International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 12 Issue 2, February-2023, Impact Factor: 7.957

A Survey on Different Threats of Network and Its Security Mechanism

C. Nagarani

Assistant Professor, Department of Computer Science, PSG College of Arts and Science, Coimbatore

ABSTRACT

Security is a fundamental component in computing and networking technology. Generally, the security configuration of a computer is dictated by specifying the policies of the security controls in the network. Network security has become very important for personal computer users, companies and the military. With the advent of the internet, security has become a major concern. Network security is given more importance due to the intellectual property that is easily accessible through the internet. There are different kinds of attacks that can be sent across the network. By knowing the attack methods, allows the appropriate security to emerge. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide and all of these require different kinds of security mechanisms. In this paper, we are trying to study different kinds of attacks along with various different kinds of security mechanisms that can be applied according to the need and architecture of the network.

Keywords: Network security, attacks, hackers,cloud-environment security.

INTRODUCTION

Network security includes accepted policies and practices to prevent and monitor unauthorized access, misuse, modification, or denial of computer networks and network-accessible resources. Network security includes authorization to access data on the network, which is controlled by the network administrator. Users choose or assign an ID and password or other authentication information that allows them to access information and programs within their authority. A home or small office may only require basic security while large businesses may require high maintenance and advanced software and hardware to prevent malicious attacks from hackers and spamming[1]. New Threats Demand New Strategies as the network is the door to your organization for both legitimate users and would-be attackers. For years, IT professionals have built barriers to prevent any unauthorized entry that could compromise the organization's network. The network security is constantly evolving, due to traffic growth, usage trends and the ever changing threat landscape [3]. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password. According to the UK Government, Information security is:" the practice of ensuring information is only read, heard, changed, broadcast and otherwise used by people who have the right to do so"(Source: UK Online for Business). Information systems need to be secure if they areto be reliable. The vast topic of network security is analyzedby researching the following

History of security in networks.

- Types of internet attacks and security methods.
- Internet architecture and vulnerable securityaspects of the Internet.
- Security for networks with internet access.
- Current development in network security hardwareand software.

A possible hacker could target the communication channel, obtain the data, decrypt it and re-insert a false message. Hence, securing the network is just as important as securing the computers and encrypting the message which we want tokeep private. When developing a secure network, the following need to be considered[1].

- **Accessibility -**authorized users are provided the means to communicate to and from a particular network.
- **Confidentiality-** information in the network remains private, disclosure should not be easily possible.
- **Authentication-**to verify the identity of a person ora device.
- **Integrity-** ensure the message has not been modified in transit, the content must be the same asthey are sent.
- **Non-repudiation-** ensure the user does not refute that he used the network.

TYPES OF NETWORK THREATS

Threats provided by the network are generally of two basic types:

Passive Network Threats:
Functions such as wiretapping and passive scan designed to intercept traffic traveling through the network.

Active Network Threats:
Activities such as service denial (DoS) attacks and SQL injection attacks attempt to execute attacker commands to disrupt the normal functioning of the network. In order to make a successful network attack, attackers usually need to seriously disable a company's infrastructure, which allows them to remotely execute commands on internal operating systems using software vulnerabilities.

Dark Net:
Dark net is that the a part of the web below the private deep web that uses custom software and hidden networks superimposed on the architecture of the web "Dark Net" was first associated with the Door Network, when the infamous drug bazaar Silk Road was once the headline. Anonymous communication between whistle-blowers, journalists and news organizations is additionally facilitated by the "Darknet" Tor network through use of applications like Secure Drop.

TECHNOLOGIES TO PROVIDE SECURITYTO THE NETWORK:

Internet threats will continue to be a major issue in the global world as long as information is accessible and transferred across the internet. Different defense mechanisms are developed to deal with this crisis. Some of the mechanisms along with advanced concepts are mentioned below.

Cryptography Systems:
Cryptography is a useful and widely used tool in security engineering today. It involves the use of codes and ciphers to transform information into unintelligible data.

Anti-Malware Software and Scanner:
Anti-malware is a type of software programdesigned to prevent, detect, and remove malicious software (malware) on ID systems, as well as personal computer devices. It protects against infections caused by many types of viruses, as well as rootkits, ransomware and spyware. It uses three strategies to protect systems from malicious software, including signature-based malware detection, behavior-based malware detection and sandboxing.These techniques protect against threats from malware in a variety of ways.

Intrusion Detection System:
An intrusion detection system (IDS) is an additional security measure that helps prevent computer intrusion. IDS systems are used to monitor connections in determining whether attacks have been launched. Some IDS systems monitor and alert the attack, while others try to prevent the attack. A typical antivirus software product is an example of an intrusion detection system. Infiltration detection in corporate and government networks is a fast-growing field of security research; This development was triggered by the realization that recording and auditing data were not being used effectively by many systems.

Firewall:
A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal Network and untrusted external network, such as the Internet. Firewalls are often classified as network firewalls or host-based firewalls. Network firewalls run on network hardware that filters traffic between two or more networks. Host based firewalls run in host computers and control network traffic in and out of those machines. Firewalls can be implemented in both hardware and software, or combination of both[2].

Dynamic Endpoint Modeling:
It is a newly emerging technology that provides an additional layer of control system network cyber security. Dynamic endpoint modeling learns the behavior of all devices in the network and triggers alerts when models detect changes in learned behavior.

VPN:
VPN provides a means to protect data while it travels over an untrusted network. VPN is intended for employee use of organization-owned computer systems only. All kinds of remote access to corporate networks should be routed via VPN with a valid corporate-approval, standard operating system along withappropriate security patches. Access

to company computers from home via the Internet should not be allowed. To protect the network when using a VPN for remote user access, the Security Administrator should ensure that adequate security is implemented at the endpoints by using L2TP with IPSec. Also, VPN vendors include a firewalling function in their client to filter traffic.

ENCRYPTION OF VIRUSES

An encrypted virus is a computer virus that encrypts its payload with the intention of making the virus more difficult to detect. However, since encryption requires an encryption or a key, an encrypt can be used as an antivirus detection method.

Cookies:
Cookies are messages that web servers pass to your web browser when you visit internet sites. Your browser stores each message in a small file called cookie.txt. When you request another page from the server, your browser sends the cookie back to the server. Cookies in themselves are harmless. They are just data stored by a website in your browser, and they are not malware. It is what sites do with them that determine whether we like them or not. Some cookies are essential to use a site properly and others might be considered a privacy risk. Identity theft is the illegal use of someone else's personal information in order to obtain money or credit. Identity theft can happen to anyone at any location across the globe.

Identity Theft:
Identity theft is the illegal use of someone else's personal information to obtain money or credit. Identity theft can happen to anyone anywhere in the country.
Steps to protect online identity:

- Locking your computer and cell phone usingpasswords.
- Not sharing specific personal information online,such as your full name or birthday.
- Setting proper privacy settings on socialnetworking sites.

CYBER SECURITY

Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security.

Cyber security is the practice of protecting systems, networks, and programs from digital attacks. These cyber attacks are usually aimed at assessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

Implementing effective cyber security measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

DATA ENCRYPTION

Data encryption is a security method where information is encoded and can only be accessed or decrypted by a user with the correct encryption key. Encrypted data, also known as cipher text, appears scrambled or unreadable to a person or entity accessing without permission.

Data Encryption is used to deter malicious or negligent parties from accessing sensitive data. An important line of defence in cyber security architecture, encryption makes using intercepted data as difficult as possible. It can be applied to all kinds of data protection needs ranging from classified government Intel to personal credit card transactions. Data encryption software, also known as an encryption algorithm or cipher, is used to develop an encryption scheme which theoretically can only be broken with large amounts of computing power.

DATA SYNCHRONIZATION

Data synchronization ensures accurate, secure, compliant data and successful team and customer experiences. It assures congruence between each source of data and its different endpoints. As data comes in, it is cleaned, checked for errors, duplication, and consistency before being put to use. Local synchronization involves devices and computers that are next to each other, while remote synchronization takes place over a mobile network. Data must always be consistent throughout the data record. If data is modified in any way, changes must upgrade through every system in real-time to avoid mistakes, preventprivacy breaches, and ensure that the most up-to-date data isthe

only information available. Data synchronization ensures that all records are consistent, all the time.

THE PROCESS OF AUTHENTICATION

Authentication is the process of determining whether someone or something is, in fact, who or what it declares itself to be. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server. Authentication is important because it enables organizations to keep their networks secure by permitting only authenticated users (or processes) to access its protected resources, which may include computer systems, networks, databases, websites and other network-based applications or services.

Once authenticated, a user or process is usually subjected to an authorization process as well, to determine whether the authenticated entity should be permitted access to aprotected resource or system. A user can be authenticated but fail to be given access to a resource if that user was not granted permission to access it. The terms authentication and authorization are often used interchangeably; while they may often be implemented together the two functions are distinct. While authentication is the process of validating theidentity of a registered user before allowing access to the protected resource, authorization is the process of validating that the authenticated user has been granted permission to access the requested resources. The process by which access to those resources is restricted to a certain number of users is called access control. The authentication process always comes before the authorization process.

BOTS AND CYBER SECURITY

Bots are ones of the most popular consumer technology trends in the industry. From chat bots to digital assistants, bots are an important enabler for user-computer interactions. As a result, bots have been increasingly becoming the target of cyber-security attacks. As a new technology trend, many of the attacks and malicious techniques in bot technologies are relatively unknown to cyber-security platforms.

Considering that bots rely on mechanisms such as natural language and voice interactions as the fundamental user interface mechanism, they pose some serious security challenges to users in ways we haven't seen before. As a result, many of the traditional cyber-security protection techniques need to be adapted to the bot world. In order to be efficient in the bot space, cyber-security platforms will have to address some of the following challenges.

By leveraging natural language processing techniques, attacks on bots can exhibit an almost infinite combination of behavior that is conducive to the same malicious result. That characteristic contrasts with the rather predictable behavior of most malware code.

Impact In The Physical World:
Boots that attack technologies such as digital assistants can have an immediate impact in the physical world. Imagine a bot that can infect Amazon Echo devices with malicious code to start altering sensors or home-devices connected to the assistant.

SOME ADVANCE NETWORK SECURITY POLICIES

Making Security In Cloud Environment: The increase in investment in IT fields is largely attributed to cloud computing to cloud[10]. Over half of IT organizations plan to increase their spending on cloud computing to improve flexible and efficient use of their IT resources. Intel Trusted Execution Technology(Intel TXT) is specifically designed to harden platforms against hypervisor, firmware, BIOS and system level attacks in virtual and cloud environments . It does so by providing a mechanism that enforces integrity checks on these pieces of software at launch time. This ensures the software has not been altered from its known state. This TXT also provides the platform level trust information that higher level security applications require to enforce role-based security policies. IntelTXT enforces control through measurement, memory locking and sealing secrets.

Zero-Trust SegmentationAdoption:
This model was initially developed by John Kindervag of Forrester Research and popularized as a necessary evolution of traditional overlay security models. One alternative that is a strong candidate to improve the security situation is the zero-trust model (ZTM). This aggressive approach to network security monitors every piece of data possible under the assumption that every file is a potential threat. It requires that all resources be accessed in a secure manner, that access control be in a need-to-know basis and strictly enforced. The systems verify and never trust; that alltraffic be inspected, logged, and reviewed and that systems be designed from the inside out instead of the outside in. It simplifies how information security is conceptualized by assuming there are no longer trusted interfaces, applications traffic, network or users. It takes the old model trust but verified and inverts it, because recent breaches have proved that when an organization trusts, it doesn't verify.

Advanced Threat Protection With Big Data- Big data makes big sense for security as it involves using specialized technologies and techniques to collect, coordinate, store and analyze truly massive amounts of related and perhaps even disparate data to uncover insights and patterns that would otherwise remain obscured. Leveraging Big Data for information security purposes not only makes sense but is necessary. Big Data analytics can be leveraged to improve information security and situational awareness. For example, Big Data analytics can be employed to analyze financial transactions, log files, network traffic to identify anomalies and suspicious activities, and to correlate multiple sources of information into a coherent view.

Data-driven information security dates back to bank fraud detection and anomaly-based intrusion detection systems. Fraud detection is one of the most visible uses of Big Data analytics. Credit card companies have conducted fraud detection for decades . However, the custom-built infrastructure to mind Big Data for fraud detection was not economical to adapt for other fraud detection uses. Off-the -shelf Big Data tools and techniques are now bringing attention to analytics for fraud detection in healthcare, insurance, and other fields.

CONCLUSION

Security is a very difficult and vital topic. Everyone has a different idea regarding security policies, and what levels of risk are acceptable. The key for building a secure network is to define what security means to your need of time and use. Once that has been defined, everything that goes on with the network can be evaluated with respect to that policy. It is important to build systems and networks in such a way that the user is not constantly reminded of the security system around him but users who find security policies and systems too restrictive will find ways around them.

There are different kinds of attacks on the security policies and also growing with the advancement and the growing use of the interneta. In this paper we saw different threats to our network system. As the threats are increasing, for the secure use of our systems and internet there are various different security policies developing. In this paper we have mentioned a few security policies that can be used easily and some advanced qualities that fit today's penetrating environments. Cyber security is a shared responsibility, and it boils down to this: in cyber security, the more systems we secure the more secure we all are.

REFERENCES

[1]. Dr. Sandeep Tayal, Dr. Nipin Gupta, "A Review paper on Network Security and Cryptography", Advances in Computational Sciences and Technology, ISSN 0973-6107 Volume 10-2017.
[2]. Marin, G.A., "Network security basics," Security & Privacy, IEEE , vol.3, no.6, - 2005
[3]. Adeyinka, O., "Internet Attack Methods and Internet Security Technology," Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on, vol., no., pp.77-82, 13-15 May 2008
[4]. F. S. Roozbahani and R. Azad, "Security Solutions against Computer Networks Threats," Int. J, pp. 2576–2581, 2015.
[5]. S. Kaushik and A. Singhal, "Network Security Using Cryptographic Techniques," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 2, no. 12, pp. 2277–128, 2012