IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

NETWORKING ATTACK THREATS

[1]A.Sindhu Devi [2] Dr.K.P.Kaliyamurthie

[1] Student ,Department of CSE, BIHER, Chennai.

[2] Professor , Department of CSE, BIHER, Chennai.

ABSTRACT

When computer was introduced it was used only to save and access data and to perform calculations faster than human. After the connection of computers sending messages became very popular. Sending messages was done internally within a building. Then came into emerge the concept of World Wide Web (WWW) which made the people across the world to connect between themselves and interact from any parts of the world. This process of connecting the computers is called networking. In this article we are going to discuss about various network threats.

Keywords: WWW, TCP/IP , P2P, MALWARE,PHISHING

1. INTRODUCTION

Computer Networking is the practice of connecting computers together to enable communication and data exchange between them. In general, Computer Network is a collection of two or more computers. It helps users to communicate more easily.

1.2 Scope of the Paper:

This paper is mainly used for dealing with the networking concepts and the threats of network and the methods to eradicate the threats.

2. COMPUTER NETWORK

2.1.NETWORK CONCEPT

A computer network is a group of interconnected nodes or computing devices that exchange data and resources with each other. A network connection between these devices can be established using cable or wireless media. Once a connection is established, communication protocols -- such as TCP/IP, Simple Mail Transfer Protocol and Hypertext Transfer Protocol -- are used to exchange data between the networked devices.

The first example of a computer network was the Advanced Research Projects Agency Network. This packet-switched network was created in the late 1960s by ARPA, a U.S. Department of Defense agency.

A computer network can be as small as two laptops connected through an Ethernet cable or as complex as the internet, which is a global system of computer networks.

2.2 HOW COMPUTER NETWORK WORKS

Devices attached to a computer network use IP addresses that are resolved into hostnames through a domain name system server to communicate with each other over the internet and on other computer networks. A variety of protocols and algorithms are also used to specify the transmission of data among endpoints.

Network systems must follow certain standards or guidelines to operate. Standards are a set of data communication rules required for the exchange of information between devices and are developed by various standards organizations, including IEEE, the International Organization for Standardization and the American National Standards Institute. For example, the Ethernet standard establishes a common communication language for wired or physical networks, and the 802.11 standard specifies connectivity for wireless local area networks (WLANs).

A computer network must be physically and logically designed in such a way that makes it possible for the underlying network elements to communicate with each other. This layout of a computer network is known as the computer network architecture.

2.3 COMPUTER NETWORK ARCHITECTURES

The following are the two most common computer network architectures:

1. Client-server. This model consists of many clients -- or nodes -- where at least one network node acts as the central server. The clients in this model don't share resources, but request the central server, as all the resources are installed on it.

2. Peer-to-peer (P2P). Each connected device on this network behaves as the client, as well as the server, and enjoys similar privileges. The resources of each peer are shared among the entire network, including memory,

processing power and printing. Many companies use the P2P architecture to host memory-intensive applications, such as three-dimensional rendering, across multiple network devices.

3. CORE COMPONENTS OF A COMPUTER NETWORK

The following building blocks -- network devices, links and communication protocols -- make computer network operations possible:

Network devices. These physical devices or nodes are the data communication equipment that is connected inside a computer network. Examples of network devices include modems, routers, PCs, servers, firewalls, switches and gateways. Each device in a computer network is identified by a network address and often has easily identifiable hostnames.

Links. A link is the transmission medium used for connecting the nodes and enabling them to transmit to each other. The links can be either wired, wireless or optical, such as an Ethernet cable or a Wi-Fi signal. The links can be configured in different ways, both physically and logically, and the network topology dictates the manner in which links and nodes relate to each other.

Communication protocols. These are the rules or protocols that all nodes on a network must follow for information transfer. Common protocols include the TCP/IP suite, IEEE 802, Ethernet, WLAN and cellular standards.

3.1 TCP/IP MODEL :

TCP/IP is a conceptual model that suggests the following four functional layers for these communication links:

Network access layer. This layer defines how the data is physically transferred through the network, as well as how hardware devices send bits through a network medium, such as coaxial, optical, fiber or twisted-pair cables.

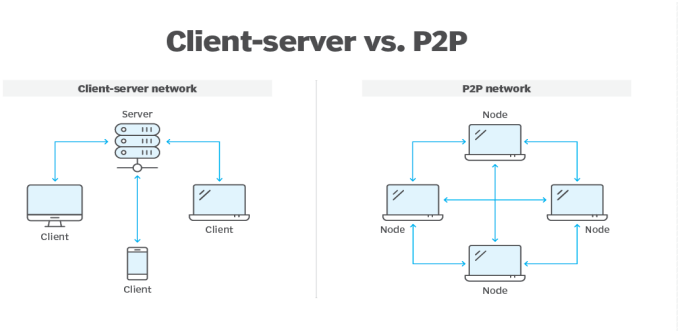
Internet layer. This is the layer where routing takes place. It packages data into packets and enables them to be sent and received over the network. The internet layer includes IP, Address Resolution Protocol and Internet Control Message Protocol.

Transport layer. This layer ensures the stable, sequenced and error-free delivery of data packets. It achieves this by swapping acknowledgment of data reception and retransmitting lost or dropped packets. Typical protocols used at the transport layer include TCP and User Datagram Protocol.

Application layer. Security protocols, such as Transport Layer Security, operate at this layer and play an integral part in ensuring network security. This is the abstraction layer that communicates directly with applications and defines how high-level apps should access the network to start a data transfer. For example, the application layer is used to define where, when and how much data should be sent at a specific rate.

The modern internet architecture is mostly built on the TCP/IP model, which is the simplified version of the more conceptual Open Systems Interconnection model.

4. FLOWCHART DIAGRAM



5. Advantages of using a computer network

Computer networks are ideal for the quick exchange of information and the efficient use of resources.

The following are benefits of using a computer network:

1. Resource sharing. Enterprises of all sizes can use a computer network to share resources and critical assets. Resources for sharing can include printers, files, scanners and photocopy machines. Computer networks are especially beneficial for larger and globally spread-out organizations, as they can use a single common network to connect with their employees.

2. Flexibility. Today's computer networks enable people to use flexible communication and resource-sharing methods based on their needs and preferences. For example, some people might use email or instant messaging to communicate, while others might prefer using an app such as WhatsApp.

3. Higher connectivity. Thanks to computer networks, people can stay connected regardless of their location. For example, video calling and document-sharing apps, such as Zoom and Google Docs, enable employees to connect and collaborate remotely.

4. Data security and management. In a computer network, data is centralized on shared servers. This helps network administrators to better manage and protect their company's critical data assets. They can perform regular data backups and enforce security measures, such as multifactor authentication, across all devices collectively.

5. Storage capacity. Most organizations scale over time and have an abundance of data that needs storage. Computer networks, especially those that employ cloud-based technologies, can store massive amounts of data and backups on a centralized remote server that's accessible to everyone, at any given time.

6. Entertainment. Computer networks, especially the internet, offer various sources of entertainment, ranging from computer games to streaming music and videos. Multiplayer games, for example, can only be operated through a local or home-based LAN or a wide area network (WAN), such as the internet.

6. COMPUTER SECURITY THREATS

Computer security threats are potential threats to your computer's efficient operation and performance. These could be harmless adware or dangerous trojan infection. As the world becomes more digital, computer security concerns are always developing. A threat in a computer system is a potential danger that could jeopardize your data security. At times, the damage is irreversible.

6.1 TYPES OF THREATS

A security threat is a threat that has the potential to harm computer systems and organizations. The cause could be physical, such as a computer containing sensitive information being stolen. It's also possible that the cause isn't physical, such as a viral attack.

1. Physical Threats: A physical danger to computer systems is a potential cause of an occurrence/event that could result in data loss or physical damage. It can be classified as:

- **Internal:** Short circuit, fire, non-stable supply of power, hardware failure due to excess humidity, etc. cause it.
- **External:** Disasters such as floods, earthquakes, landscapes, etc. cause it.
- **Human:** Destroying of infrastructure and/or hardware, thefts, disruption, and unintentional/intentional errors are among the threats.

2. Non-physical threats: A non-physical threat is a potential source of an incident that could result in:

- Hampering of the business operations that depend on computer systems.
- Sensitive – data or information loss
- Keeping track of other's computer system activities illegally.
- Hacking id & passwords of the users, etc.

The non-physical threads can be commonly caused by:

(i) Malware: Malware ("malicious software") is a type of computer program that infiltrates and damages systems without the users' knowledge. Malware tries to go unnoticed by either hiding or not letting the user know about its presence on the system. You may notice that your system is processing at a slower rate than usual.

(ii) Virus: It is a program that replicates itself and infects your computer's files and programs, rendering them inoperable. It is a type of malware that spreads by inserting a copy of itself into and becoming part of another program. It spreads with the help of software or documents. They are embedded with software and documents and then transferred from one computer to another using the network, a disk, file sharing, or infected e-mail. They usually appear as an executable file.

(iii) Spyware: Spyware is a type of computer program that tracks, records, and reports a user's activity (offline and online) without their permission for the purpose of profit or data theft. Spyware can be acquired from a variety of sources, including websites, instant chats, and emails. A user may also unwittingly obtain spyware by adopting a software program's End User License Agreement.

Adware is a sort of spyware that is primarily utilized by advertising. When you go online, it keeps track of your web browsing patterns in order to compile data on the types of websites you visit.

(iv) Worms: Computer worms are similar to viruses in that they replicate themselves and can inflict similar damage. Unlike viruses, which spread by infecting a host file, worms are freestanding programs that do not require a host program or human assistance to proliferate. Worms don't change programs; instead, they replicate themselves over and over. They just eat resources to make the system down.

(v) Trojan: A Trojan horse is malicious software that is disguised as a useful host program. When the host program is run, the Trojan performs a harmful/unwanted action. A Trojan horse, often known as a Trojan, is malicious malware or software that appears to be legal yet has the ability to take control of your computer. A Trojan is a computer program that is designed to disrupt, steal, or otherwise harm your data or network.

(vi) Denial Of Service Attacks: A Denial of Service attack is one in which an attacker tries to prohibit legitimate users from obtaining information or services. An attacker tries to make a system or network resource unavailable to its intended users in this attack. The web servers of large organizations such as banking, commerce, trading organizations, etc. are the victims.

(vii) Phishing: Phishing is a type of attack that is frequently used to obtain sensitive information from users, such as login credentials and credit card details. They deceive users into giving critical information, such as bank and credit card information, or access to personal accounts, by sending spam, malicious Web sites, email messages, and instant chats.

(viii) Key-Loggers: Keyloggers can monitor a user's computer activity in real-time. Keylogger is a program that runs in the background and records every keystroke made by a user, then sends the data to a hacker with the intent of stealing passwords and financial information.

6.2 How to make your system secure:

In order to keep your system data secure and safe, you should take the following measures:

1. Always keep a backup of your data.

2. Install firewall software and keep it updated every time.

3. Make use of strong and difficult to crack passwords (having capital & small alphabets, numbers, and special characters).

4. Install antivirus/ anti-spyware and keep it updated every time.

5. Timely scan your complete system.

6. Before installing any program, check whether it is safe to install it (using Antivirus Software).

7. Take extra caution when reading emails that contain attachments.

8. Always keep your system updated.

7. CONCLUSION

This paper is mainly used to discuss about the computer network systems and its security threats. In this paper we have a detailed discussion about the types and components of network and the types of threats and how to secure our system from the threats.

8. REFERENCES

1. P.C. van Oorschot, Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin (2021, 2/e; Springer). Personal use copy openly available on author's web site.

2. Wenliang Du, Computer Security: A Hands-on Approach (2017, self-published). Updated May 2019.

3. Stallings and Brown, Computer Security: Principles and Practice (2014, 3/e; Prentice Hall).

4. Dieter Gollmann, Computer Security (2011, 3/e; Wiley).

5. Smith, Elementary Information Security (2011, Jones & Bartlett Learning).

6. Mark Stamp, Information Security: Principles and Practice (2011, 2/e; Wiley).

7. Goodrich and Tamassia, Introduction to Computer Security (2010, Addison-Wesley).

8. Smith and Marchesini, The Craft of System Security (2007, Addison-Wesley).

9. Pfleeger and Pfleeger, Security in Computing (2007, 4/e; Prentice Hall).

10. Matt Bishop, Computer Security: Art and Science (2002, Addison-Wesley). Shorter version "omits much of the mathematical formalism": Introduction to Computer Security (2005, Addison-Wesley).