CYBER SECURITY TECHNIQUES FOR VARIOUS CYBER ATTACKS

Rashmi B H
Assistant Professor
Department of Computer Science & Engineering
Global Academy of Technology, INDIA

Abstract: Cyber-Security is becoming most critical capability for the defense and protection of our society. Under this Cyber security, Cyber-crime is one of the most happening and fast growing event under various categories of crime. The main impact of Cyber-crime is that it is costing our global economy for more than $445 billion USD per year. Take anything, say smallest company to wide government organizations or say Educational institutions would be having great amount of Intellectual and Confidential information or data being lost due to the impact Cyber-Security. Basically, this loss is due to some intruders or some malicious agents being introduced into the network knowingly or unknowingly. Organizations or Institutions should gear up now and should start defending against these Cyber-attacks by adapting certain Cyber Security techniques and strategies in order to maintain the Integrity and Confidentiality of the Data.

IndexTerms **- Cyber-Attacks, Cyber Security Techniques, Sniffing, Malwares, Eavesdropping, Firewalls.**

I. INTRODUCTION

The field of Cyber Security is gaining more importance because of increase in technologies used over Internet such as Bluetooth, WI-FI or any other Smart devices. The major systems like Organizations, Educational Institutions, Financial systems, Aviation, Government organizations, Automobile Industries and Heath care systems. Threat is increasing as the uses of technologies are used over internet. But there is a saying that "Technology is not the problem….People are the problem." from the outsight of this saying, most important task is to change People's mind. But bringing these changes is a complex task towards the protection of society. The initial section of this paper focuses on various types of Cyber-attacks, the institution or Organization is facing and the latter section focuses on the various Cyber Security techniques in order to protect the civil society from Cyber-crime and threat. The main strategies to be followed in order to protect the civil society from Cyber-attacks or threats are to form a goal and certain metrics to avoid threats entering the network. A legal rules and regulations should be maintained in order to support the system. People should be educated regarding the on goings inside the network, which they are operating in. Last but not the least R & D Investment should be done.

2. CYBER-SECURITY ATTACKS

The Cyber-attack is an offensive action which targets computer systems present in various organizations or institutions to steal the confidential data or to destroy computer hardware or software. The following are the various types of Cyber-attacks.

- Denial-of- service (DoS) and Distributed Denial-of-Service (DDoS) attacks.
- Man in the Middle Attack.
- Phishing and Spear phishing attacks.
- Drive-by-attack.
- Password attack.
- Cross-site Scripting (XSS) attack
- Eavesdropping attack.
- Birthday attack
- Malware attack.

Denial-of-Service and Distributed Denial-of-Service attacks: A denial-of-service attack overwhelms a system's resources by not responding to service requests. A DDoS attack is also an attack on system's resources, which is launched from a large number of host machines that are infected by malicious agents or viruses controlled by the attacker as shown in the Figure 2.1.

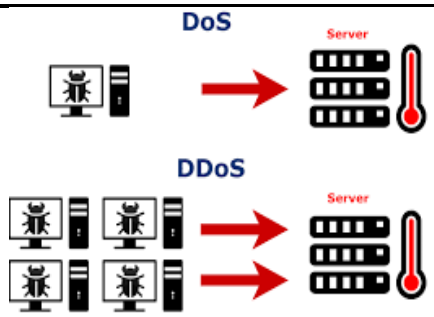

Figure 2.1: DoS and DDoS Attack.

There are different types of DoS and DDoS attacks namely TCP SYN Flood attack, smurf attack, ping-of-death attack and various Botnets.

Man-in-the Middle Attack: A Man-in-the-middle attack occurs when a hacker itself becomes a communicator between the communications of a client and a server. One of the most common type of Man-in-the middle attack is Session Hijacking as shown in the Figure 2.2. It is a type of Man-in-the-middle attack where a session is hijacked between a client and network server. The attacking agent substitutes its IP address for the trusted client while the server continues the session, believing it is communicating with the client without being aware of the session hijacked

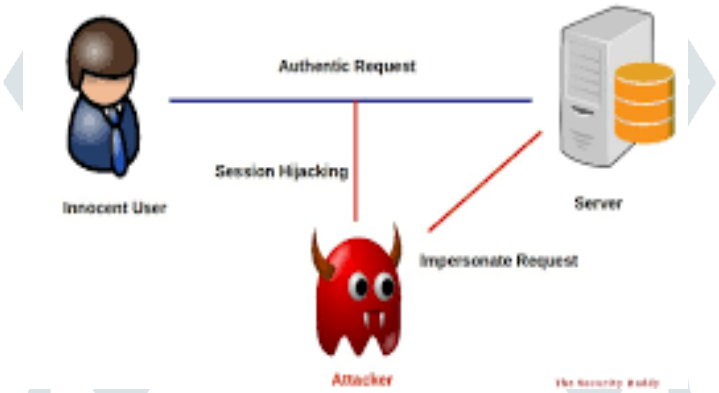

Figure 2.2: Session Hijacking

Phishing and Spear phishing attacks: Phishing attack is one of the Cyber-attack which indulges in to the practice of sending emails, which are portrayed as trusted one, with the intention of stealing personal information of the users or motivating users to do unusual activities in the social networking field. A malware will be loaded into the computer system as an Email attachment, which in turn could lead the user to download malwares or any unusual things like personal information.

Spear phishing is a type of phishing attack which can't be identified easily and cannot be defended against many types of attacks. Most common example of Spear phishing attack is Email Spoofing, which is a process of falsifying the mails, as if it appears as the mail received from the person whom the user knows.

Drive-by-attack: These are the types of Cyber attacks where malwares are downloaded into the system and is spread across the entire system. Hackers will be looking for an insecure file or a website, if found these hackers will implant or install a malicious agent into the computer system. Basically Drive-by-attacks can happen when the user tries to visit any insecure pages or any blocked pop-up-window pages. A drive-by-attack takes the advantage of an app, operating system or web browser that contains security flaws due to unsuccessful updates or due to malicious agents present inside the network. Drive-by attack doesn't rely on Users to launch any types of attack into the system as shown in the Figure 2.3.

In order to overcome this type of Cyber attack, users should keep their browsers and operating systems updated and also see to it that systems do not contain any malicious agents and not many plug-ins should be installed in order to avoid Vulnerabilities.

Figure 2.3: Drive-by Attack

Password Attack: Passwords are the most common type of authentication mechanism to authorize and authenticate users to computer systems. The major part of concern is that how safe is our Passwords. Passwords can be easily detected by a process called "Sniffing", where in it is a connection to computer system to acquire unencrypted Passwords by using Social Engineering technologies or gaining access to password database. Brute Force and Dictionary attack are the most common types of Password attack. Brute force attack is the one where in Passwords can be guessed randomly by trying out various combinations or applying various logic related to user name, title etc. Dictionary attack is the type of attack where dictionary of common passwords is used to gain access to computer system.

In order to safeguard the computer system from Brute force or Dictionary attack, an account lockout policy should be implemented that will lock the account after invalid password attempts.

Cross-site Scripting (XSS) attack: These are the types of Cyber attacks which use third-party web resources to run scripts into victim's web browser or application. When the attacker discovers a website for having an XSS Script, the attacker injects a malicious database to steal cookies. This database will be provided to user, and the user executes these malicious scripts, and sends these cookies to the attacker. To defend against these scripting attacks, data should be validated and filtered before reflecting the data back to the user.

Eavesdropping attack: Eavesdropping attacks occur through the disturbance caused in network traffic. This is a type of Cyber attack, wherein the attacker can obtain passwords, credit card numbers and other confidential information of the user, who would be sending over the network as shown in the Figure 2.4. There are two types of Eavesdropping namely

- Passive eavesdropping.
- Active eavesdropping.

Data Encryption is the best method to counter strike Eavesdropping.

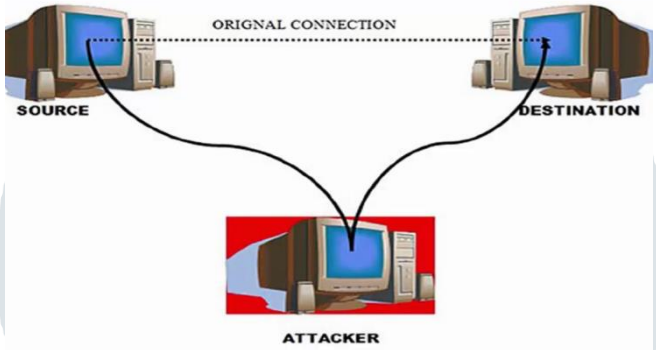

Figure 2.4: Eavesdropping Attack.

Birthday Attack: Birthday attack is the type of Cyber attack which is used against hash algorithms to verify the integrity and confidentiality of a message, software or digital signatures. The message generated using hash function produces a Message Digest. This message digest is of Fixed length. This cyber attack is the probability of finding two random messages which consists of fixed length message digest obtained from hash function. If an attacker replaces the user's message with his message and calculates same Message digest, the receiver will not be able to detect the replaced message even after comparing several Message digest.

Malware Attacks: Certain malicious software or unwanted software which is installed in the system without the user consent is said to propagate this type of attack which attaches itself to legitimate code and replaces the good applications with the damaged one or replicates the applications across the internet. Most common types of malwares as shown in the figure 2.5 are as follows:

- Macro Viruses.
- File infectors.
- Polymorphic Viruses.
- Stealth Viruses.
- Trojans.
- Worms.
- Ransom wares.

Figure 2.5: Malware Attacks

3. CYBER SECURITY TECHNIQUES

The following are the techniques to measure Cyber security

- **Access Control and Password Security:** Measures should be taken to properly authorize and authenticate data, so that there is no place for intruder to gain access to confidential data. Passwords must be made secured to avoid a Sniffing attack. Measures should be taken up to create a account lockup system, where in account will be closed, if the attacker is trying to use random passwords to gain access to confidential information.

- **Malware Scanners:** Measures should be taken to install Malware scanners in computer system to protect the system from various viruses, Ransomwares and Trojans. These scanners scan the entire incoming and outgoing network traffic and prevent malicious agents or software's entering the network thus preventing various Cyber attacks.

- **Firewalls:** Firewalls are the backbone of network security, as it monitors incoming and outgoing traffic and prevents all the unusual malicious agents entering the network at Router or Gateway level. Measures should be taken to install enterprise level Firewalls to carry out Deep inspection method to prevent certain threats entering the network.

- **Anti-Virus Software:** Anti-virus software is also known as Anti-malware, is a computer program used to detect and prevent malwares. The advantages of using these anti- virus malwares is that it provides protection against the installation of malware software on a computer and also used for the detection and removal of malwares which are already installed on the Computer system.

CONCLUSION

Cyber attacks are increasing as the new technologies are evolving. As we can see that attackers have many options like DoS attacks, Malware Infections, man-in-the middle attacks, brute force password attacks to gain unauthorized access to critical or confidential information. Measures to mitigate these threats should be taken up with the same security basics. Systems and anti-virus databases should be kept up to date, and training should be given to users to configure firewall to white list only the specific ports and hosts needed for business use. Passwords must be kept strong and ensure that there is a continuous audit of IT systems to detect suspicious activity.

REFERENCES

[1] Youngsoo Kim,ikkyun Kim,Namje park,(2014),” Analysis of Cyber attacks and Security Intelligence”, *James J. (Jong Hyuk) Park et al. (eds.), Mobile, Ubiquitous, and Intelligent Computing*, pg 489-494.

[2] Haydar Teymourlouei, *International Scholarly and Scientific Research & Innovation 9(3) 2015*,” Cyber Attacks Awareness and Prevention Method for Home Users”,pg 678-684.

[3] Fabio Pasqualetti,, Florian Dörfler, Francesco Bullo,” Attack Detection and Identification in Cyber-Physical Systems”, *IEEE transactions on automatic control, vol. 58, no. 11, November 2013*,pg2715-2729.

[4] Kutub Thakur , Meikang Qiu , Keke Gai , Md Liakat Ali4,” An Investigation on Cyber Security Threats and Security Models”, *Conference: Conference: 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing (CSCloud 2015).*