A Taxonomy of Cyber-attacks on Computer Networks

Ali Sajid

A Taxonomy of Cyber-attacks on Computer Networks

Sajid Ali
Faculty of Engineering and Informatics
University of Bradford
Bradford, UK
Sali173@bradford.ac.uk

***Abstract* — Computer networks in the current state of the world have become an inevitability all around the world ever since it was put in motion. It has constantly gained users within businesses and organisations, and the users will tend to increase as more technology is invented. We need computer networks day-by-day, as it uses different computers within the same network to share files, resources and significant data. It is used within businesses and schools or could be part of the network which may be connected to the internet. When computer networks start growing as a whole, then the chances of cyber-attacks also starts to increase and the attack can happen when it is least expected. This is due to the fact that solutions aren't as effective as such. For example, resources, tools and framework cannot detect cyber-attacks that affect the organisation, before the attack is carried out [1]. Alongside this, when there is a large number of users on a specific network, then the network can become slow as it is sharing resources with more users, which could eventually lead it to shut down.**

***Keywords—*Cybersecurity, computer networks, cyber attacks, information security.**

I. INTRODUCTION

As studies have taught us, there is a high demand for technologies that are used for computer networks within the interaction and business industries. A lot of cyber-attacks have occurred where businesses, as well as individuals, have made a great loss. There are a lot of cyber-attacks out there, but a few are known as denial-of-service (DoS), Man in the Middle (MitM), Cross-site Scripting (XSS), and etc. [2]. Attacks tend to happen due to the vulnerability of the system, but as the system learns about the different attacks, it classifies it and learns it for the future. The classification file is called a taxonomy which embraces a variety of consequences such as digital harm, physical or psychological harm, reputational harm, and societal harm [3]. Assailants will also use the above attacks in order to steal sensitive information such as identities, to sell on the dark web for other crimes to be committed by different assailants [4]. This journal will contain the different types of cyber-attacks, how they are carried out, and ways of preventing it for future use. Also, this journal with finish with a conclusion to conclude the effects that cybercrimes have.

II. TAXONOMY OF CYBER-ATTACKS

In 2018, over 9 billion records were accessed and tampered with by hackers [7]. Hackers will hack anything that benefits them in some way to either gain money or something else that will benefit them in the future. Some of the types will be explained below such DDoS, Man in the middle and etc. it is helpful to know what the types of attacks are and how they can be prevented to the maximum possible ability [7].

A. DDoS Attack

Around 28,700 different attacks happen daily around the world, which is just under 2000 attacks an hour [9]. In order for a DDoS attack to be established, the assailant must create a connection and gain control of the oppositions system for the attack to be successful. The way DDoS attacks work is, malware is sent to the oppositions system and installed, which in turns blinds the individual computer from seeing anything and turns it into a robot, which means the computer is unable to do anything [6]. This is also known as bots, and once the assailant has turned a group of PC's into bots then it is known as a botnet. After botnet has been achieved, this is how the attacker knows that the attack is becoming successful. As soon as the botnet stage has been created, the assailant will be able to send traffic to the user's computer remotely through the IP address by the use of bots and at this stage, it is very difficult to realise which part of the traffic is normal or harmful. Within this, bots will randomly send traffic to the server of the chosen IP address causing it to process more than it can handle which will eventually shut down due to it over flooding. This is called the denial of service because the attacker is literally denying the service to legitimate traffic [10].

B. Man in the Middle Attack

Man in the Middle attacks is a great threat to businesses as well as organisations because, in 2018, 35% of exploitation activity happened as attackers were using man in the middle attacks [12]. A Man in the Middle is a very devious attack that intercepts the communication between two parties by placing himself in the middle to imitate to the other user, making it look like the messages are being sent and received as normal. The main aim of this attack is to thieve personal information and sensitive data such as login credentials, account details, credit card numbers and etc. this type of attack usually takes place with e-commerce websites that look fraudulent [8]. Most of the time, Man in the Middle attacks are hard to notice as there is hardly any evidence to tell that anyone is spoofing. Identity theft is the highest possible chance of happening, alongside financial theft and unauthorised password change, but there are many purposes alongside this, as each individual attacker has his own intentions [11]. In different terms, Man in the Middle is like someone opening up your mail which contains your bank statement to copy your bank details and financial information [13].

C. Cross-site Scripting Attack (XSS)

An example of an XSS attack could be, if a hacker was to send a victim a suspicious or unorthodox email containing code that the victim cannot account for and is clicked on, then a chain of custody could be introduced and would lead to a misleading web-page for harmful reasons [15]. In basic terms, cross-site scripting is when the assailant/hacker places harmful and malicious code into a defenceless website or send it within emails to gullible victims. Within this, the users are targeted before and can have devastating consequences, which may be at the mercy of the attacker [14]. If successful, data could be modified, account details can be bypassed and gullible users can evasively give private data. In conjunction with this, cookies can be penetrated to imitate valid users and abuse the data that they're most protective of. There are two types of cross-site scripting which are known as stored and reflective, stored cross-site scripting (persistent XSS) is more dangerous than the two as it places harmful code directly into the webpage. On the other hand, the reflected script uses the link rather than the content to inject malicious code and harm can only occur once clicked on [16].

D. Drive-by attack

IBM states that the time frame to detecting a breach within 2019 is 206 days [18]. This is because cyber attackers tend to look for sites that are insecure and is easy for it to insert malware. As this is a method used by many attackers to insert malware, it is inserted into the HTTP or PHP part of the webpage [17]. When the site is visited, the malware within the code could be automatically downloaded or can direct the user to another site that is controlled by the assailants that directed the victim. Drive-by attacks can happen in ordinary places like emails and website which makes it least expected. With this being said, the assailant doesn’t have to depend on the user to do anything in order to take control of his/her computer, this is very rare and most cyber-attacks can’t do what drive-by attacks can [19]. If the victim doesn’t have to depend on the user to do anything, then the victim doesn’t have to click or do anything in order to become infected, which means advantage can be taken of apps and operating systems or even web browsers that haven’t had successful updates. There are many ways to be protected from drive-by attacks but the main ways are to keep everything updated [21].

E. Password attack

Throughout 2019, there has been a breach of 5.3 billion records due to password attacks which took home addresses, phone numbers, credit cards number and etc. [22]. Passwords are used for nearly everything we own digitally, so for hackers to obtain passwords is their primary goal which is most likely effective for them. Some of the time, victims could leave passwords lying around on desks in which the attacker will sniff around. The attacker will use other means such as social engineering, password databases or basic guessing to obtain unencrypted passwords, which can either be done at random or systematically [20]. There are two ways of obtaining passwords which are Brute Force and dictionary attack. A Brute Force attack means trying random passwords differently and guessing that one will work. This uses a trial and error method and utilises passwords that are affiliated with the user such as the users name, address, job title and etc. in dictionary attacks, this method uses passwords that have already been utilised by a password database that has been gained unlawfully, this also uses a trial and error method that guesses passwords from the database.

III. Requirements for taxonomy

When using a taxonomy, the system will need to know which sector of the data is to be recorded and how similar or different the samplings are to be figured out. When creating a taxonomy, there are certain requirements that need to be achieved in order for the taxonomy to be successful and for it to be universally accepted [23]. Also to make a new taxonomy, previous taxonomies need to be researched and understood fully before moving on. The requirements are, as follows [25]:

- Accepted – which means that methods are used from previous work that is well accepted.

- Mutually exclusive – when detection of several attacks has occurred, it is fit into one classification, rather than overlapping with another sector.

- Comprehensible – this means, that it can be understood by computer scientist and anyone a little less educated.

- Complete/exhaustive – the categories that are already available have to be complete and thorough within each group and is assumed to be complete.

- Unambiguous – this means that the classification has to be precise of what attack belongs to the classification without a doubt.

- Repeatable – this should be repeatable.

- Terms well defined – the categories that belong to the taxonomy should be defined really well and precise terminology so the system understands and be within the laws of security.

- Useful – it is used to gain awareness into a specific field of study in which the interest lies within the field of study.

IV. Attack Taxonomies

One form of taxonomy that was proposed from the Computer Emergency Response Team (CERT) for cyber intrusions by Kjaerland [27]. This type of system focuses more on user profiling to capture the cybercriminals and victims. Within this taxonomy, attacks were used using facet theory and multidimensional scaling (MDS) with the method of Operation, target, source and impact. This means that it checks the similarity levels of individual cases [35] and the systematic approach to coordinating theory and research [36]. Each feature contains a certain number of elements with a thorough explanation. The creator used these features to compare the commercial side against the government side. Kjaerland's method focuses more on user behaviour and figures out what their intentions are to find out why and how the attacks take place, and where the attack would take place from [26]. Like others, this method also contains dis-advantages which is that it has a high-level view of the taxonomy of operations which doesn't include a further description to the methods that can be used in recognising the foundation of the attack.

Another taxonomy was proposed, where the method could use four unique dimensions that provide an all-inclusive group by covering network and computer attacks which were created by Hansman and Hunt [29]. Their type of taxonomy gives help in improving computer and network security, moreover, it uses regularity in language with an explanation of the attack. An attack vector is the first part of the method that is used to put the attack in a group, the second part of the method puts the target in a group. The third dimension states the vulnerability classification number and the final dimension highlights the effects that are involved within the attack. In each dimension of the taxonomy, there is a detailed description provided of the attack, which is a disadvantage within their method [28]. A final disadvantage to this method is that it doesn't provide enough information, which doesn't allow to capture information in protecting a system from attacks.

Mirkovic and Reihner [30] proposed a taxonomy that deals with Distributed Denial of Service otherwise known as DDoS attacks and defence tools used in order to put the attacks in groups and various defence strategies involved. This specific method gives an overview of the features and attacks strategies that are used within the method. Strategies are an important factor as a defence mechanism. This method uses a degree of automation, exploited weaknesses, source address validity, attack rate dynamics, the possibility of characterisation, persistent agent set, victim type, and impact on the victim which is used to classify the DDoS attacks. The creators also created a defence which provides activity level, cooperation degree, and deployment location. The grouping that is used within this method is used to group DDoS attacks and defence within a method provides a form of communication between researchers to discuss solutions.

Validation Exposure Random Deallocation Improper Conditions Taxonomy otherwise known as VERDICT is a more focused taxonomy that is used on attacks that were created by Daniel Lough [32]. There are four parts that this method focuses on, which are shown as security errors. These are improper validation, improper randomness, improper exposure, and improper deallocation. These four types are easy to notice as they are labelled with improper, which means that the attacks are within an improper environment. When validating attacks within this taxonomy, it can be done incorrectly or with biased data, this also embraces physical security [31]. The improper exposure, which is the second part to the taxonomy, which can be used to expose attack directly or indirectly depending on its vulnerability. The third part which is randomness deals with the cryptography of the attack and in inconsistent use of randomness involved. The final part is improper deallocations which refer to the inaccurate demolition of data, or residuals of data, which also include dumpster diving. There is more than one way within this taxonomy that can explain the vulnerability within the method. A disadvantage to this method could be that it doesn't have the grouping of the types of attacks such as virus, Trojans and etc.

A final taxonomy that can be provided is a taxonomy that groups attacks based on events, which could be an attack that may be successful that is heading towards a target that can end up changing the result in a state. In order to work out the event, the action of the attack is needed as well as the target. The creator includes all the phases in the detection of the attack and how the attack grows. Within this taxonomy, to use event management, the creator included five steps that an attacker must do in order for the method to receive a result. The chosen phrases are tools, vulnerability, action, target, and unauthorised result [34]. The first part of the taxonomy refers to the tools that are used in order to carry out the attack, the second part is vulnerability which used to define the type of exposed mechanism used to carry out the attack. The third part is an action which shows the method used to carry out the attack, the fourth and fifth part of the taxonomy is the intention the attack is attempting to damage and the unauthorised result in the aftermath of the attack that has left it vulnerable. One disadvantage for this is that it doesn't provide enough of a report of the attack that has been performed [33].

V. CONCLUSION

To conclude this journal, the taxonomy of cyber-attacks on computer networks has been explained to the maximum. In the introduction, the different cyber-attacks have been explained briefly alongside the different type of taxonomies which are also known as existing systems, different cyber-attacks and another type of taxonomy which explains the damages caused to users after the attack has been carried out. After this the different types of cyber-attacks were explained in more detail such as DDoS attacks, password attacks and etc. when creating a taxonomy, there are certain requirements which have to be met in order for anyone with knowledge of taxonomies can understand was understood and written after the cyber-attacks but before the attack taxonomies. Attack taxonomies are basically methods or existing systems that are used in order to detect and deal with attacks, but mainly to classify them into different groups that can be dealt with at the next phase. There are different taxonomies which were explained, some attacks are detected by events and some by human behaviours and the list goes on. To finish, computer networks are becoming more secure day-by-day from cyber-attacks using taxonomies.

REFERENCES

[1] Agrafiotis, I., Nurse, J., Goldsmith, M., Creese, S. and Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity, 4(1).

[2] Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, 28, pp.24-31.

[3] I. Ghafir, V. Prenosil, and M. Hammoudeh, “Botnet Command and Control Traffic Detection Challenges: A Correlation-based Solution.” International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 7(2), pp. 27-31, 2017.

[4] Ignatuschtschenko, E., Roberts, T. and Cornish, P. (2016). Cyber Harm: Concepts, Taxonomy and Measurement. SSRN Electronic Journal.

[5] Bluefin. (2019). Cyber Attacks In 2018: Biggest Cyber Security Data Breaches of 2018. [online] Available at: https://www.bluefin.com/bluefin-news/cyber-attacks-biggest-breaches-2018/ [Accessed 16 Dec. 2019].

[6] I. Ghafir, J. Svoboda and V. Prenosil, “Tor-based malware and Tor connection detection,” International Conference on Frontiers of Communications, Networks and Applications. Kuala Lumpur, Malaysia, pp. 1-6, 2014.

[7] Rapid7. (2019). Common Types of Cybersecurity Attacks and Hacking Techniques. [online] Available at: https://www.rapid7.com/fundamentals/types-of-attacks/ [Accessed 16 Dec. 2019].

[8] J. Svoboda, I. Ghafir, V. Prenosil, “Network Monitoring Approaches: An Overview,” International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 5(2), pp. 88-93, 2015.

[9] Reo, J. (2019). Academic Research Reports Nearly 30,000 DoS Attacks per Day. [online] Neptune Web, Inc. Available at: https://www.corero.com/blog/853-academic-research-reports-nearly-30000-dos-attacks-per-day.html [Accessed 16 Dec. 2019].

[10] Mahjabin, T., Xiao, Y., Sun, G. and Jiang, W. (2017). A survey of a distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks, 13(12), p.155014771774146.

[11] I. Ghafir and V. Prenosil, "DNS query failure and algorithmically generated domain-flux detection," International Conference on Frontiers of Communications, Networks and Applications. Kuala Lumpur, Malaysia, pp. 1-5, 2014.

[12] Swinhoe, D. (2019). What is a man-in-the-middle attack? How MitM attacks work and how to prevent them. [online] CSO Online. Available at: https://www.csoonline.com/article/3340117/what-is-a-man-in-the-middle-attack-how-mitm-attacks-work-and-how-to-prevent-them.html [Accessed 16 Dec. 2019].

[13] Conti, M., Dragoni, N. and Lesyk, V. (2016). A Survey of Man In The Middle Attacks. IEEE Communications Surveys & Tutorials, 18(3), pp.2027-2051.

[14] I. Ghafir and V. Prenosil, "Malicious File Hash Detection and Drive-by Download Attacks," International Conference on Computer and Communication Technologies, series Advances in Intelligent Systems and Computing. Hyderabad: Springer, vol. 379, pp. 661-669, 2016.

[15] Veracode. (2019). Cross-Site Scripting (XSS) Tutorial: Learn About XSS Vulnerabilities, Injections and How to Prevent Attacks. [online] Available at: https://www.veracode.com/security/xss [Accessed 16 Dec. 2019].

[16] Fogie, S., Grossman, J., Hansen, R., Rager, A. and Petkov, P. (2014). XSS Attacks. Burlington: Elsevier Science.

[17] I. Ghafir, M. Husak and V. Prenosil, "A Survey on Intrusion Detection and Prevention Systems," IEEE/UREL conference, Zvule, Czech Republic, pp. 10-14, 2014.

[18] Inside Out Security. (2019). 110 Must-Know Cybersecurity Statistics for 2020 | Varonis. [online] Available at: https://www.varonis.com/blog/cybersecurity-statistics/ [Accessed 16 Dec. 2019].

[19] U. Raza, J. Lomax, I. Ghafir, R. Kharel and B. Whiteside, "An IoT and Business Processes Based Approach for the Monitoring and Control of High Value-Added Manufacturing Processes," International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, 2017.

[20] I. Ghafir and V. Prenosil. "Proposed Approach for Targeted Attacks Detection," Advanced Computer and Communication Engineering Technology, Lecture Notes in Electrical Engineering. Phuket: Springer International Publishing, vol. 362, pp. 73-80, 9, 2016.

[21] Simmonds, M. (2016). Beware the drive-by attack. Computer Fraud & Security, 2016(10), pp.19-20.

[22] SelfKey. (2019). All Data Breaches in 2019 - An Alarming Timeline - SelfKey. [online] Available at: https://selfkey.org/data-breaches-in-2019/ [Accessed 16 Dec. 2019].

[23] I. Ghafir, J. Svoboda, V. Prenosil, "A Survey on Botnet Command and Control Traffic Detection," International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 5(2), pp. 75-80, 2015.

[24] Design of Password Guessing Prevention Protocol for Levelled-Security System. (2018). HELIX, 8(5), pp.3787-3791.

[25] Hansman, S. and Hunt, R. (2005). A taxonomy of network and computer attacks. Computers & Security, 24(1), pp.31-43.

[26] I. Ghafir, V. Prenosil, M. Hammoudeh, F. J. Aparicio-Navarro, K. Rabie and A. Jabban, "Disguised Executable Files in Spear-Phishing Emails: Detecting the Point of Entry in Advanced Persistent Threat." International Conference on Future Networks and Distributed Systems. Amman, Jordan, 2018.

[27] Kjaerland, M., "A taxonomy and comparison of computer securityincidents from the commercial and government sectors". Computers and Security, 25:522–538, October 2005.

[28] I. Ghafir, V. Prenosil, M. Hammoudeh and U. Raza, "Malicious SSL Certificate Detection: A Step Towards Advanced Persistent Threat Defence," International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, 2017.

[29] Hansman, S., Hunt R., "A taxonomy of network and computer attacks". Computer and Security (2005).

[30] Mirkovic, J., and Reiher, P. "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. In ACM CCR (April 2004)

[31] I. Ghafir and V. Prenosil, "Advanced Persistent Threat and Spear Phishing Emails." International Conference Distance Learning, Simulation and Communication. Brno, Czech Republic, pp. 34-41, 2015.

[32] Lough, Daniel. "A Taxonomy of Computer Attacks with Applications to Wireless Networks," PhD thesis, Virginia Polytechnic Institute and State University, 2001.

[33] Howard, John D. and Longstaff, Thomas A. "A Common Language for Computer Security Incidents," Technical report, Sandia National Laboratories, 1998.

[34] I. Ghafir, V. Prenosil, M. Hammoudeh, T. Baker, S. Jabbar, S. Khalid and S. Jaf, "BotDet: A System for Real Time Botnet Command and Control Traffic Detection," IEEE Access (IF=4.098), vol. 6, pp. 1-12, 2018.

[35] Carlson, J. (2017). Unidimensional Vertical Scaling in Multidimensional Space. ETS Research Report Series, 2017(1), pp.1-28.

[36] Levy, S. (2014). Facet Theory. Encyclopedia of Quality of Life and Well-Being Research, pp.2112-2119.