AI Tech International Journal
Vol. 1, No. 1, July-December, 2023
Journal homepage: https://techaijournal.com

The Development of a System to Address the Cyanenes of Indian Smartphone Users

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.

Article Info

Article history:
Received July 07, 2023
Revised September 12, 2023
Accepted September 17, 2023
Published September 22, 2023

Index Terms:. *Software-Defined Networking (SDN),IP Traceback, Intrusion Detection System (IDS), MPLS Labeling, SMITE Framework.*

ABSTRACT

By taking advantage of weaknesses in the Internet and the apps that run on it, criminals are able to carry out a wide range of attacks on individuals, organizations, businesses, and the population as a whole. As a result of attacks such as Denial of Service (DoS), Distributed Denial of Service (DDoS), Probe, Remote to Local (R2L), User to Root (U2R), HeartBleed, Exploits, Malware, Botnet, and Worms, a great number of online services and apps have become very unstable. The fact that the Internet's core technology, Internet protocol (IP), makes it possible for an attacker or attackers to cover their traces by faking the original IP address of a packet is one of the most significant problems with the Internet. As a result of hackers taking advantage of this vulnerability, several assaults have been carried out, interrupting a variety of internet services and activities and inflicting longterm damage to the individuals who were supposed to be the targets of these attacks. Since the beginning of time, the scientific community has been struggling with the question of how to maintain the integrity of the Internet in the face of breaches such as this one.

A great number of suggestions have been put up in an effort to put an end to or lessen the frequency of attacks, which have grown more frequent. The following are all examples of things that fall under this category: security software, firewalls, encryption, decoding, IP traceback, and intrusion detection and prevention. The purpose of this thesis is to give fresh techniques to recognizing and preventing attacks in software-defined networking (SDN) by combining two methods that have been studied in the past: IP Traceback and Intrusion Detection. In order to take the required steps to fix any difficulties that may occur, it is standard practice to utilize an intrusion detection system (IDS) to monitor the network for any odd activity or policy violations. This allows for the potential resolution of any issues that may arise. IP traceback is a technique that may be used to identify the individuals responsible for malicious attack packets by tracking their origin.

The "SDN and MPLS Integrated Traceback Mechanism (SMITE)" is an Internet Protocol (IP) traceback system that will be deployed in a single SDN-based autonomous system (AS). The first work is being presented by myself. SMITE makes use of MPLS labels in order to maintain the original source IP addresses of data packets as they travel from their point of origin to their final destination inside an AS. Using the power of MPLS and the adaptability of SDN, it is able to accomplish a low false positive rate, post-hoc packet tracing, the capability to detect and delete a single fraudulent attack packet, and all of this with a minimal amount of data and hardware expense. I-SMITE, which is a variation of Inter-AS SMITE, is the secondary option. In order to

do this, OpenFlow utilizes a combination of software-defined networking (SDN), border gateway protocol (BGP), and multiprotocol labeling (MPLS), which it refers to as "protocol labels." IP traceback is able to work between ASes because BGP Update Messages are used to transfer traceback information across ASes. This allows IP traceback to function from one ASe to another. I-SMITE is made more appealing by the use of BGP, which is an additional example of the many benefits that SMITE offers. Thirdly, there is some research being done on Intrusion Detection Systems (IDS) that make use of Support Vector Machines (SVM) to identify intrusions and selectively record IP addresses for the purpose of IP traceback. Both the whole NSL-KDD dataset and a subset of its features are used by the proposed intrusion detection system (IDS), which results in a significant increase in the chance of attack detection. Through the use of the PACKET_IN event, the manager has the ability to identify network intrusions as well as unusual data. Starting from this point forward, the OpenFlow switches will be used for the gathering of daily flow statistics. A PACKET_IN event allows you to selectively capture suspicious packets or flows, which allows you to begin an IP traceback in the event that an attack is launched against your network. One potential solution would be to log at the CPU level; doing so would greatly cut down on the amount of RAM that is being used overall. Additionally, the solution makes use of in-memory structures at the manager for reporting operations, which results in a considerable reduction in the amount of memory that is used in comparison to the traditional file-based database.

INTRODUCTION

At this point in time, almost everyone has access to a smartphone, the internet, and Internet of Things devices. Every one of us relies on these technologies on a daily basis, and they have a huge impact on the way we behave both at home and in the workplace. Additionally, it has become ubiquitous in the business sphere. A significant number of transactions in the contemporary era are conducted online. These transactions include those involving the corporate and governmental sectors, the armed forces, healthcare, social services, finance, and industrial institutions. Internet technologies such as cloud storage have also made it feasible to keep a broad range of sensitive data online. This is a significant development. There is information on individuals' medical records, bank accounts, and military records that may be found in this section. The management of garbage and the production of power is just another example of an infrastructure activity that is becoming more reliant on software-driven systems. As a result of the growing dependence on the Internet and the improvements in technology, cybercriminals have developed a strong interest in hacking. The findings of the "Global Economic Crime Survey 2016" indicate that hacking has an effect on 32 percent of surveyed firms. On account of the fact that these offenses have grown so pervasive, they are now among the most talked about problems in the field of international finance.

According to the findings of the study, hacking does a great deal of damage, but the damage that is carried out to someone's reputation is the most serious. Nearly one-third of the individuals who participated in the survey reported losses that were more than one hundred million dollars (PS69 million), and fifty or more businesses reported losses that were greater than five million dollars (PS3.5 million). It has been determined by the "Cyber Security Breaches Survey 2020" conducted by the government of the United Kingdom that hacking has developed and grown more widespread in recent years. According to the findings of the survey, in the last year, over half of all enterprises (46%) and a quarter of all non-profit organizations (26%) were victims of some kind of data breach or hacking. The Kaspersky Lab reports that in the year 2020, an additional 360,000 dangerous files were detected each and every day.

That is an increase of almost 18,000 when compared to the previous year. In addition to that, the data indicate that there was an increase of 5.2%. Object-finding devices were used in the laboratory in order to detect the malicious program. It is clear that criminals are developing and disseminating an increasing amount of malware, as the number of dangerous file types that are identified each day continues to increase. Even though there have been great breakthroughs in technology, the Internet is still susceptible to attacks from hackers and other criminals that target people, businesses, the government, and the military. There are a wide variety of different types of internet services that have been severely impacted by DENIAL OF SERVICE (DoS) assaults. At this point in time, these are among the most common threats that businesses need to be aware of and defend themselves against.

In the world of hacking and cyberattacks, new forms and varieties are always being developed and introduced."Malware" is an umbrella term that encompasses a wide variety of malicious software programs that are designed to cause damage to computers and networks in order to steal data or inflict harm. As a result, ransomware, spyware, worms, Trojan horses, and viruses are all included in the category of malware. This package contains adware, bloatware, and harmful apps all rolled into one. The information is uploaded to the server whenever a user either opens an email or clicks on a link and opens it. Malware, when it is implemented, has the ability to restrict access to vital areas of the network, so imitating the behavior of ransomware. There are other organisms that may be harmed by viruses besides humans. Further, it is able to steal important information from the system of the victim, as well as damage or destroy devices, rendering them useless in the process. In order to commit cybercrime, it is standard practice for hackers to send malicious emails that are disguised as contact from reputable companies. It is known as phishing. It is possible that those who receive the email may be persuaded to click on the malicious link, which might put their computer at risk and reveal personal information such as passwords and credit card numbers.

Spear phishing is a more advanced kind of phishing that involves targeting specific persons, corporations, or organizations with the intention of stealing sensitive financial or banking information. Scammers employ spear phishing to do this. Individuals who make use of systems, such as corporate leaders and managers, are considered to be the intended users. An example of a man-in-the-middle attack would be someone listening in on a conversation that is taking place between two people without having their knowledge. This phenomenon is sometimes referred to as the "eavesdropping danger." This information might then be used by an enemy in order to get access to the accounts of both of the individuals who participated in the chat.

Attacks that are classified as "Denial of Service" (DoS) in nature render it difficult for systems, networks, or websites to respond to legitimate requests by flooding them with an excessive amount of data. On occasion, the culprit may even steal the agreements that are being struck between the people involved. Distributed denial of service attacks, sometimes known as DDoS attacks, are among the most crafty of these attacks. In order to put the target system at risk, they make use of a large number of vulnerable personal computers and other devices.

The process of importing SQL It is possible for hackers to get access to a database using a technique known as SQL injection. This technique involves putting malicious code into SQL queries that make use of online inputs from a website. When SQL injection is carried out, the malicious actor has access to the databases and has the ability to modify or remove data that is vital to the operation.Attack That Is Unpredictable When a security hole in a network is found and made public, but no fix has been installed at this time, this is an example of a zero-day risk.

The decryption code is sometimes supplied to the receiver after the ransom has been paid when it is finally received. *: The Domain Name System is Under Attack In an attempt to take advantage of weaknesses in the Domain Name System (DNS), attackers undertake a DNS attack. DNS assaults may be broken down into two separate categories. The practice of hackers exploiting weaknesses in the Domain Name System (DNS) in order to route people to malicious websites is referred to as DNS Hijacking. When hostile actors move data to a system that is not secured, this is an example of the behavior known as DNS tunneling.

The Dangers of the Internet of Things In both their homes and places of employment, an increasing number of individuals are using internet-connected smart devices, which are also commonly referred to as Internet of Things devices. Unbelievably, just a small percentage of Internet of Things devices really adhere to stringent security protocols. Because of this, they are susceptible to infections caused by malware, whereby malware infestations may be used by hackers to get into your home or office network.

The term "denial of service attack" does not refer to all forms of hacking attempts. The hacker who launches a denial-of- service assault (also known as a DoS attack) does not need physical access to the network that has been infiltrated, which differentiates it from other types of hacking attack. There are three basic forms of denial-of-service attacks that may be separated from one another based on the reason behind them. DDoS attacks that are launched from a distance: Ping attacks, Smurf attacks, and ARP storm attacks are the most popular kind of denial-of-service (DoS) attacks that may be carried out via the Internet without compromising a network. Smurf attacks are even more prevalent than Ping attacks.

• Making use of a vulnerability that is already known In the initial stage of the second kind of denial-of-service attack, the hacker takes control of a limited number of websites by taking advantage of weaknesses in the network. When that time comes, they make full use of all of the resources that are available to them.

Digital Denial of Service Attacks (DDoS): This is the fourth and last kind of denial-of-service attack that may be carried out. This kind of hack is also known as a digital denial of service attack, which is another term for it. Defending oneself against this kind of assault is challenging because of the intricacy and difficulty of such attacks. In order to launch a distributed denial of service (DDoS) assault against a target website, it is necessary to breach the security measures of machines that are controlled by third parties.

The attack is then started by using these devices in the subsequent stages. Another word for computers that have been infiltrated is "zombies." Figure 1.1 illustrates a typical distributed denial of service attack that may be seen in its entirety. A hacked manager might unleash a data deluge on weak intermediate sites, which are commonly referred to as "zombies." This kind of assault is typically carried out by these sites. A hacker may flood devices with data in order to make them unworkable. One example of this would be the Web Server for example.

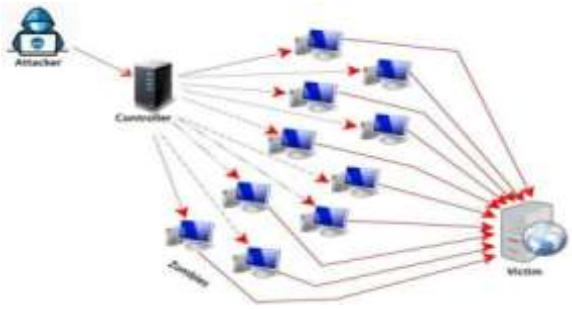

Figure 1.1: DDOS attack example

LITERATURE REVIEW

1. The literature consistently shows that India has emerged as one of the world's largest and fastest-growing smartphone markets. Increased affordability, widespread 4G/5G access, and government initiatives such as Digital India have pushed millions of citizens toward daily smartphone usage. Researchers point out that smartphones have become central to essential activities such as digital payments, e-governance services, entertainment, and communication.
2. Studies report that mobile applications now dominate banking, shopping, bill payments, and social media interactions. The convenience of mobile wallets, UPI-based apps, and online services has significantly increased dependency on smartphone ecosystems. This growing reliance has expanded the threat landscape, making smartphones a primary target for cybercriminals.
3. With increased usage, Indian smartphone users face a variety of cyber threats. Existing research lists common risks such as phishing (fake links and messages), malware-infected apps, spyware, data theft, SIM swapping attacks, and sophisticated social engineering scams. Cybercriminals often exploit users' lack of awareness to steal personal data, financial information, or access online accounts.

BACKGROUND WORK

An examination of the research that investigates the security behavior of mobile users and the frameworks that are currently in use is presented in this chapter. At the beginning of the chapter, consideration is given to the significance of an integrated cybersecurity strategy as well as the human aspect in the field of cybersecurity. Within this part, we will examine research that has been conducted on the behavior of smartphones and cybersecurity. In this chapter, we will discuss the many elements that have an impact on security behavior, as well as the behavior theories that are most often used in the field of cybersecurity. The chapter comes to a close with a discussion of cybersecurity education, training, and understanding (SETA) programs as well as a discussion of the necessity for research. Researchers in the subject of cybersecurity have been expanding their work. The majority of the time, when individuals think about cybersecurity, they do it from the perspective of engineers and computer scientists. The vast majority of research projects pertaining to cybersecurity have focused on the technical aspects of the field. An important aspect of this is identifying possible dangers and determining how to prevent them. Threats to cybersecurity may manifest itself in a variety of ways, such as malicious software, distributed denial of service attacks (DDoS), and unauthorized computer access. A multitude of technical security solutions, including as intrusion detection prevention systems (IDPS), firewalls, anti-malware applications, and encryption, are suggested in the research literature as potential countermeasures to this issue. The use of a personal identification number (PIN) or pattern for authentication, screen locks, automatic updates, remote tracking, wiping, and a locking function are all examples of security measures that may be found on smartphones. These precautions are meant to prevent malware from infecting the device. This article will go over a lot of the precautions that are provided by mobile phones.* Authentication method: A smartphone users may choose to use authentication mechanisms such as PIN/password, pattern or biometric to secure their phone against unauthorized access. Users of smartphones can choose the right method of authentication for their setting of their phone.

METHODS AND MODELS

Over the course of the years, a number of suggestions calling for IP traceback have been put up in an effort to avoid or minimize specific types of online risk. As was covered in Chapter 2, a number of the currently available IP traceback methods, including Probabilistic Packet Marking (PPM), Deterministic Flow Marking (DFM), and others, have deficiencies that restrict their use in actual situations. The IP traceback technique has not been successful in producing a workable solution because of problems with its implementation. SMITE, which stands for SDN and MPLS Integrated Traceback Mechanism, is an innovative method for IP traceback that incorporates SDN and MPLS services into OpenFlow. If the source address of a communication is either wrong or fake, it is still possible to correctly track the origin of the message using this method. Because of the adaptability and strength of software-defined networking (SDN), SMITE has created a revolutionary IP traceback solution that is compatible with the SDN framework. This

approach is based on MPLS. The unified control architecture of software-defined networking (SDN) may be leveraged in a number of different ways when MPLS is used for IP traceback in SDN. Due to the fact that the control plane and the data plane are often located in close proximity to one another in networks, it is rather difficult to make changes to the sending policy once it has been specified. If you want to make the required modifications, you will need to visit the settings menus of every switch and router that is affected by the issue.

Because of the amount of time and effort that is necessary, the expansion of the network is hampered. Given the dynamic nature of MPLS label creation and encoding on moving packets, the adaptability of software-defined networking (SDN) has the potential to significantly enhance the functioning of SMITE. Furthermore, in addition to researching MPLS, we also studied the idea of delivering the traceback data using a Virtual Local Area Network (VLAN). However, there are a great deal more advantages to using MPLS as opposed to VLAN. There are around four thousand different virtual local area networks (VLANs) that may be individually recognized by the 12-bit VLAN ID. This ID can take on values ranging from zero to forty-ninety-five (with a few being designated for particular uses). There is a VLAN tag field in the Ethernet header that is two bytes long, and that is where the VLAN ID is stored. 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.

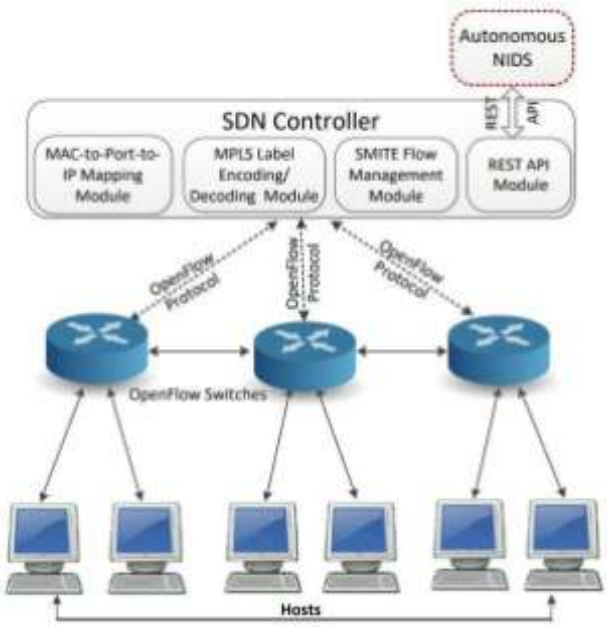

Figure 3.1: SMITE Architecture

The feature selection module is an interesting component of the process of constructing a successful prediction model. It accelerates machine learning, reduces complexity, and prevents overfitting while simultaneously improving

performance. It is possible to see in Figure 3.7 that the Feature Selection Module makes use of three different methods. In the first approach, the Best Feature Selection module makes use of a number of different feature selection techniques in order to extract the most valuable features from Allfeatures. These strategies include the Filter method, the Wrapper method, and the Embedded method. In this section, we are able to see how the Best Feature Selection tool prioritized the available characteristics after doing an evaluation of all of them. PCA, which stands for principal component analysis, is the second approach that the feature selection tool employs. Using its assistance, it is much simpler to discover the relationship between hundreds of different characteristics. Principal component analysis (PCA) increases program performance by minimizing the number of dimensions, which in turn reduces the amount of training that is required via the process.

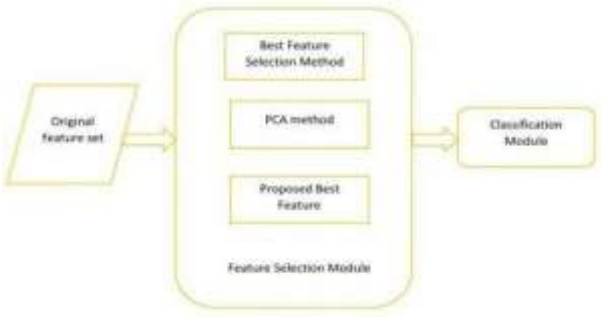

Figure 3.7: Feature selection module

EXPERIMENTS & RESULTS

The I-SMITE, which stands for the Inter-Autonomous Systems SDN and MPLS Integrated Traceback Mechanism, is presented in this chapter. A system that is based on SMITE and provides traceback across inter-Autonomous Systems (AS) is what we mean when we talk about software-defined networking (SDN). In the first version of SMITE, an Intra-AS IP traceback technique was introduced for one of the SDN-based AS services. In order to reach the destination, an MPLS label is used to transmit the source IP address. On the other hand, I- SMITE may provide IP traceback capabilities for communication both inside and across associated systems. A combination of the SDN architecture, which is comprised of the Ryu controller and the OpenFlow protocol, and the Border Gateway Protocol (BGP) is used in order to carry out inter-AS IP traceback services. Among the protocols that are used for Internet routing, BGP is considered to be the gold standard. It serves as the backbone protocol for logical routing operations and global connections so that they may function properly. It is possible for different computers on the Internet to learn how to connect with one another and share routing information thanks to the Border Gateway Protocol (BGP). I-SMITE takes use of a particular transitive feature of BGP that is optional in order to guarantee that information on I-SMITE is sent to the appropriate BGP speakers. This is performed even in the event that some intermediate BGP speakers do not support it. BGP was chosen as the Inter-AS protocol because it does not need any new hardware and it is simple to incorporate into the network that is already in place. In addition, BGP makes it possible to make a progressive transition from a traditional network to an SDN network. This is preferable to the alternative of deploying OpenFlow all at once, which is a risky move. When it comes to the transmission of data between controllers in a software-defined network (SDN), there are no multi- domain standards either. For this reason, it is required to choose and correctly install an Internet-level multi-domain communication protocol, such as the Boarder Gateway Protocol (BGP), in order to be able to offer an Inter-AS IP traceback mechanism.

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].
[3]. Available: https://www.gov.uk/government/ statistics/cyber- security-breaches-survey-2020/cyber-securitybreaches-survey- 2020 (visited on 11/03/2020) (page 1).
[4]. 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).
[5]. 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).
[6]. 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).
[7]. Y. Xiang, K. Li, and W. Zhou, “Low-rate DDoS attacks detection and traceback by using new information metrics,”
[8]. IEEE Transactions on Information Forensics and Security, vol.
[9]. 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).
[10]. V. M. Igure and R. D. Williams, “Taxonomies of attacks and vulnerabilities in computer systems,” IEEE
[11]. Communications Surveys Tutorials, vol. 10, no. 1, pp. 6– 19, 2008. doi: 10.1109/COMST.2008.4483667 (page 3).
[12]. 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.
[13]. N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, “OpenFlow:
[14]. Enabling innovation in campus networks,” ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69–74, 2008 (pages 6, 11, 27, 44, 59).
[15]. 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).
[16]. 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).
[17]. 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 (page 6).