Computer Network

COMPUTER NETWORK, INTERNET AND INTRANET

Computer Network

A computer network is a set of one or more computers connected to share data and resources, like access to the Internet, file servers, printers, and many other types of information. This connection gives authorized users the ability to access information stored on other computers on the network. Computer networking has made many electronic human-to-human communications, electronic businesses, and even teleworking possible. Computers can be connected via cabling, most commonly the Ethernet cable, or wirelessly through radio waves.[1]

Internet

Although many people use the terms Internet and the World Wide Web interchangeably, they are not the same. The Internet is the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link devices worldwide. It is a network of networks that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The internet has a wide range of resources and services such as the applications of the World Wide Web (WWW), e-mail or peer-to-peer networks for file sharing. [1]

The Differences Between Internet and Intranet

Internet is a wide network of computers open for everyone; whereas, intranet is a local network of computers designed for a specific group of users. Internet in itself contains numerous amounts of intranets. [2]

TYPE OF NETWORKS

Client-Server Architecture

Client-server architecture is a network architecture consisting of clients and servers. Each computer or process is either a client or a server. Servers are powerful computers or processes. There are different types of servers, according to their function – e.g. managing disk drives (file servers), printers (print servers) or network traffics (network servers). Clients are either PCs or workstations on which users run applications. Clients rely on servers for resources, such as files, devices and even processing power. [3]

Peer-To-Peer Architecture

Another type of network architecture is the peer-to-peer architecture (peer-to-peer/P2P). Each workstation has equivalent capabilities and responsibility.[4]

Division by covered area

PAN, LAN, MAN, WAN are different network types. The 'N' in the end stands for network. [5]

PAN

„Personal Area Network” is a network covering a small (personal) area (e.g. a room). The most popular PANs are Bluetooth (wireless PAN), USB (wired PAN).

LAN

„Local Area Network” is a network covering a local area. The most common method is Wi-Fi (wireless LAN), although the wired LAN is still used. (Modern) wired or wireless LANs are based on Ethernet.

MAN

„Metropolitan Area Network” connects nodes located in the same metropolitan area – e.g. a company has different offices in one metropolitan area (for example Tokyo-Yokohama) and they are connected via a network.

WAN

„Wide Area Network” covers an area wider than LAN. The Range is not clear. It can reach from connecting belonging campus buildings up to satellite links connecting location in different countries. The most popular WAN is the Internet (it is basically a collection of other networks).

IP ADDRESS

IP address is the short form of Internet Protocol Address. It is something that is particular to a certain device logged onto a certain TCP/IP network. Static and dynamic are two forms of IP address, in which static as the name suggests never changes as you access the internet. Dynamic, however is temporary and hence changes upon each log in onto the network. [6]

IPv4

An IPv4 is a 32-bit number. IP address is divided into 4 sets of numbers, in which the separation between each set or octet is by dots. The decimal number in each octet ranges from 0 – 255. Example of n the binary form could be 192.23.22.21.[6]

IPv6 Implement

Whilst there are 4,294,967,296 available unique IPv4 addresses to be found from the rearrangement of the 32-bit numbers, eventually they will run out. Therefore, IPv6 addresses were created in order to accommodate more people since it has 128 bit numbers, which is far more than the 32-bit numbers offered by IPv4.[7]

Domain Address

Domain names/addresses essentially represent one or more IP addresses. They are used in URL's and particularly contain a suffix which belongs to a top-level domain, such as ".com". The example of domain could be www.google.com [8]

DNS

DNS stands for Domain Name System and it's a naming system for computers, services or any resource connected to the Internet or private network. For people in daily life we just think of it as a website address (www.facebook.com or www.lf1.cuni.cz). IP address stands for Internet Protocol address. To make it simple an IP address is the actual address to the Internet websites and the DNS are there to make it easier for people to find the websites. The DNS supports the lookup of IP addresses because it makes it easier for people to find the webpage their searching for, and they don't have to remember a long line of numbers. It's the connection between the domain name and the IP – address. [8]

MAC Address

MAC stands for 'media access control'. Every electrical equipment that can be connected to the network has a unique MAC address. MAC addresses are often assigned by the manufacturer of a computer and is a specific identity of the computer. The MAC address can be seen by the internet host[8]

COMMON INTERNET ATTACK METHODS

Eavesdropping

with this method, an unauthorized person can intercept communication which can cause sensitive information to be exposed. Passive eavesdropping is when the intruder only listens without interrupting to the networked messages. Active eavesdropping is when the intruder not only listens but also inserts something into the communication stream. With this the intruder, can gather important and restrict knowledge and information [9]

Viruses

A Virus is a self-replication program. It uses files to infect and insert itself into the system. If the operator open the infected file, the virus will be activated and start to interfere with the system function. [9]

Worms

Much like Viruses, the worm replicates itself. The difference between them is that a worm doesn't need a file to allow it the insertion into the system. There are 2 types of worms:

1. Mass-mailing worm – this type of worm uses e-mail as its way to infect other computers.

2. Network-aware worm – once this type of worm selects a target and gets an access to the host it can infect it with Trojan or other types of internet attack methods. The Network-aware worms are a great problem to the internet. Once a worm intrudes into the system it'll start to interfere with the system function. [9]

Trojans

Trojan appear to the user to be as a guileless and harmless program, but in fact it has negative effects on the system function. Most of the time Trojans accompanied with other infecting tools like viruses. [9]

Phishing

is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. [10]

IP Spoofing Attacks

The definition of spoofing is to show a familiar or friendly IP address to the victims so they will think that the package is coming from a trust worthy source; The intruder then gets access to other computers while keeping his identity covered. This sort of attack in the current way internet is being used, cannot be prevented. [9]

Denial of Service (DoS)

This sort of attack basically flooding the system with false requests which make it in an overload state. That leaves the system without the ability to deal with anymore requests which causes it to be without service. [10]

Cookies

Cookies are small files that are stored on the user's computer, designed to hold a small amount of data specific to a particular client or website. [11]

DEFENCE AND DETECTION MECHANISM

There are several different methods of defense and detection mechanisms from Internet attacks. Some of the most common methods are Cryptographic systems, Firewall, Intrusion Detection Systems, Anti-Malware Software and scanners, and Secure Socket Layer (SSL). [12][13]

Cryptography

Cryptography is the science of providing security for information. It involves the use of codes and transforms the information into unintelligible data. The two basic types of cryptosystems are symmetric and public-key systems (or asymmetric systems). In symmetric systems, both parties use the same key in encryption and decryption transformation whereas in public-key systems, the parties use one secret key and one publicly disclosed key in which both keys are related. [13]

Firewall

Firewall is a front-line network security system against intruders that controls incoming and outgoing network traffic. It can be hardware, software- based, or a combination of both. A firewall only allows the traffics that are defined in the firewall policy on to the network, while all other traffics are denied.

Anti-Malware scanners

Anti-Malware scanners are simply special tools used to detect malicious software such as viruses, worms, and Trojan horses; and cure an infected system. [14]

Differences between Firewall and Anti-Malware

The main differences between firewall and Anti-Malware software is that a firewall is designed to block unauthorized communications. It will not protect the system against malicious software. On the other hand, Anti-Malware software is used specifically for the detection and prevention of these malicious softwares. [15]

REFERENCES

[1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [12] [13] [14] [15]

1. http://explainingcomputers.com/networking.html
2. http://www.techcuriosity.com/articles/difference_between_internet_and_intranet.php
3. http://www.webopedia.com/TERM/C/client_server_architecture.html
4. http://www.webopedia.com/TERM/P/peer_to_peer_architecture.html
5. https://www.techopedia.com/2/29090/networks/lanwanman-an-overview-of-network-types
6. http://www.webopedia.com/TERM/I/IP_address.html
7. http://www.thegeekstuff.com/2012/01/ip-address-fundamentals/
8. http://www.webopedia.com/TERM/D/domain_name.html
9. 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

AICMS 08. Second Asia International Conference on, vol., no., pp.77-82, 13-15 May 2008
10. Marin, G.A., “Network Security Basics,” Security & Privacy, IEEE, vol.3 no.6, pp. 68-72, Nov.-Dec. 2005
11. Daya, B., Network Security: History, Importance, and Future. University of Florida Department of Electrical and Computer Engineering.
12. Daya, Bhavya. "Network Security: History, Importance, and Future." (n.d.): n. pag. Print.
13. Marsic, Ivan. "Network Security." Computer Networks: Performance and Quality of Services. N.p.: n.p., 2013. 405-11. Print.
14. "What Is Firewall? - Definition from WhatIs.com." SearchSecurity. N.p., n.d. Web. 23 Nov. 2016.
15. "What Is the Difference between Antivirus and Firewalls." Information Security Stack Exchange. N.p., n.d. Web. 23 Nov. 2016.