The Internet as a network – Security

Bharat Halai - 9917398

Advanced Topics in Networks, first assignment, University of East London, Dagenham, Essex

Abstract

With the recent explosion of the Internet into the global market many of its disadvantages have been blown into proportion. Initially it started off as a military system whereby machines would be linked together using lines so that information can be successfully shared among military machines during wars. It has since then outgrown this objective and is now being extensively used to share general information from simple text documents to providing live feed and updates for customers who are home users to multi-billion pound organisation. This was certainly not expected.

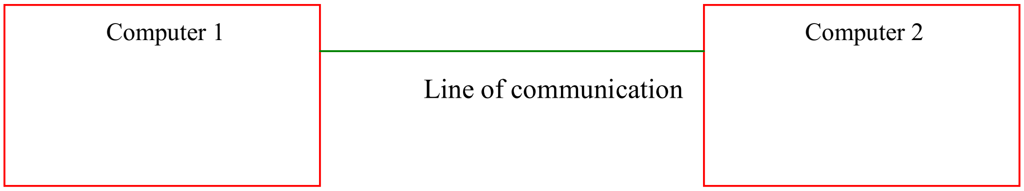
Keywords: Internet

Introduction

With the recent explosion of the Internet into the global market many of its disadvantages have been blown into proportion. Initially it started off as a military system whereby machines would be linked together using lines so that information can be successfully shared among military machines during wars. It has since then outgrown this objective and is now being extensively used to share general information from simple text documents to providing live feed and updates for customers who are home users to multi-trillion pound organisation. This was certainly not expected.

Being public, the Internet like any road or highway is available to be used by any and every one. Therefore with anything that is public there is an element of security that needs to be acknowledged. It is commonly known that the Internet is unsecure due to the design and nature of it. In order to understand it is best if we start from the basics of the Internet and how it works.

Essentially the Internet is two machines talking to each other, one obtaining information from the other to either provide this information to its operator or to carry out tasks that it may need to complete:



The line of communication does to have to necessarily be a physical connection from point to point, it could be a connection of several million of metres working of a connectionless network therefore travelling over several other network. This is the problem, the fact that this information travels over different networks making it prone to attacks. With one computer communicating with another it has a set of rules (could be loosing related to a language) known as a set of protocols, a set of rules that govern the way that a device communicates with another. The most widely used protocol if known as TCP/IP.

TCP/IP

Transmission Control Protocol with Internet Protocol consists of four layers that all work together to produce the end result of a packet reaching the destination from the host:

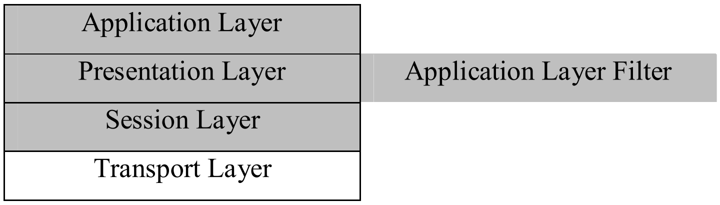
Application layer – consist of applications and processes that use the network
Host-to-host layer – provides the end to end data delivery mechanisms
Internetwork layer – defines the datagram and handles the routing of data
Network access layer – consists of routines for accessing physical networks **[1]**

Each layer in the stack has to add its own control information such as destination address, routing controls and checksum, these ensure proper delivery of information from source to destination. This information is usually referred to as a header and/or a trailer as it is placed in front or behind the data that is to be transmitted.

Firewalls

Firewalls play an important part in preventing access to systems. There are two types of architectures available on the market and that of which are designed for:

- Packet level firewalls – these firewalls operate at the network (IP) and on the transport (TCP) layers, these are commonly referred to as screening routers or packet filters and clock transmission of certain classes to traffic.
- Application level firewalls – these operate at the session, presentation and application layers. These firewalls are usually implemented for specific and specialised software packages for their custom requirements, for example proxy servers running on UNIX or Windows NT.



Packet Level Filter	Network Layer
	Link Layer
	Physical Layer

[2]

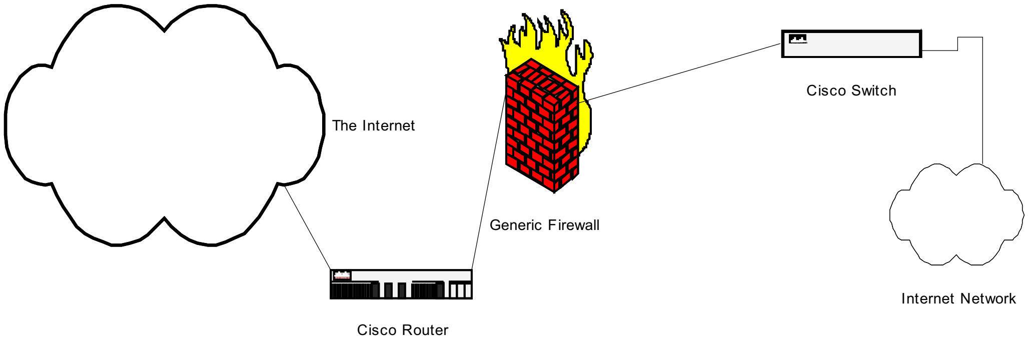
This is the most commonly form of firewall found on the Internet protecting company networks from the Internet as a whole. Essentially a firewall checks for the packet's port number that it wishes to access within a particular network. Each program no matter how small or big has its own port number that it will use within the TCP/IP network, for example:

Protocol / software package	**Port number**
File Transfer Protocol	21
Telnet	23
ICQ	5190
SMTP	25
SSL	443

[3]

An administrator can block communication by blocking any of these ports, typically SMTP and ICQ ports are blocked from the external network as users from both inside the network and outside can cause problems such as exploit weaknesses that a custom written package may have. **[2]**

A firewall would sit in between a router that has the connection to the Internet and company switch although more complex networks may be planned differently according to requirements:



The above diagram shows a typical physical set up whereby packet come in through the Internet straight into a router which only lets in specific IP ranges that have been allocated to the company. All packets that are of this range are then accepted into the network. The next obstacle is the firewall which only lets in packets that are of a particular port number. Typically companies will let in the following port numbers according to their requirements:

Protocol / software package	**Port number**
HTTP	80
FTP	21
TELNET	23
SSL	443

Application level gateways and firewalls

As well as providing general protection using firewalls applications can be programmed in such away to prevent and avoid hackers from getting into the software package. For example an application can be programmed to disregard software that it is not concerned with. An example would be Telnet which works on port 23, this package will only accept packets that arrive from the computer and only accept port 23.

There are several advantages to these firewalls:

- There may be many sub programs within a program that may need to access external resources, having a gateway built in prevents hackers from knowing the structure of the program that is being used. On the outside the program would appear as one but may have several running inside it.
- Traffic can be pre-authenticated whereby control packets before reaching internal hosts therefore preventing breaches within the application itself.
- Cost effective has third party software would be need to audit or authenticate packets.
- Filters are less complex as they only apply to the application is question therefore avoiding problems whereby delaying traffic. **[4]**

Viruses

Another major problem on the Internet is the threat of viruses. Viruses are usually associated with trojan houses and worms whereby a program is written to take advantage of security loopholes that may not have been tested for when the operating system or software was created.

Traditionally viruses are perceived as programs that will cause problems/destruction on the application layer as they are affect programs, this is not true. Commonly these viruses are spread through the Internet causing great damage and problems to internal networks. The latest network virus was code red which would attach itself to Microsoft IIS servers and would send out broadcasts, this is turn would clog up a corporate network making it impossible for the business to function as it should. This virus caused problems on the network layer as it sent out broadcasts. Other viruses would consume CPU time preventing other tasks from being processed.

Proxies

Proxy server provide an important way of filtering WWW traffic entering a network. This is usually a package that will run within a firewall server as they work very closely within the task their both perform. A range of protocols may be filtered or allowed into the network through the proxy, theseare decided by the administrator administering the network.

Requirements for Internet Firewalls [4]

If an Internet firewall is set up properly it will provide the following advantages:

- Implement a safe subset of the protocol
- Perform extensive protocol validity checks
- Use an implementation methodology designed to minimize likelihood of bugs
- Run in an insulated, “safe” environment, or
- Use some combination of these techniques in tandem.

Depending on the rules set by the firewall configuration the firewall will direct packets accordingly:

- If the rules allow the packet through and meet the criteria with it lets it through unchanged.
- Drop the packet entirely if it does not meet the criteria

Firewalls have their downfalls due to the nature of security required. Algorithms developed still need to be optimised and improved. Software packages need to be aware that there is a firewall on the network therefore cross network requests can be processed without being disrupted. Often software packages will try to talk to software servers on the Internet through an unauthorised ports. An example would be the messaging program ICQ, registration and general software interaction between the Internet servers at ICQ HQ normally communicate over port 5190. Most companies block this protocol to avoid unauthorised access through a corporate network, in the same way employees within the network can not sign up to ICQ using this port. However ICQ allows traffic to travel through port 23 which most networks do allow for web access.

IPSec

There are several mechanisms in place to avoid breaches of security within and outside organisations. These are not essential to the running of companies but many companies do use them to communicate with each other and also to prevent hackers from intercepting information between there customers. IPSec is one such mechanism that provides security services to the IP layer allowing certain security protocols to be required before services are approved. IPSec can be used to protect several paths from internal workings of the network to communication through gateways and the Internet, therefore providing universal security without having to change protocols for specific types of network.

> “The set of security services that IPSec can provide includes access control, connectionless integrity, data origin authentication rejection of replayed packets (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality. Because these services are provided at the IP layer, they can be used by any higher layer protocol, e.g. TCP, UDP, ICMP, BGP, etc.” [5]

IPSec makes use of two protocols to provide the security:

- AH (Authentication Header)

AH is designed to provide connectionless data integrity service and data origin authentication server for IP datagrams and optionally to provide protection against replay attacks. AH works by authenticating the upper layer packets and IP packet where possible.

- ESP (Encapsulating Security Payload.

ESP is designed to provide a mix of security services, especially data confidentiality service in IP. ESP works by being encapsulated by the IP header. At the same time the ESP encapsulates either the transport layer or the IP header/ tunnel mode.

IPSec makes use of both of these protocols to create a form of preventing packets from being sniffed. They can also be used separately or in combinations with other protocols. They are both based of distribution of cryptographic keys and the management of traffic flows relative to these security protocols.

Auditing

Auditing is an important of any system. It allows administrators to monitor whether packets are safely reaching their destination as quite often packets are sniffed and hackers will often try to modify packets. Administrators can then modify the way in which the packets are being sent out.

Conclusion

Internet is and will remain a huge realm of unexplored space (hence the name world wide web). Due to the scale of the Internet it is not easy to control what happens and who connects. The information super highway, as it is commonly known is not easy to maintain. If we think about an every motorway we have, it is practically impossible for it to be policed and to avoid who travels on it or indeed who travel in the vehicles on the motorway. It is possible that rogue packets can travel on the Internet, they may appear to be normal good-doing packets but could potentially cause great damage to a company's network and indeed reputation. This document has covered potential ways of preventing such occurrences; firewalls, virus checkers, IPSec but unfortunately there is no way that network security will be 100% covered, there will always be a way around security. A hacker who knows what they are doing will always know how to get around a feature, all they have to do is read about how the feature works and then work around the security.

It has never been easy controlling the Internet, with the introduction of IPv6 we should hopefully one day see that the work of a hacker is somewhat impossible to do. IPv6 has many in built features that will help in the fight to save companies network.

References

[1] Cisco, Appendix A – Understanding TCP/IP, LA, 1996

[2] Elsevier, Internet – services, facilities, protocols and architecture, Ray Hunt, 1997

[3] Elsevier, Network system and world wide web security, B.C. Soh, S. Young, 1997

[4] IETF, Behavior of and Requirements for Internet Firewalls, N. Freed, 2000

[5] IETF, Security Architecture for the Internet Protocol, S. Kent, BBN Corp, 1998