ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue I, January 2016 in association with
KARUR VELALAR COLLEGE OF ARTS AND SCIENCE FOR WOMEN, KARUR
Conference on Emerging Trends and Functional Applications of Computer Technology - 12th January 2016

# THE SURVEY ON NETWORK SECURITY

**M.ALEXANDER [1] Dr. Shanthi[2]**

1. Research Scholar (Part-Time),Bharathiyar University,Coimbatore, TamilNadu, India.
2. *Vice Principal, Alpha Arts and Science College, Chennai, Tamil Nadu, India.*

## Abstract:

Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. The architecture of the internet, when modified can reduce the possible attacks that can be sent across the network. Knowing the attack methods, allows for the appropriate security to emerge. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms. The businesses create an "intranet" to remain connected to the internet but secured from possible threats. The entire field of network security is vast and in an evolutionary stage. The range of study encompasses a brief history dating back to internet's beginnings and the current development in network security. In order to understand the research being performed today, background knowledge of the internet, its vulnerabilities, attack methods through the internet, and security technology is important and therefore they are reviewed.

## 1. Introduction:

The world is becoming more interconnected with the advent of the Internet and new networking technology. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide. Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet. There are currently two fundamentally different networks, data networks and synchronous network comprised of switches. The internet is considered a data network. Since the current data network consists of computer-based routers, information can be obtained by special programs, such as "Trojan horses," planted in the routers. The synchronous network that consists of switches does not buffer data and therefore are not threatened by attackers. That is why security is emphasized in data networks, such as the internet, and other networks that link to the internet.

## 2. Technology for Internet Security

Internet threats will continue to be a major issue in the global world as long as information is accessible and transferred across the Internet. Different defense and detection mechanisms were developed to deal with these attacks.

### 2.1 Cryptographic systems

Cryptography is a useful and widely used tool in security engineering today. It involved the use of codes and ciphers to transform information into unintelligible data.

### 2.2 Firewall

A firewall is a typical border control mechanism or perimeter defense. The purpose of a firewall is to block traffic from the outside, but it could also be used to block traffic from the inside. A firewall is the front line defense mechanism against intruders. It is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both [8].

### 2.3 Intrusion Detection Systems

An Intrusion Detection System (IDS) is an additional protection measure that helps ward off computer intrusions. IDS systems can be software and hardware devices used to detect an attack. IDS products are used to monitor connection in

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue I, January 2016 in association with
KARUR VELALAR COLLEGE OF ARTS AND SCIENCE FOR WOMEN, KARUR
Conference on Emerging Trends and Functional Applications of Computer Technology - 12th January 2016

determining whether attacks are been launched. Some IDS systems just monitor and alert of an attack, whereas others try to block the attack.

### 2.4 Anti-Malware Software and scanners

Viruses, worms and Trojan horses are all examples of malicious software, or Malware for short. Special so-called anti-Malware tools are used to detect them and cure an infected system.

### 2.5 Secure Socket Layer (SSL)

The Secure Socket Layer (SSL) is a suite of protocols that is a standard way to achieve a good level of security between a web browser and a website. SSL is designed to create a secure channel, or tunnel, between a web browser and the web server, so that any information exchanged is protected within the secured tunnel. SSL provides authentication of clients to server through the use of certificates. Clients present a certificate to the server to prove their identity.

## 3 Attacks through the Current Internet Protocol IPv4

There are four main computer security attributes. They were mentioned before in a slightly different form, but are restated for convenience and emphasis. These security attributes are confidentiality, integrity, privacy, and availability. Confidentiality and integrity still hold to the same definition. Availability means the computer assets can be accessed by authorized people [8]. Privacy is the right to protect personal secrets [8]. Various attack methods relate to these four security attributes. Table 1 shows the attack methods and solutions.Common attack methods and the security technology will be briefly discussed. Not all of the methods in the table above are discussed. The current technology for dealing with attacks is understood in order to comprehend the current research developments in security hardware and software.

### 3.1 Common Internet Attack Methods

Common internet attacks methods are broken down into categories. Some attacks gain system knowledge or personal information, such as eavesdropping and phishing. Attacks can also interfere with the system's intended function, such as viruses, worms and trojans. The other form of attack is when the system's resources are consumes uselessly, these can be caused by denial of service (DoS) attack. Other forms of network intrusions also exist, such as land attacks, smurf attacks, and teardrop attacks. These attacks are not as well known as DoS attacks, but they are used in some form or another even if they aren't mentioned by name.

#### 3.1.1 Eavesdropping

Interception of communications by an unauthorized party is called eavesdropping. Passive eavesdropping is when the person only secretly listens to the networked messages. On the other hand, active eavesdropping is when the intruder listens and inserts something into the communication stream. This can lead to the messages being distorted. Sensitive information can be stolen this way [8].

#### 3.1.2 Viruses

Viruses are self-replication programs that use files to infect and propagate [8]. Once a file is opened, the virus will activate within the system.

#### 3.1.3 Worms

A worm is similar to a virus because they both are self-replicating, but the worm does not require a file to allow it to propagate [8]. There are two main types of worms, mass-mailing worms and networkaware worms. Mass mailing worms use email as a means to infect other computers. Network-aware worms are a major problem for the Internet. A network-aware worm selects a target and once the worm accesses the target host, it can infect it by means of a Trojan or otherwise.

#### 3.1.4 Trojans

Trojans appear to be benign programs to the user, but will actually have some malicious purpose.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue I, January 2016 in association with
KARUR VELALAR COLLEGE OF ARTS AND SCIENCE FOR WOMEN, KARUR
Conference on Emerging Trends and Functional Applications of Computer Technology - 12th January 2016

Trojans usually carry some payload such as a virus[8].

### 3.1.5 Phishing

Phishing is an attempt to obtain confidential information from an individual, group, or organization [9]. Phishers trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information.

### 3.1.6 IP Spoofing Attacks

Spoofing means to have the address of the computer mirror the address of a trusted computer in order to gain access to other computers. The identity of the intruder is hidden by different means making detection and prevention difficult. With the current IP protocol technology, IPspoofed packets cannot be eliminated [8].

### 3.1.7 Denial of Service

Denial of Service is an attack when the system receiving too many requests cannot return communication with the requestors [9]. The system then consumes resources waiting for the handshake to complete. Eventually, the system cannot respond to any more requests rendering it without service.

## 4.CONCLUSION

Network security is an important field that is increasingly gaining attention as the internet expands. The security threats and internet protocol were analyzed to determine the necessary security technology. The security technology is mostly software based, but many common hardware devices are used. The current development in network security is not very impressive. Originally it was assumed that with the importance of the network security field, new approaches to security, both hardware and software, would be actively researched. It was a surprise to see most of the development taking place in the same technologies being currently used. The embedded security of the new internet protocol IPv6 may provide many benefits to internet users. Although some security issues were observed, the IPv6 internet protocol seems to evade many of the current popular attacks. Combined use of IPv6 and security tools such as firewalls, intrusion detection, and authentication mechanisms will prove effective in guarding intellectual property for the near future. The network security field may have to evolve more rapidly to deal with the threats further in the future.

**REFERENCES**

[1] Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously," *Computer*, vol.31, no.9, pp.24- 28, Sep 1998

[2] Kartalopoulos, S. V., "Differentiating Data Security and Network Security," *Communications, 2008. ICC '08. IEEE International Conference on*, pp.1469-1473, 19-23 May 2008

[3] "Security Overview," www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/security-guide/ch-sgs-ov.html.

[4] Molva, R., Institut Eurecom,"Internet Security Architecture," in *Computer Networks & ISDN Systems Journal*, vol. 31, pp. 787-804, April 199913

[5] Sotillo, S., East Carolina University, "IPv6 securityissues,"August 2006,www.infosecwriters.com/text_resources/pdf/IPv6_SSotillo.pdf.

[6] Andress J., "IPv6: the next internet protocol," April2005, ww.usenix.com/publications/login/2005-04/pdfs/andress0504.pdf.

[7] Warfield M., "Security Implications of IPv6," *InternetSecurity Systems White Paper*,documents.iss.net/whitepapers/IPv6.pdf

[8] 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

[9] Marin, G.A., "Network security basics," *Security & Privacy, IEEE* , vol.3, no.6, pp. 68-72, Nov.-Dec. 2005[10] "Internet History Timeline,"www3.baylor.edu/~Sharon_P_Johnson/etg/inthistory.htm.

[11] Landwehr, C.E.; Goldschlag, D.M., "Security issues in networks with Internet access," *Proceedings of the IEEE*, vol.85, no.12, pp.2034-2051, Dec 1997

[12] "Intranet." *Wikipedia, The Free Encyclopedia*. 23 Jun 2008, 10:43 UTC. Wikimedia Foundation, Inc. 2 Jul 2008 <http://en.wikipedia.org/w/index.php?title=Intranet&ol did=221174244>.

[13] "Virtual private network." *Wikipedia, The Free*

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue I, January 2016 in association with
KARUR VELALAR COLLEGE OF ARTS AND SCIENCE FOR WOMEN, KARUR
Conference on Emerging Trends and Functional Applications of Computer Technology - 12th January 2016

*Encyclopedia*. 30 Jun 2008, 19:32 UTC. Wikimedia Foundation, Inc. 2 Jul 2008 <http://en.wikipedia.org/w/index.php?title=Virtual_priv ate_network&oldid=222715612>.

[14] Tyson, J., "How Virtual private networks work," http://www.howstuffworks.com/vpn.htm .

[15] Al-Salqan, Y.Y., "Future trends in Internet security," *Distributed Computing Systems, 1997., Proceedings of the Sixth IEEE Computer Society Workshop on Future Trends of* , vol., no., pp.216-217, 29-31 Oct 1997