem to have originated from reputable firms. One of these strategies is known as "phishing." It is possible that the personal computers of potential victims may be hacked if they were to click on the malicious link included within the email. This could result in the exposure of sensitive information such as passwords and contact information.

The term "spear phishing" refers to a sophisticated kind of email fraud that is directed against specific persons, businesses, or organizations with the intention of stealing critical financial information. One of the strategies that con artists use is known as spear phishing. Managers and executives of companies are the focus of these assaults since they are dependent on the technology in question.

The term "man-in-the-middle attack" refers to the situation in which one party covertly listens to the conversation of another party. The word that is often used to describe this is the "eavesdropping danger." An person who has access to this information could be able to access the accounts of both of the people who were participating in the chat. The systems, networks, or websites that are the targeted targets of "denial of service" (DoS) attacks are subjected to an excessive volume of data, which makes it hard for them to differentiate between legitimate requests and spam. Despite the fact that possibilities are presented to them, the criminal may choose not to take use of them. For instance, a global denial of service strike is an example of a DDoS attack that has been meticulously prepared. In the vast majority of cases, they are able to get access to the system that they want to attack by using personal computers and other devices that are readily hackable. You may load SQL by following these steps: The vulnerability known as SQL injection makes it possible for malicious actors to obtain access to computer systems. Due to this, it is possible for malicious code to be injected into SQL queries that are sent by websites. Through the use of SQL queries in databases, criminals have the ability to access sensitive data and modify or delete entries at their discretion.

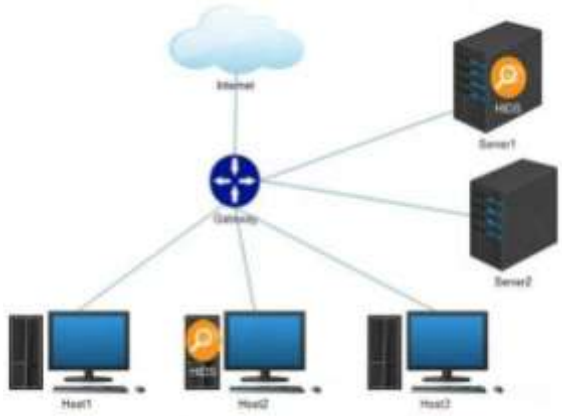

Figure 1.3: Host based IDS

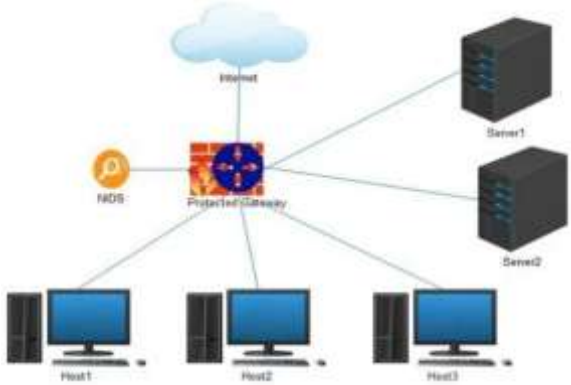

Figure 1.4: Network based IDS

LITERATURE REVIEW

1. Studies emphasize that technological tools alone cannot safeguard users if they lack basic knowledge of cyber threats. Awareness programs ensure that individuals understand risks such as phishing, malware, unsafe browsing, and data privacy violations, making them active participants in their own security.
2. Existing literature highlights the effectiveness of structured training modules that explain cybersecurity concepts in simple, understandable formats. Educational content—delivered through videos, tutorials, quizzes, or workshops—helps users learn essential skills such as password hygiene, secure app practices, and recognizing suspicious links or messages.
3. Research shows that gamification techniques—like rewards, badges, points, and interactive challenges—make cybersecurity training more engaging and memorable. Users who participate in gamified learning demonstrate higher retention of security rules and improved long-term behavior.

BACKGROUND RESEARCH

Companies are beginning to see cybersecurity measures as a means to safeguard themselves against one of the most significant threats they face. The United States, the United Kingdom, and India are just a few of the many countries that have passed anti-hacking legislation to safeguard their citizens' personal information. The prevalence of hacking has prompted the establishment of regulations aimed at securing the internet. More and more, cyber-physical technologies, like the Internet of Things (IoT) and smart grids, are placing a premium on security. Cybersecurity is more than simply a field for engineers and computer scientists. A perspective is required instead. End users and technological security measures Several different kinds of personal information, including but not limited to medical records, bank passwords, and phone numbers, have all been hacked. There are two types of errors: deliberate and inadvertent. Weak passwords, poor data management, employing obsolete or malicious software, and unwittingly unleashing malware are the most common types of mistakes that may occur. According to a research conducted by CybSafe using data obtained from the Information Commissioner's Office (ICO) in the United Kingdom in 2019, human mistake was responsible for ninety percent of all data breaches. "Inappropriate sharing of data through mobile devices" and "inappropriate use of IT resources by employees" are the two leading causes of data catastrophes, according to the research that was conducted by Kaspersky (Kaspersky 2021). According to the study conducted by Netwrix (Netwrix 2020), over half of the respondents did not follow the safety procedures and requirements.

A wide variety of behavioral and social science ideas have been used by researchers over the course of the last two years in order to investigate several elements of hacking. Among these studies, Vieane et al. conducted an investigation on the impact that pauses in work have on the operations of cyber security. During the course of the study, it was found that taking breaks reduces the level of defense. The impact of distractions and situational awareness on cyberdefense activities have been explored by researchers Fugate, Rogers, and Gutzwiller Ferguson-Walter. Both of these researchers have conducted their studies. According to Nurse et al., Assarut, Bunaramrueang, and Kowpatanakit, as well as Mohamad, Hamin, Nor, and Aziz, the personalities of the individuals who carried out the attacks have also been investigated via the use of behavioral and social scientific methodologies. Previous studies focused mostly on the behaviors of individuals when they were at their places of employment or at home. Because it has the capacity to strengthen the weakest link, it is conceivable to perceive greater human utilization of technology as a safety guarantee. This is so because of the potential that technology possesses. According to Mashane and Kritzinger, a person's cybersecurity behavior includes their behaviors, emotions, and general attitude when they participate in online activities. Activities related to cybersecurity are carried out by individuals when they make use of security technologies, adhere to security behavior, and steer clear of potentially harmful user behavior.

PROCEDURES AND SCHEMAS

Companies are beginning to see cybersecurity measures as a means to safeguard themselves against one of the most significant threats they face. The United States, the United Kingdom, and India are just a few of the many countries that have passed anti-hacking legislation to safeguard their citizens' personal information. The prevalence of hacking has prompted the establishment of regulations aimed at securing the internet. More and more, cyber-physical technologies, like the Internet of Things (IoT) and smart grids, are placing a premium on security. Cybersecurity is more than simply a field for engineers and computer scientists. A perspective is required instead. End users and technological security measures

Ethernet switches have the ability to manage traffic from distinct VLANs in a variety of different ways, depending on the identification of the VLAN. These methods include accepting, blocking, or promoting certain patterns of VLAN traffic. It is unfortunate that the VLAN tag is not sufficient to convey the source IP address. If you want to utilize additional data in the IP header, you will need to do so. Because of this, it is evident that the use of a separate object for IP traceback is rendered worthless, with the exception of the data included in the IP header. In addition to this, MPLS may support a considerable number of standards, while VLAN may only support Ethernet. When using MPLS, rather of using large network names, short route labels are used. The packet routing approach is now easier to comprehend, which has resulted in the network being managed in a manner that is both much more efficient and less complicated. As a result of the rigorous Class of Service (CoS) and Quality of Service (QoS) guarantee, the network is able to effectively manage and organize data in order to fulfill all of its requirements.

See Figure 3.1 for an illustration of the construction of the SMITE device. (i) linking Macs to ports and ports to IPs; (ii) maintaining SMITE Flow; (iii) encoding and decoding MPLS labels; and (iv) the REST API module are the four key components included inside this system. Port-to-MAC address mappings are stored in the MAC address database, whereas IP address mappings from ports are stored in the area reserved for the ARP table. The following two essential data structures are looked after by this utility: both Mac-to-Port and Port-to-IP ports. The Media Access Control (MAC) address table is the very first item that is generated once a network is booted up. When there is a change in the status of a port or switch, it is often updated. An ARP table is filled with information whenever the first packet in a flow arrives, which is referred to as the PACKET_IN event. When flow items in the switch come to an end, the data structures for the ARP table are likewise filled in. When a manager adds a flow entry for the next packet in the same flow at the

switch, a new PACKET_IN event is generated when the packet enters the network. This occurs just as the packet is entering the network.

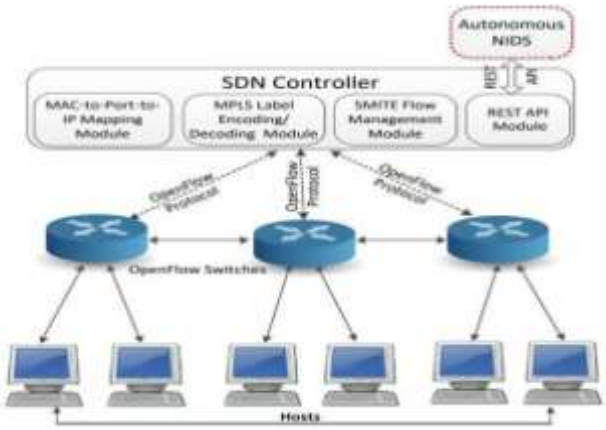

Figure 3.1: SMITE Architecture

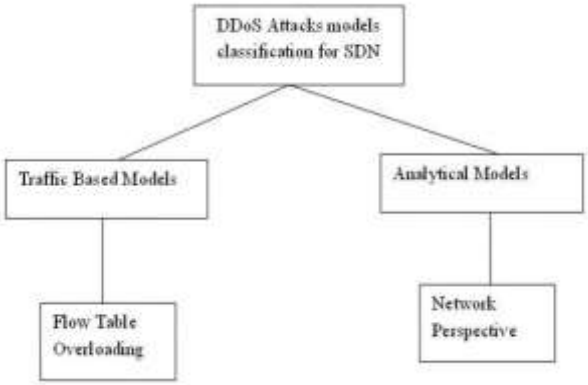

Figure 3.5: Classification of DDoS attacks models for SDN

Forecasts based on traffic data: These studies replicate both the context of the network as well as the behavior of attack techniques. The idea that software-defined networking (SDN) networks might be susceptible to flow table overflows was first proposed by B. Yuan and colleagues. The queuing theory model is used in order to establish the mathematical limits that are placed on the resources that OpenFlow forwarding devices may be able to retain. Through the use of this method, it is possible to readily determine the effect that distributed denial of service attacks have on SDN device flow tables. There are a number of characteristics that are taken into account, such as the number of switches, the size of the flow table, the arrival and service rates, the attack rates, the length of time that attacks last, and the waiting times. Unfortunately, the model does not give any insight into the mechanics of attacks since it does not incorporate the influence of other SDN components, such as the controller and the SBI.

This is the reason why the model could not provide any insight. Multiple points of view were: When specific characteristics are taken into consideration, analytical models are used in order to ascertain the likelihood of an attack occurring. In their study, X. Wang and colleagues proposed a model for a distributed denial of service (DDoS) attack and detailed the criteria for such an attack from the point of view of network architecture. A set of hosts, switches, linkages, target hosts, routing protocol, attackers, attack length, and assault rates are all important factors to take into account. It looks more like a network diagram than a statistical model did when it was first created. A security solution that applies tight access control is proposed by the authors as a means of reducing the possibility of distributed denial of service attacks.

The transmission of an excessive number of requests is the main purpose of a denial-of-service attack, which is designed to prevent the network from making use of its resources. The picture makes it very evident that the two fundamental factors that contribute to distributed denial of service attacks are the exhaustion of resources and the exhaustion of bandwidth. Remember to keep the reasoning in mind. In accordance with the information presented in Section, a statistical model is constructed in order to ascertain the single feature that is the most effective DDoS assault defense. It is possible that we will talk about a better mathematical model in this part. This model is based on the idea of resource depletion and the internet. These are some of the things that are covered in the conclusion for improved management of distributed denial of service attacks.

TESTS AND FINDINGS

Within the Reserved Flag (RF) field of the Internet Protocol (IP) header, the first bit of the source IP address is encoded. An MPLS label is included within the 31 bits that are shown below. It is always the case that the SMITE Label is the top label in MPLS. We are not going to use this label for the purpose of label swapping as our label. Figure 1 and Equation 4.1 both provide a schematic that illustrates the design of the I-SMITE Label device.

Additionally, it is the duty of the MPLS Label Encoding/Decoding Module, which is situated at the very last MPLS edge router (LER), to decode the message and ascertain the IP address that was used as the message's initial source. 31 bits are taken from the MPLS label of the packet, and one bit is taken from the RF field. These are the bits that are retrieved from the IP header. The original source IP address of the packet is referred to as the I-SMITE Address. This address is rebuilt by the MPLS Label Encoding/Decoding Module of the router. Combining the 31-bit I-SMITE Label field with the 1-bit RF field of the packet allows for its discovery at the exit Label Edge Router (LER). By using Equation 4.2, it is possible to achieve this goal.

The I-SMITE Module is the one that is accountable for the creation of the I-SMITE Flow as well as the configuration of it on the OpeFlow switches at the packet_in event. A flow rule that is referred to as the I-SMITE Flow is the one that is responsible for putting the I-SMITE Label as the first MPLS label on IP packets that are traveling over the I-SMITE network. It is shown in Algorithm 4.1 that the I-SMITE Flow control module is activated whenever the packet is processed via the algorithm. When used with ISMITE, the Inter-AS BGP tool makes it possible to track IP addresses from one host to another. Critical I-SMITE data was sent using BGP update messages in order to shut down ASes. (See Figure 4.3a) Every single BGP update message is made up of three different components that make up the Path Attributes. The attribute type field has two octets, and each of them is occupied by one of the two attributes: the attribute flags and the attribute type code. One of the highorder bits in the attribute flags specifies whether the attribute is well-known, while the other bit indicates whether the optional attribute is transitive (0). Both of these bits are components of the attribute flags. It can be seen in Figure 4.3a that both of these bits have been set to the value 1. It is common practice to include the attribute code number of a certain BGP route attribute inside the attribute type code. A new attribute code number, on the other hand, will be included in the attribute type code alongside the I-SMITE. As long as you have the appropriate permissions, you will be able to generate a new BGP feature type code and send it to IANA. In spite of the fact that RFC 6938 recommends against the use of Path Attribute Value 11, it is still possible for I-SMITE to be allocated a BGP Path Attribute Value of 11.

The code that represents the length of the property is included inside the third bit of the BGP Path Attributes. The quantity of octets that constitute the value of the attribute at the given time. It is common for attribute number fields to have a length of sixteen octets, which is enough for our needs when the Attribute Length Code field is set to sixteen. The Attribute Length Code provides an indication of the various lengths that may be assigned to the Attribute Value. In order to read the Attribute Value, which is made up of the last eight bits of the Path Attribute, the values of the Attribute Flags and the Attribute Type Code are used. In the new BGP I-SMITE Attribute Value field, the I-SMITE Address, the Source IP address, and the Destination IP address each take up four octets corresponding to their respective addresses (Fig. 4.3b). In a similar fashion, the AS number that came before it is made up of four octets. Through the integration of BGP with SDN and MPLS, I- SMITE evolved into a technology that can track IP addresses throughout the whole Internet. The scope of its use has broadened to include a number of AS SDN-based networks. After that, we will discuss the technique for I-SMITE Inter-AS traceback operations. The ARP tables and the MAC tables are the two tables that are responsible for storing the mappings that exist between ports and IP addresses. It is these two data structures that are updated that are considered to be the most essential. When the manager first starts the process of detecting networks, the first thing they do is update the MAC and ARP databases with new entries. In order to reflect any modifications that have been made to the ports and switches, these records are updated. The processes that must be followed in order to implement I-SMITE are outlined in pseudocode. The process packet that is included inside the handler is responsible for classifying incoming packets according to the forms that they take, as shown in Figure 4.1. IPv4, Address Resolution Protocol (ARP), Multiprotocol Label Switching (MPLS), and other categories are included among them. Therefore, this is very important since the manager is required to do a variety of activities for each kind of packet. For example, the "paketin_arp" sub-procedure is called upon in order to complete the processing of an ARP message. For the purpose of processing the MPLS packet, the sub-procedure known as "_packetin_to_lsr()" is called upon in the event that the router type is an LSR. The "_packetin_from_mpls_network()" subprocedure is executed when an LER router type is triggered to initiate its execution. In the event that the IPv4 packet is ICMP-based, a sub-procedure known as "_packetin_icmp_req()" is carried out, and one known as "_packetin_tcp_udp()" is carried out in the event that the packet is TCP-based. It is important to note that the subprocedure is activated whenever there is an extra IPv4 message.

CONCLUSION

There are a multitude of security measures that have been offered in order to stop and limit the many types of hacking. Some of these ways include IP traceback, intrusion detection, intrusion prevention, encryption and decoding, firewalls,

antivirus software, and many more. Our objective in this study is to improve the safety of the network by integrating the detection of intrusions with the tracking of IP addresses. The process of finding invasions has been approached from a wide variety of perspectives up to this point. On the other hand, these intrusion monitoring systems are plagued with a multitude of issues. Any method of attack detection is subject to the two primary problems of false positives and false negatives. False positives refer to packets that are improperly detected as attacks, while false negatives refer to packets that are incorrectly classified as normal. In the event that detecting and preventing attacks is not sufficient, we need to acquire a method that can reliably identify the origin of assaults in order to ensure that those responsible are held accountable. IP traceback is a practical response to the problem of cyberattacks, which shows the real source of a phishing message. This strategy is one of the practical approaches.

If you use IP traceback, you will not be able to stop or avoid an attack. Instead, its objective is to determine the origin of the problematic packet, either during or after an attack. This may be done either during or after the attack. The identification of the offender, the disclosure of their name, and the implementation of measures to guarantee that they are held accountable for the attack are the key goals of IP traceback. The combination of an intrusion detection system (IDS) with a traceback mechanism is a logical step that would considerably enhance the level of security that existing networks possess. The public has been made aware of certain logging IP traceback systems in order to counteract the many different types of hacking. The SPIE, which was developed by Snoeren and colleagues, is an instrument that has received a lot of attention in this area. Certain servers along the path of the network are responsible for storing information on packets that are currently in transit. According to the authors of the proposal, in order to generate a packet fingerprint, one should make advantage of the fixed aspects of the IP packet header. They recommend avoiding the ToS, TTL, Checksum, and Options fields, which are subject to major changes.

REFERENCES

[1]. PricewaterhouseCoopers, PwC, Global economic crime survey 2016, 2016. [Online]. Available: https://www.pwc.com/gx/en/economic- crime- survey/pdf/ GlobalEconomicCrimeSurvey2016.pdf (visited on 11/03/2020) (page 1).
[2]. Department for Digital, Culture, Media and Sport, Govt. of UK, Cyber security breaches survey 2020, 2020. [Online]. Available: https://www.gov.uk/government/ statistics/cyber- security-breaches-survey-2020/cyber-securitybreaches-survey- 2020 (visited on 11/03/2020) (page 1).
[3]. Kaspersky Team, Kaspersky malware detection 2020, 2020. [Online]. Available:https://www.kaspersky.com/about/press- releases/2020_the-numberof-new-malicious-files-detected-every-day-increases-by-52-to360000-in-2020 (visited on 11/03/2020) (page 2).
[4]. P. G. Neumann, “Inside risks: Denial-of-service attacks,” Commun. ACM, vol. 43, no. 4, p. 136, Apr. 2000, issn: 0001- 0782. doi: 10.1145/332051.332797. [Online].Available: https://doi.org/10.1145/332051.332797 (pages 2, 3).
[5]. G. Carl, G. Kesidis, R. R. Brooks, and Suresh Rai, “Denial- of-service attack-detection techniques,” IEEE Internet Computing, vol. 10, no. 1, pp. 82–89, 2006. doi: 10. 1109/MIC.2006.5 (pages 2, 14).
[6]. Y. Xiang, K. Li, and W. Zhou, “Low-rate DDoS attacks detection and traceback by using new information metrics,”
[7]. IEEE Transactions on Information Forensics and Security, vol.
[8]. 6, no. 2, pp. 426–437, 2011. doi: 10.1109/TIFS.2011.2107320.[Online]. Available: https://doi.org/10.1109/TIFS.2011.2107320 (pages 2, 14, 78). [7] V. M. Igure and R. D. Williams, “Taxonomies of attacks and vulnerabilities in computer systems,” IEEE
[9]. Communications Surveys Tutorials, vol. 10, no. 1, pp. 6– 19, 2008. doi: 10.1109/COMST.2008.4483667 (page 3).
[10]. N. Hoque, M. H. Bhuyan, R. Baishya, D. Bhattacharyya, and J. Kalita, “Network attacks: Taxonomy, tools and systems,” Journal of Network and Computer Applications, vol. 40, pp. 307–324, 2014, issn: 1084-8045. doi: https://doi.org/10.1016/j.
[11]. N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, “OpenFlow:
[12]. Enabling innovation in campus networks,” ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69–74, 2008 (pages 6, 11, 27, 44, 59).
[13]. H. Kim and N. Feamster, “Improving network management with software defined networking,” IEEE Communications Magazine, vol. 51, no. 2, pp. 114–119, 2013 (pages 6, 11, 27, 44, 59).
[14]. T. D. Nadeau and K. Gray, SDN: Software Defined Networks: an authoritative review of network programmability technologies. " O’Reilly Media, Inc.", 2013 (pages 6, 11, 27, 44, 59, 78, 79).
[15]. S. Sezer, S. Scott-Hayward, P. K. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller, and N. Rao, “Are we ready for SDN? implementation challenges for software- defined networks,” IEEE Communications Magazine, vol. 51, no. 7,pp. 36–43, 2013. doi: 10.1109/MCOM.2013.6553676