# Security Issues of Firewall

Aakanksha Chopra

*Assistant Professor (IT), Jagan Institute of Management Studies (JIMS), Rohini, New Delhi-110085*

*Affiliated to GGSIPU, Dwarka Sector-16C*

***Abstract-****The need of Network Security is accelerating at the same pace as that of increased Internet usage. Network Security prevents from illegitimate admittance, hacking andauthentic data transportation. Network Security consist of provisions and policies adopted by a network administrator to preclude and monitor unauthorized access, alterations, perversion, declination of a computer network and network-accessible resources. Network Security is achieved by Firewall. Firewall is a hardware or software device which is designed to permit or refuse network transmissions based upon certain protocols. Firewall is a locus at the end-points of the system which strains out all illegitimate traffic and users. But conventional or traditional firewalls rely strictly on the restricted topology and restrained entry points to function; which results in difficulty in filtering certain protocols, end-to-end encryption problem etc. Hence, it resulted inthe evolution of Distributed Firewall which strengthens the network security policies without delimitating its topology from inside or outside. Distributed Firewall is a host-resident security software application that protectsthe enterprise network's servers and end-user machines against unwanted intrusion. Thispaper is a literature review paper focussing on traditional firewalls, it evolution, security issues various policies and theconcept of distributed firewall.*

***Keywords-****Firewall, Network Security Issues, Firewall Policies, Distributed Firewall.*

## I. INTRODUCTION

Today every business in this world regardless of its size or type believes that internet access is very crucialif they want to compete with their competitors effectively. Also it is virtually impossible to compete in today's fast-paced business without connecting your private network to the public network[3]. People need to quickly access and exchange the data with other people in the business, customers and the whole world at a large scale to stay one step ahead in the business. Though there are many advantages of connecting to the internet but simultaneously, there are many threats attached with it.

Today, computers are widely used in transmitting data and information rather than processing, for example, a large amount of confidential transaction occur every second. Fatefully such connectivity provides an easy way for unfrosted parties outside to enter in a company's private network and access or tamper the internal information and resources[2]. But in order to have a secure transmission of the information being exchanged over internet, one needs the concept of Network Security, which needs to takepunitive action to Ease of Use protect from different types of attackers like- hackers, interested computer neophytes, deceitful vendors or disenchanted employees of an organization [9,12]. Network Security helps in maintaining authorized access of data from hackers and authenticated data transfer. Network security is achieved by installing a firewall.

A firewall is a hardware device or software system or group of systems (router, proxy or gateway) designed to permit or deny network transmission based upon set of security rules and regulations to enforce control between two networks to protect "inside" network from "outside" network. A firewall could also be a hardware device or a software program which might be running on a secured host computer as stated above. Actually, in both the cases it must have two network interfaces, one for the network it is intended to protect, and one for the network it is exposed to. A firewall protects a local system or network systems from all the network- based security threats while at the same time it same provides access to the outside network through WAN and internet[2].According to Frederic Avolio - "many people feel that internet security and internet firewall are same"[6].

Internet firewalls have been around for a hundred years in the Internet. Internet firewall also protects against some of the following attacks also but not all[6]-

A. ***Denial-of-service attack***
DOS attack is an interruption in authorized user's access to a computer or networks. It includes all types of attacks such that the genuine end user of a computer or a network cannot use it.

B. ***Eavesdropping***
(literally means secretly listening to a conversation) is basically all kinds of attacks like stealing the e-mail passwords, messages,

files, data, information over the network connection by listening on the connection.

C. ***Host Attacks***
It basically attack the vulnerabilities of operating systems or in how the system is organized and administered.

D. ***Password Guessing***
Guessing of the password for malicious activities.

E. ***Protocol-based attacks***
Which takes advantage of known/ unknown weaknesses or network services.

F. ***Social Engineering***
This is an attack by the social means. Basically attacker acts as a genuine user or administrator and extracts all the secretive information from the user socially.

G. ***War Dialing***
This type of attack is a unique in its own way which basically means entering into someone's personal desktop via modems.

Early firewalls were easy to maintain and support as they were bounded to the fewer Internet services available at that time. Nowtoday's scenario has changed upside down as today the requirement is not only secure access of Telnet, FTP, SMTP,USENET; rather today people want to connect to WWW, file sharing, news, music, audio videoconferencing, database access and what not. The hefty range of information is nowadays accessible & reachable and also in demand.

Internet was introduced much later after a discovery of computers. As before the mode of communication was not through e-mails, rather people relied only on postal, telegram or telephone services. The Internet actually started as the Advanced Research Projects Agency NETwork (ARPANET) which was small and a closed group. In late 1980's Morris worm attack resulted in the change in the INTERNET forever (Peter Yee, NASA, Ames Research centre, 1988). Morris worm actually showcased that the internet was no longer a community of trusted people. Henceforth, alert mails were sent dedicated to security and bug tracking to alert the users. There were many other renowned attacks like- Bill Cheswick's "evening with Berfered", the massive password capture of winter of 1994, etc. [6].

A firewall plays a very crucial role in foster networked computers from wilful hostile intrusions that could comprise of confidentiality or result in data corruption or denial-of-service or any of the above mentioned network attacks. Firewall could be a hardware device (as shown in Fig 1) or a software program (as shown in Fig 2).

***Hardware firewall:*** provides protection to a local network, Hardware firewall is usually part of TCP/IP router.

***Software firewall:*** it is a computer with firewall software which provides protection from intruders, which may also provide internet connectivity between Private LAN and Public Network/ Internet. Maximum penetration of intruders happens and is seen on the public network only.

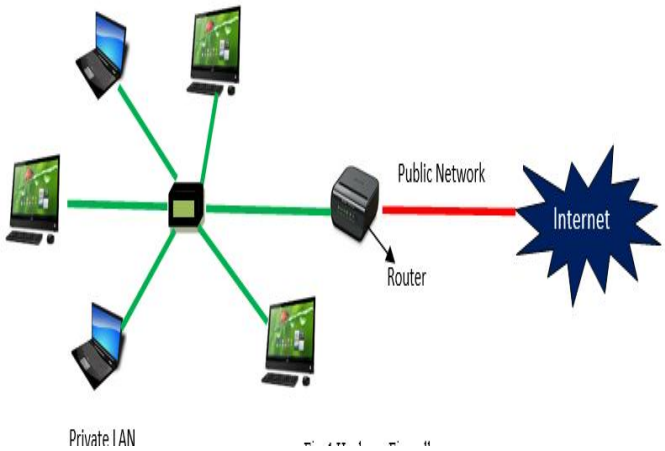



Fig 1: Hardware Firewall

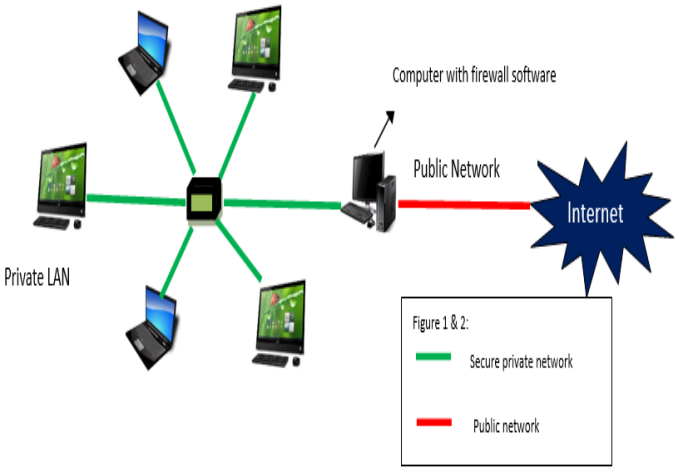



Fig 2: Software Firewall

## II. Firewall History

Firewalls are the barricade to different types of attacks, meant to slow down its spread, [*Cheswick and Bellovin*] in the definitive text on Internet firewalls said an Internet firewall has the following properties: it is a single point between two or more networks where all traffic must pass also called choke point (a choke point is a strategic narrow route providing passage to another region); traffic can be controlled by and maybe authenticated through the device, and all traffic is logged. In a talk, Bellovin

also stated that- "Firewalls are barriers between 'us' and 'them' for arbitrary values of 'them' "[6].

- In late 1980's came to the first network firewalls& those were the routers used to divide Network into smallerLAN's. Such kind of firewalls was put in place to impede obstacles from one LAN to unveil & affect the entire network.
- In 1990's first security firewall was used. These were IP routers with filtering rules/ refining rules. This security policy allowed "anyone in" Organization to access data "outside" the organization. Also, it does not allow anyone who is "out there" (who is not trusted) to get access to "inside" data of an organization. The **Advantage** of this firewall was that they were effective fromthe security point of view, but they were limited. The major **Drawbacks** of this firewall were firstly, it was difficult to get filtering rules right. Secondly, it was difficult to identify all the parts of an application that should be restricted in some cases.
- Next security firewall were built on the concept of Bastion Host-(which is a special purpose computer on a network specifically designed and configured to withstand attacks.)These were more refined & more skilful&were likely first commercial firewalls of this type. They used filters and application gateways (proxies) from DEC(Digital Equipment Corporation) & were based on DEC corporate firewall.
- Later Marcus Ranum at DEC invented security proxies and that product was called DEC SEAL(Secure External Access Link.) The DEC SEAL System was made up of an external system, called Gatekeeper,a filtering gateway called gate & an internal system Mail Hub [6]. Gatekeeper is the only system the internet could talk to. The Mail Hub is used to denote a Message Transfer Agent(MTA) or MTAs used to route email but it does not act as a mail server(having no end-user email store) since there is no Mail User Agent(MUA) access [13].
- Around 1992, "Cheswick & Bellovin" at Bell Labs were experimenting with ***Circuit-Relay Based firewalls***- it is a type of security firewall (proxy firewall) that provides a controlled network connection between Internal & external systems[14].***Raptor Eagle*** came after DEC SEAL was delivered, followed by the ANS Interlock.
- On Oct 1, 1993, Trusted Information System (TIS) Firewall Toolkit(FWTK) was released in source code from the internet community. It was later named ***Gauntlet***. This is still used by experimenters as well as in the industry as a basis for internet security.
- In 1994, Check Point followed with the Firewall-1 product which introduced "user-friendliness" to the world of internet security. Check points introduced icons, colors & mouse-drivers tools etc.The firewalls before Firewall-1 required editing of ASCII files with ASCII editors[6].

## III. Basics of Firewall

Basically, a firewall inspects all the traffic between the two networks and checks that they meet all the prettified prototype and protocols.A firewall is routed between that networks only if they follow the prettified prototype else if they do not follow the prototype then it is stopped. A firewall helps not only in limiting the entry of unwanted or malicious host or users but also helps in dismaying with all the upcoming threats as follows-

- A firewall refines both the incoming and outgoing transit.
- It can also manage public access to the private networked resources such as host applications.
- Firewalls can filter packets based on their source and destination addresses and port numbers- called address filtering.
- Firewalls can also filter specific types of network traffic- called protocol filtering.
- Firewalls can also filter traffic by packet attribute or state.
- It can be used to record all the attempts to enter the private network and elicit alarm when a hostile or unauthorized entry is there.

Considering above points still there are many security issues on which firewall simply have no control. A firewall act as a bridge between two networks LAN but,preciouslyit is unable to deal with following threats[6]-

### A. *Malicious employees*

Actually firewalls are horrible at examining and analysing people perception, or finding the packets of data with "wrong intent". If any employee tries to do a malicious activity or any misconduct is done by an employee

then these kinds of activities could not be controlled by the firewall.

B. ***Modem users***
A firewall cannot safeguard the connections which are not surpassing through a firewall. A firewall cannot baffle individual users with modems from dialing into or out of the network, bypassing the firewall altogether.

C. ***Policies***
Firewall has no control over the policies involving the use of passwords which actually results in misuse of individual passwords and user accounts. This must be strictly enforced.

D. ***Previous Attacks***
The Firewalls provide very lesssalvation against previously unknown attacks.

E. ***Viruses***
Proffer typically down- and- out protection against computer viruses.

Above mentioned management issues hamper efficient working of a firewall hence, these issues must be resolved while planning of a security policy as they can never be solved alone by firewalls.

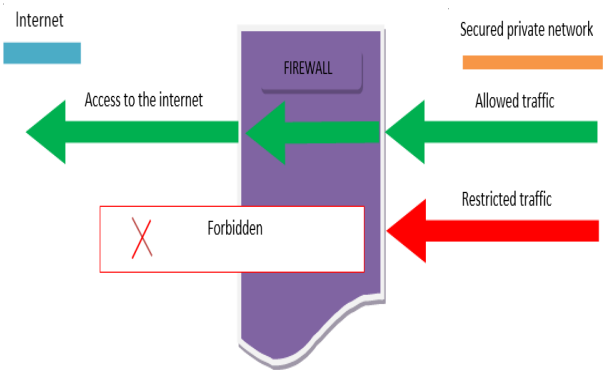
## IV. Working of Firewall

A conventional firewall has certain policies to protect the data from outsiders, but not all data or information could be protected internally from insiders of the network.Firewall is a security impulsioniota to separate a reliable network from unreliable ones. There are two access denial approaches used by firewalls. A firewall shrouds all the connections between two networks, itmay allow all the traffic through,till it meets assertive criteria, or it may deny all the traffic unless and until it meets assertive criteria based on some form of security policy decisions determined in advanced bythe security administrator.Conventional or Perimeter firewalls are the devices placed on the edge if the network that act as a security guard. The firewall forces a central policy of which firewall will be allowed in and out of the network. The assertive criteria used to find whether to allow or deny the traffic depends on one type of firewall to another[2].

When traffic flows through thefirewall it is evaluated by a set of rules based ona type of traffic, or with source or destination IP address or with the port numbers. Sometimes the firewall also exercisescomplicated rule bases that evaluate andanalyses the application data to determine if the traffic should be conceded to pass through or not. All traffic arriving orleaving the network must always pass through this point/iota. This necessity is the main declension of a firewall. Forexample, users might go around the firewall by using a modem or some other connection to the Internet. Another problem isencrypted tunnels, which allows traffic to flow freely through the firewall without any prototype or protocol checking. Some problems with the standard firewall are discussed in the section “problems with conventional firewalls” topic in this paper.

Following justifies how a firewall in realityclinch which traffic to allow in or deny. This is decided by the firewall depending on the network layer it works on. The intrinsic functioning of the firewall is shown in Fig. 3. The firewall keeps an eye on both the entry and exit points of data. Primarily, when the secured private network intends to interact with the Internet, there are two types of traffics- allowed traffic and restricted traffic. Allowed traffic is one which meets all the prettified criteria and hence the secured private network is allowed to interact with the public or social network famously known as the Internet. On the other hand, the restricted traffic is the one which fails in meeting the set predefined criteria and is not conceded to interact with the public network.

The firewalls correspondingly keeps a check on data immigrating from the internet into the private network. Looking at figure 3 we can see that in order to keep it immunetwo types of traffics- specified allowed traffic and unknown traffic. Specified allowed traffic is one coming from the Internet on some request and is allowed into the secured private network because it could meet the predefined criteria. Once an entry is allowed into the secured network then it gets access to the specified resources. Unknown traffic is the one anticipated from the internet and aggravating to enterthe secured private network, but not concede to enter as it could not meet the criteria.



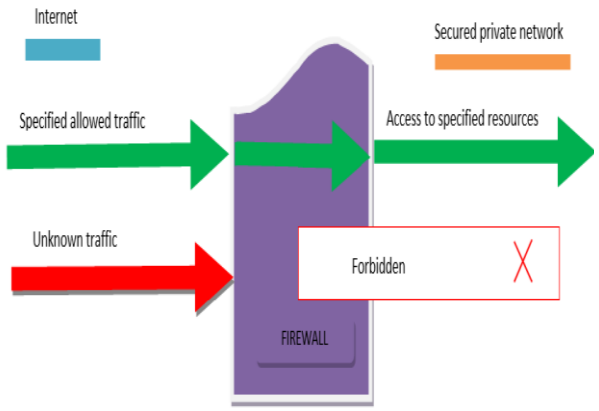



Fig 3: Intrinsic functionality of the Firewall

Firewalls working depends upon how different layers of network work. Two well know models called OSI and TCP/IP model have different layers and each layer in both the models have their well-defined responsibilities[4]. Networks generally mix and match network protocols and physical supports. A single protocol can travel and interact through more than one layer in a given network because the physical layer is disaffiliated with network layers (layer 3 to 7 in OSI model [4]).

As discussed earlier also firewall have a different functionality on a different layer. In reality, the firewall starts it's working from layer 3, i.e. Network layer in OSI model and Internet Protocol Layer (IP layer) in TCP/IP model[4]. At this layer, a firewall can easily track whether a packet is from a legitimate source or not as this layer is concerned with routing of the packets. But at the same time a firewall placed at this layer cannot determine the contents of the packet or what other packets it is associated with. Firewalls placed on the Transport layer can find out a little extra information about the packet; a firewall here can also accept or deny the access depending upon more disenchanted criteria. At the final application layer firewalls become highly selective in granting access as they know almost everything about the packet.

It is generally considered that firewalls should behave exceptionally well atthe paramount level in the stack of network layers. But this is not actually true. The lower the malicious packet is interloped in the stack, the higher secure is the firewall. Also, if the intruder is unable to cross layer 3, then it is almost impossible for him to have control of the operating system.

There are some Professional firewall products that have their own Firewall IP layer that catches each network packet before the operating system does, henceforth, there is no explicit path from the Internet to the operating system's TCP/IP stack. Therefore, it becomes very struggling for an invader to gain control of the firewall host computer then "open the doors" from the inside (refer Fig 4.)

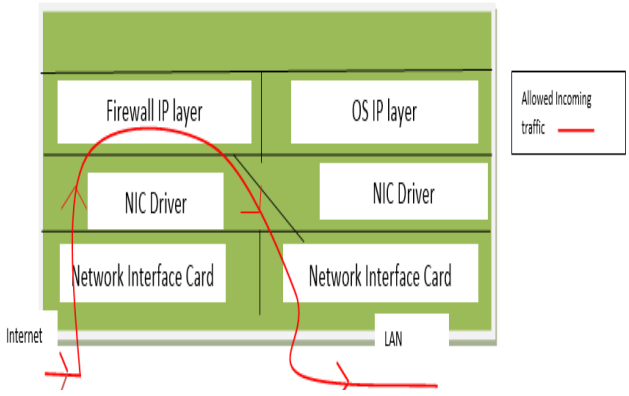



Fig 4 Firewalls with their own IP Layer

## V. Problems With Conventional Firewalls

Reading and analysing about the traditional firewall plenty of loop holes were found and also discussed[3]. All the four different firewalls namely Packet filters, circuit level gateways, application level gateways and stateful multilayer inspection firewalls are having discrete wizards and deceptions. Few of them are also specified below-

- Packet filtering firewall which only works on network level of OSI model, does not support sophisticated rule based models.
- Circuit level gateways works at session layer of OSI model, though they stash the information about protected networks, but they do not strain distinct packets.
- Application level gateways famously known as proxies are very much analogous to the circuit level gateways except that they are application specific. They also pitch a very high level of security, but have a momentousimpingement on network performance.
- Stateful multilayer inspection firewalls are the amalgamation of above three firewalls, but they are supremelycostly and also due to their complexity are potentially less secured than simpler firewalls.

## VI. Who Needs Firewall?

There are many places and organizations where the firewall is needed. Firstly, any private network which is connected to the public network need firewall protection. Secondly, anyone who connects as a single computer to the Internet through modem should have a personal firewall software. Dial-up internet users think that no illegitimate user would be entering into their system, but these users have been

the victim of illegitimate attacks and have lost most of the data. Firewall is also required by these users to avoid such attacks.

## VII. Conclusion

Computer networks are prone to attacks and it has wide range of attacks associated with it. There are chromatic types of internet attackers like- hackers, interested computer neophytes, deceitful vendors or disenchanted employees of an organization. It is not necessary that attacks always originated from extrinsic(external) parties but can also be caused by lack of intrinsic (internal) information security, and due to bad policies and procedures. Also, new security risks could arise from evolving attack methods or newly detected holes and bugs in existing software & hardware.Social Engineering, War dialing, Denial-of service attacks, Protocol based attacks, Host attacks, password guessing, Eavesdropping [6]. Back doors, Brute force, Exploiting known security vulnerabilities, Guessing passwords, Hijacking, Random Dialing/ War Dialing, Sniffers, Social Engineering, Spoofing, Trojan Horses, Viruses, Impersonation, Exploits, Transitive Trust, are many internet attacks which could also fool conventional firewall and harm individual desktop or entire networks like anything. To avoid this impact of internet attacks and the later consequences Distributed Firewall is used.

Distributed Firewall is a mechanism to enforce a network domain security policy through the use of a policy Language, policy distribution scheme enabling policy control from a central point and certificates, enabling the identification of any member of the network policy domain. It secures the network by protecting critical network endpoints, exactly where hackers want to penetrate. It filters traffic from both the Internet and the internal network. They provide unlimited scalability and also they overcome the single point of failure problem presented by the perimeter firewall.

## ACKNOWLEDGEMENT

I would like to thank all people who have helped me to give the knowledge about these research papers. Finally I would like to thank all the website and CISCO, International Journal of Computer Science and Applications paper which I have gone through and have refer to create my research paper successfully.

## REFERENCES

[1] Kahate, A. *Cryptography and Network Security*. ISBN-13: 978-0-07-064823-4, ISBN-10:0-07-64823-9, McGraw Hill Higher Education.

[2] Forouzan, B. A., & Mukhopadhyay, D. *Cryptography and Network Security.* ISBN-13:978-0- 07-70208-0, ISBN-10: 0-07-070208-X, Mc Graw Hill Higher Education.

[3] Stallings, W. *Cryptography and Network Security Principles and Practices.* ISBN-978-81-775-8774-6.

[4] Tanenbaum, A. S., Watherall, D. J. *Computer Networks.* ISBN-13: 978-0132126953, ISBN-10: 0132126958, 5th Edition, Paperback, 2010, pp: 34-39.

[5] Rathod, R.H., & Deshmukh, Prof. V.M. (2013). Role of Distributed Firewalls in Local Network for Data Security. *International Journal of Computer Science and Applications*, Vol. 6, No. 2, Apr 2013, ISSN: 0974-011 (open access), pp: 360-364.Retrieved from official website: www.researchpublications.org

[6] Zeng-gang, X., & Xue-min, Z. (2010). Research and Design on distributed Firewall based on LAN. *Computer and Automation Engineering (ICCAE), 2010*, E-ISBN: 978-1-4244-5586-7, Print ISBN: 978-1-4244-5585-0, INSPEC Accession Number: 11259785, DOI: 10.1109/ICCAE.2010.5451596, Publisher: IEEE, Singapore, *pp: 517-520*

[7] Patel, H. B., Patel, R. S., & Patel, J. A. (2011). Approach of Data Security in Local Network using Distributed Firewalls. *International Journal of P2P Network Trends and Technology (IJPTT)*, Vol. 1 Issue 3- 2011, ISSN: 2249-2615, pp: 26-29. Retrieved from: http://www.internationaljournalssrg.org

[8] Avolio, F. Firewalls and Internet Security, the Second Hundred (Internet) Years. *The Internet Protocol Journal*, Vol. 2, No. 2.Retrieved from official website of CISCO: http://www.cisco.com/web/about/ac123/ac147/ac174/ac200/about_cisco_ipj_archive_article09186a00800c85ae.html

[9] Sahare, S., Joshi, M., & Gehlot, M. (2012). A Survey Paper: Data Security in Local Networks Using Distributed Firewalls. *International Journal on Computer Science and Engineering (IJCSE)*, Vol. 4 No. 9 Sep 2012, ISSN: 0975-3397, pp: 1617-1622.

[10] Gaud, J.V., & Bartere, M.M. (2014). Data Security Based on LAN Using Distributed Firewall. *International Journal of Computer Science and Mobile Computing (IJCSMC)*, Vol. 3, Issue. 3, March 2014, ISSN pp: 386-391.Retrieved from IJCSMC official website:www.ijcsmc.com

[11] Bhovare, S. R., & Chaudhari, B. K. (2014). A Survey on Data Security Provided in Local Network Using Distributed Firewall. *International Journal of Research in Advent Technology*, Vol. 2, No. 4, April 2014, E-ISSN: 2321-9637, pp: 169-171.

[12] Warade, S. J., Tijare, P. A., & Sawalkar, S. N. (2014). Data Security in Local Network using Distributed Firewall: A Review. *International Journal of Computer Applications (0975-8887), National Conference on Emerging Trends in Computer Technology (NCETCT-2014)*, pp: 19-21.

[13] (2009) Wikipedia. [Online]. Available:https://en.wikipedia.org/wiki/Distributed_firewall.

[14] S. Tom. Networking defined & Hyperlinked. [Online]. Available:www.linktionary.com/c/circ_firewall.html

[15]Marcus J. Ranum (1997). [Online]. Available:www.ranum.com/security/computer_security/archives/internet-attacks.pdf

[16] Security Attacks. [Online]. Available: http://www.comptechdoc.org/independent/security/recommendations/secattacks.html