EXPLORATION OF NETWORK SECURITY ISSUE AND ITS ATTACK

J.Jayanthi[1] | S.Joseph Gabriel[2]
[1](Research Scholar, Department of Computer Science, Mazharul Uloom College, Ambur)
[2](Associate Professor& Head, Dept. of Computer Science, Mazharul Uloom College, Ambur)

Abstract— *Today's computer networks have gone from typically being a small local area network, to wide area networks, where users and servers are interconnected with each other from all over the world. This development has gradually expanded as bandwidth has become higher and cheaper. But when dealing with the network traffic, bandwidth is only one of the important properties. Delay, jitter and reliability are also important properties for the quality of network connection. This is because different applications has different needs, and therefore require different properties from the network. System administrators are in an increasing degree involved with the troubleshooting of solving network problems concerning the quality of service for the different applications. This research paper analyzed techniques for measuring, analyzing, presenting and interpreting the different properties for the administration of remote computer network. In this way system administrators can benefit from this thesis when administrating their remote computer networks.*

1. INTRODUCTION

The most used network architecture is the client-server architecture. In a client-server architecture the server passively waits for a request, until the client actively sends a request to the server. The server then executes the request and sends the reply back to the client.

One of the first computer networks were isolated local area networks (LANs), with a client-server architecture. The clients were cheap terminals, attached to a screen and a keyboard. At the time, the clients required low network bandwidth. The only data transmitted was the keyboard activity sent to the server, and the screen updates sent back to the client.

The terminals used in these networks are classified as thin clients. This is because most of the processing is done at the server, while the client typically process keyboard input and screen output.

Some advantages with the thin client approach are:

- A lower hardware costs, as there is usually no need for disk, a lot of memory, or a powerful processor. This also creates a longer turnover time, because it takes a longer period of time before the equipment becomes obsolete.
- A lower administration cost, as the clients are almost completely managed from the server. All installations and upgrades are done on the servers, and not on each client.
- A higher client reliability, as the client hardware has less points of failure.
- Increased security, as no sensitive data ever resides on the client. The local environment is usually highly restricted, and the protection against malware is centralized on the servers.

The need to connection to other networks or clients from the existing network, created the next step for computer networks. The connection between the networks was typically created by leased lines or by dial-up connections. The new networks were called metropolitan area networks (MAN) or wide area networks (WAN) depending on the range of the networks. With the creation of these new networks, terminals could now connect to other servers in other networks, and process data in other computer environments.

The personal computer (PC) was intended to conquer the private marked, but the corporate marked also showed great interest. And as time went by, the pc replaced the terminal as the preferred client.

The pc can be a thick client, because it has a disk, memory and a powerful processor that allows the client to run its own operating system and programs. But even though the pc has the properties of a thick client, it can behave like a thin client. This all depends on the software that the pc is running. Applications like telnet and stimulates a thin client environment, because the applications connects to a remote server, and utilizes the resources which is provided by that server. Keyboard actions are sent to that server, and the server only replies with screen changes, just like in a thin client environment.

Traditionally the server had processed both the client environment and the production environment. But with the arrival of the pc, user environment processing could be removed from the servers, and done on the clients own processor. This meant a more efficient usage of the processing servers. In situations where the data could be stored on the pc itself, the processing of the production data could be executed on the local processor. But this moved the bottleneck away from the production server processors, and to the network bandwidth.

Some advantages with the thick client approach are:

- Lower server requirements, as a thick client does most of the application processing itself.

- Lower user environment network bandwidth usage, because there is no keyboard or screen data that has to be sent to and from the server.
- Higher system reliability, as the thick clients can operate even when the processing servers are unavailable.
- Better multimedia processing, because multimedia processing require high band- width and high performance processors.

The internet started off as a few computer networks interconnected with each other. The connection speed, at that time, was only about 64 kilobits per second (kb/s), and the connection between the networks was within the United States of America. Since then, hundreds of millions of people, all around the world, has connected to the inter-net.

The bandwidths available today typically range from 64 kilobits per second on dial-up connections, to gigabits per second on high performance broadband connections. The high bandwidth available on the internet today, enables new possibilities for network applications.

But bandwidth is not the only property for a good internet connection. Properties like delay, jitter, and reliability have become the main focus area in the resent years. Together these four properties make up the basis for quality of service (QoS).

As the internet service providers improve their quality of service, this enables organizations and businesses to structure their computer networks in new ways. There is no longer the need for one location where both the user environment and the production environment are located.

2. Computer Security

To create a secure computer system, three properties are necessary[10]:

- Confidentiality
- Integrity
- Availability

Confidentiality
Confidentiality is about keeping data unavailable for non-authenticated users. This can be achieved by access control and encryption[1][10].

Access Control
Access control is about controlling who has access to specific resources. In a operating system functions are available to provide access control, but if these functions are bypassed or fail, the data are fully compromised[1][10].

Cryptography
Cryptography or encryption is a method to descramble the data so that it is only read- able for authenticated users. Cryptographic methods can be used on data located in a operating system, or data transmitted through a insecure network[1][10].

3. Conclusion

The objective with this master thesis was to assist network and system-administrators in administration of remote computer networks. This was primary done by identifying the properties for securing the remote computer networks, and the properties that are important for the quality of the services. The properties provide quality of service for the connection between the remote computer networks.

Secondary, some simple methods for analyzing and presenting the measured data was identified. These methods simplify the interpretation part of the administration of remote computer networks. The three case studies were created to demonstrate the functionality for some of the tools used to measure the four properties in quality of service.

In Case One, the objective was to make use of passive throughput measurement tools, to monitor the traffic on two different nodes for one day. The tcpstat tool successfully measured the data on both nodes, and provided enough information to create a good understanding of what had happened on the network for the last 24 hours. The only mistake in these two experiments was that the filter functionality in tcpstat should had been used to filter input and output traffic. But as the objective was demonstrate, the experiments can still be classified as successful.

References

[1] Andrew S. Tanenbaum. Computer Networks, Fourth Edition. Prentice Hall, 2003.
[2] Kevin Hamilton Kennedy Clark. Cisco LAN Switching (CCIE Professional Development). Cisco Press, 1999.
[3] Annabel Z. Dodd. The Essential Guide to Telecommunications, Second Edition. Prentice Hall PTR, 1999.
[4] Sergio Verdú. Wireless bandwidth in the making. IEEE, 2000.
[5] Gene Spafford Simson Garfinkel, Alan Schwartz. Practical Unix & Internet Security, 3rd Edition. O'Reilly, 2003.
[6] Fred Halsall. Data Communications, Computer Networks and Open Systems, Fourth Edition. Addison-Wesley, 1996.
[7] William Stallings. Local networks. ACM, 1984.
[8] Mahbub Hassan and Raj Jain. High Performance TCP/IP Networking. Pearson Prentice Hall, 2004.
[9] W. Richard Stevens. The Protocols (TCP/IP Illustrated, Volume 1). Addison- Wesley, 1993.
[10] Matt Bishop. Computer Security, Art and Science. Addison-Wesley, 2002.
[11] Cross-Industry Working Team. Internet service performance: Data analysis and visualization. Technical report, The Cross-Industry Working Team (XIWT), 2000.