Survey on Network Security Threats and Attacks

Amit Kumar and **Santosh Malhotra**

kamit5@iitk.ac.in, mahotsan@iitk.ac.in

Department of Computer Science and Engineering

Indian Institute of Technology Kanpur

Kanpur, Uttar Pradesh 208016, India

1. INTRODUCTION

In a brave new age of global connectivity and e-commerce, interconnections via networks have heightened, creating for both individuals and organizations, a state of complete dependence upon vulnerable systems for storage and transfer of information. Never before, have so many people had power in their own hands. The power to deface websites, access personal mail accounts, and worse more the potential to bring down entire governments, and financial corporation's through openly documented software codes. This paper discusses the possible exploits on typical network components; it will cite real life scenarios, and causes. At the end of this paper conclusion is provided to guide contributors for the development of more security measures to prevent network attacks.

2. RELATED WORK

Network security threats have been studied extensively by the research community. Network Attacks can be also classified [1,2,3] as a) Passive attack b) Active attack c) Distributed attack d) Insider attack and e) Close-in attack. Attacks can be also on the infrastructure level such as on the cloud [4] DDoS [5, 6, 7], or routers [8]. In [4], author addressed the importance of network attacks at the cloud level and some key mitigation techniques. He explained that many attacks can still cause great harm to Cloud Computing, impacting all the important security aspects (confidentiality, integrity, isolation, availability, etc.). Among those attacks, the DoS and DDoS attacks are arguably the easiest to mount and the most destructive, yet huge gaps still exist to efficiently deal with those attacks. DDoS attacks were studied extensively by the research community [5, 6, 7]. Ahmad Sanmorino [5] has proposed a pattern of matching detection technique that overcome the drawbacks of the other detection techniques of the DDoS attacks. Traffic flows through the network is checked based on the specified pattern and can easily find that packet is malicious or not. This technique of detection has an advantage of lower cost of infrastructure since it only uses routers and switches which exist already. It does not use high technology resources such as multicore CPU technology. This paper shows three topological environment which consists of 3 phases. In the 1st environment normal behavior of the traffic was shown, In the second phase unsecured network with attacks launched on it was shown. In the third phase handling of the attack was shown with firewall and successful dropout the packets.

In [6] Adrien Bonguet and Martine Bellaiche presented some state-of-the-art solutions: some were rather easy to incorporate in existing Cloud infrastructures for Cloud providers to prevent or reduce DoS and DDoS attacks and in [7], they shown that there are various detection and mitigation mechanisms to prevent the network from various kinds of DDoS attacks, also they gives a survey about various kinds of DDoS attacks and how to handle them. It helps to give a basic idea of the techniques to the reader who wants to get started his research work from network security. In [8] Kamal Ahmat and Ammar Elnour discussed threats at the packet level and introduced a simple yet effective method to overcome this issue.

PyungKoo [9] has studied that pseudo states in the router are one of the best method to protect the services. As routers, switches and other devices on the network are not much capable to differentiate between all the packets so the service oriented based detection mechanism using pseudo state (SDM-P) is used to counter the attack packets before it falls into the network. A Hash key algorithm is used to evaluate the performance of this detection scheme. In other techniques the attack is detected when the services accommodation gets down, but proposed technique is used for the detection before entering the data packets. The implementation has done on the NS-2 platform to identify the difference between the packets whether it is legitimate packet out the attacker's packet.

Saman Taghavi [10] has presented about DDOS flooding attack as it is one of the challenging issue to prevent the network security. In this type of attack an armies are set up to launch an attack. Various computers are hired by an attacker, it is called botnets or Zombies, the coordinated attack is performed by all the hired computers. The appropriate defense mechanism is required to bar the DDOS flooding attacks. The purpose of this paper is to seek about DDOS flooding trouble and the various steps to encounter it. The Study is about the consideration of previous counter steps to handle the DDOS Flooding attacks. The main consideration of this paper is to give the survey of traditional and current handling mechanism which helps the research community to develop their DDOS flooding handling problem when or after attack launched. IlkerOzcelik [11] has presented about the detection approach on Denial of Services. The detection is based on the anomaly based metrics. The Cumulative Sum (Custom) approach has applied to detect the effect of the attack on the network. This algorithm is performing at high and low bandwidth of the network. The main purpose of this work is to show the better detection results with the custom algorithm as it reduces the utilization of the network. This whole work was performed by using the background traffic in the paper's scenario.

3. NETWORK SECURITY THREAT MODELS

Network security refers to activities designed to protect a network. These activities ensure usability, reliability, and safety of a business network infrastructure and data. Effectual network security focuses on a variety of threats and hinders them from penetrating or spreading into the network. Figure 1 shows some of the typical cyber attack models.

The most common threats include:

- Trojan horses and spyware (spy programs)
- DOS (Denial of service attacks)
- Data interception and theft

Network Attacks can be also classified [1,2,3] as a) Passive attack b) Active attack c) Distributed attack d) Insider attack and e) Close-in attack. Passive Attacks: This type of attack makes use of information from the system but not affect system resources. The attacker can observe the data or information transmitted between the sender and receiver. This data can include usernames, passwords and confidential e-mail messages. Passive attacks result in the disclosure of information or data files to an attacker without the knowledge of the user. Passive attack threatens the confidentiality of the system, and is difficult to detect because it gets the required information without altering the system resources. Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords.

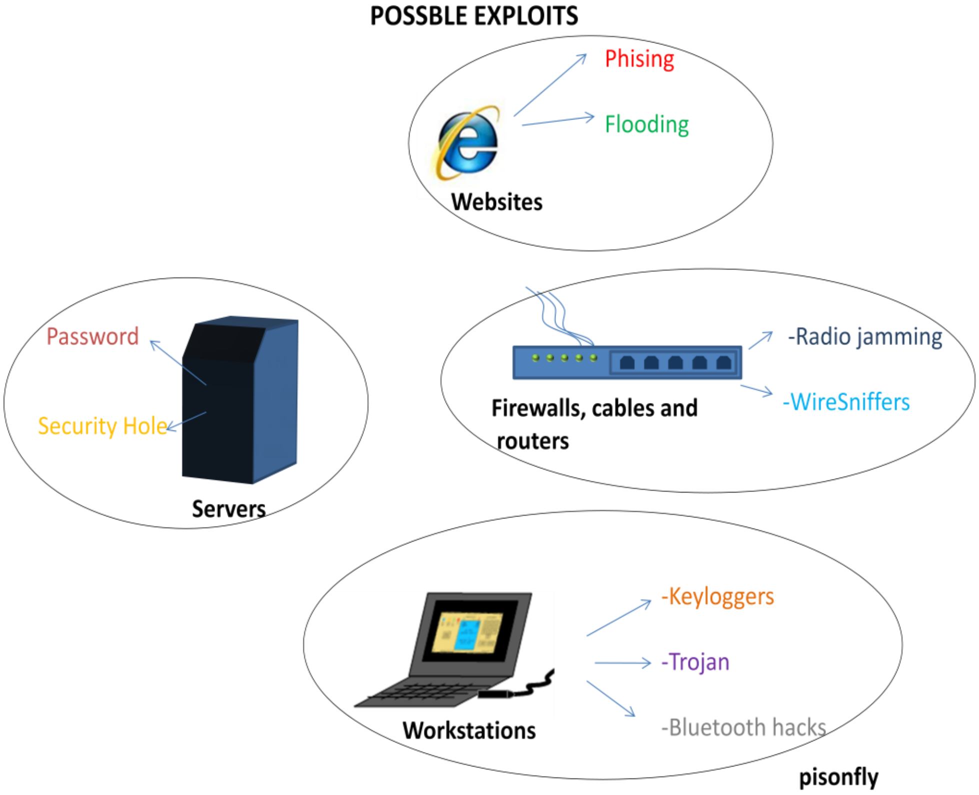

Figure 1: Common Cyber Attack Models

a. FLOODING

In 1998, an American elite group, “The Digital Disturbance Theater”' came up with Floodnet, an application set to halt the Mexican president’s webpage (for political reasons). Floodnet is a java applet that automates the “refresh” button to click repeatedly. Sufficient users online would run the application and hence cause the site’s server to continuously refresh until saturation and thus halt and disable the webpage. An attacker has used similar applications to take into hostage commercial websites in exchange for ransom. It is advisable for an organization to have for emergency, a savvy security expert (White-hat hacker); seeing that web technology is dynamic, with the ever changing trends in web scripting languages and browser configurations.

b. KEYLOGERS

These are simple software codes that exploit what we call ‘hooks’ on a computer’s kernel. Hooks capture vital hardware traffic like Keystrokes and mouse movements. Software based Key loggers are programmed to capture any button stroke you type on the keyboard and save words as a text file. That includes all private information you type like Passwords, Google searches, Credit card number, emails, to name but a few. Regularly updating of the Antivirus is a sure way to beat this. Let it also be known that Hardware key loggers exist, masquerading as flash disks. USB password applications should deter such.

c. TROJANS

An experienced programmer is capable of creating a Trojan, a concealed application that runs in the background. A Trojan allows a hacker to become a ghost user on your PC/Workstation. They monitor when your computer is online to deliver captured keystroke log files to their preferred address. Hackers can always come back and upload a malicious code via the Trojan. Such a code maybe the one that kills your antivirus program after which, it takes your snap via webcam or taps into your office conversations from your laptop microphone. Trojans come tucked away neatly on pirated software and the so-called cracks we all like to use. As the adage goes, it is difficult to cheat an honest person. The converse is true for those who would escape this pitfall. Let them invest in genuine software.

d. BLUETOOTH

Bluetooth is emerging as a versatile networking technology connecting workstations to printers, smart phones etc. I see potential for mischief; where data could be wirelessly intercepted for malicious use. Such technology is currently non-existent, to the best of my knowledge, but nonetheless, a practical possibility.

e. PHISING

This is when emails appearing to come from well known organizations pop up on your browser, sending you links and requesting for private information like credit card numbers, account passwords or congratulating you for winning. Watch out for that nice email from a website you do not even have an account with.

Look-alike websites are also not uncommon. They will have you login and ‘refill’ your personal details; after which they can make online purchases under your name or if they be diabolical enough, they will lock you out of your own account. (I lost my yahoo account that way).

Numerous cyber security forums and workshops exist where one can always learn ways to have an edge over scammers and keep your business team informed

f. RADIO JAMMING

This can be a rare DOS (Denial of Service) technique to disrupt information flow in a wireless router network, accomplished by use of noise-generating radio devices. However, special Equipment exist, that can be used to track anonymous radio-noise sources, should interference be detected.

g. WIRE SNIFFERS

Attackers can always insert wire sniffing hardware at cable junctions. It should always be ensured that cable terminals and switch boards are always locked & access be granted only to authorized personnel.

h. COMPROMISED SERVERS

An exploited server is a server that is not entirely under your power. Someone else will have gained control of your server, using it for their own motives. Use of a Weak password is often one way a hacker will gain access to your server by guessing your password. People tend to use simple passwords to keep them memorable. Such include dates, lover/pet names, office surrounding etc. Caution must therefore be exercised by combining letters with numerals to create a simple yet strong password.

i. SERVER SECURITY HOLES

Server Security can be compromised via security holes in a web application like addons/plugins such as joomla / wordpress. It is advisable to use only secure connections whenever possible. This includes the use of SSL connections for email, and SFTP (Secure File transfer Protocol) instead of the more common but unsecure FTP protocol.

j. ZERO DAY/HOUR ATTACK

Take this for example. The ‘sticky keys’ feature (sethc.exe) on your XP or Windows7 OS. It is a good accessibility feature that allows one to press special keys only once at a time. This application runs on the logon window when you press shift key five times even before you’ve entered your password. One only needs to rename the command prompt shell (cmd.exe) to sethc.exe on a logged-in computer. By this, they will have gained full control of your laptop or workspace computer anytime later without passing through any known account. How? By simply pressing the shit key five times and *voila*, the command prompt! Try this for yourself (Hope they got that patched on Windows 8).

Zero hour/day attacks take advantage software vulnerabilities that are yet to catch the eye of a software manufacturer. Should you discover such a bug, report to the software company for a patch to make up for the bug in later releases. Otherwise a hacker may discover the same loophole later, and use it maliciously.

4. CONCLUSION

In conclusion, a dedicated network security organ is vital for protecting infrastructures. If you have good network security, your company or organization is protected against interruption, employees remain productive. Network security helps you meet compulsory regulatory compliance. Protecting your client's data means no lawsuits emanating from cases about data theft.

Components of the dedicated security organ include:

- A constantly updated Anti-virus software.
- A Firewall, that blocks unauthorized access to workstation PCs (USB ports, LAN, WIFI).
- Virtual Private Networks (VPNs), to give secure remote admission.

5. REFERENCES

[1] http://technet.microsoft.com
[2] Classification of attacks. http://computernetworkingnotes.com
[3] Threats and countermeasures. http://msdn.microsoft.com
[4] Kamal Ahmat "Emerging Cloud Computing Security Threats" in arxiv.org/1512.01701
[5] Ahmad Sanmorino, and Setiadi Yazid. "DDos attack detection method and mitigation using pattern of the flow." International Conference of. IEEE, 2013.

[6] Adrien Bonguet, Martine Bellaiche. A Survey of Denial of Service and Distributed Denial of Service and Defence in Cloud Computing, Future Internet. 2017; 9(43).

[7] Sakshi kakkar, and Dinesh kumar in "A Survey on Distributed Denial of Services (DDOS)" in International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014

[8] Kamal Ahmat, and Ammar Elnour "Towards Effective Integrated Access Control Lists in Internet Networks" in the 2012 International Conference on Security and Management (SAM'12), Las Vegas, USA, July 16 – 19, 2012.

[9] PyungKoo Park, SeongMin Yoo, Chungnam Nat, Service-Oriented DDoS Detection Mechanism Using Pseudo State in a Flow Router , 2013 International Conference on Information Science and Applications (ICISA)

[10] Saman Taghavi Zargar, Joshi, Member, IEEE, and David Tipper,A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, ACCEPTED FOR PUBLICATION (2013)

[11] Ilker Ozcelik, Yu Fu , Richard R. Brooks ,DoS Detection is Easier Now, 2013 Second GENI Research and Educational Experiment Workshop.

[12] A. Alvare, "How Crackers Crack Passwords or What Passwords to Avoid", Proceedings, UNIX Security Workshop II, August 1990.

[13] R. Bace, R., and P. Mell, “Intrusion Detection Systems”, NIST Special Publication SP 800-31, November 2000.

[14] D. A. Applegate, G. Calinescu, D. S. Johnson, H. Karloff, K. Ligett, and J.Wang, “Compressing rectilinear pictures and minimizing access control lists”, in Proc. ACM-SIAM SODA, Jan. 2007, pp. 1066–1075.

[15] Liu, Alex X., Chad R. Meiners, and Eric Torng. "TCAM Razor: A Systematic Approach Towards Minimizing Packet Classifiers in TCAMs", IEEE/ACM TRANSACTIONS ON NETWORKING 18.2 (2010).