Peripheral Review and Analysis of Internet Network Security

Aru Okereke Eze and Okonba Brown
Department of Computer Engineering
Michael Okpara University of Agriculture, Umudike, Umuahia, Abia State, Nigeria

ABSTRACT: This paper is on the exploration of Internet Network security. With the advent of the internet, security became a major concern for computer users, organizations and the Military. The internet structure itself allows for many security threats to occur. Knowing the attack methods, the architecture of the internet when modified can reduce the possible attacks that can be sent across the network. The internet can be secured by the means of VPN, IPSec, Anti-Malware Software and scanners, Secure Socket Layer, intrusion-detection, security management, firewalls and cryptography mechanisms. The essence of this research is to forecast the future of internet network security.

KEYWORDS: Internet, Network, Security, VPN, IPSec, Firewalls, Cryptography

I. INTRODUCTION

With the advent of the Internet and new networking technologies, there is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide. Thus, Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet [1]. The internet is considered as data network consisting of computer-based routers, thus, information can be obtained by special programs such as “Trojan horses,” planted in the routers. In many cases today, the “vehicles” that hackers use to conduct illicit activities are “compromised” computers (sometimes called bots or botnets), usually owned by home Internet users and small businesses who are unaware that their computers have been “recruited”[2]. This research examined Internet Network Security and also suggested future recommendations for improvement.

II. BACKGROUND REVIEW

The birth of the internet takes place in 1969 when Advanced Research Projects Agency Network (ARPANet) is commissioned by the department of defense (DOD) for research in networking [3]. As more locations with computer joined the ARPANET, the usefulness of the network grew. The ARPANET becomes a high-speed digital post office as people use it to collaborate on research projects and discuss topics of various interests. In 1988, the ARPANET has its first network security incident, usually referred to as “the Morris worm” [3]. In 1989, the ARPANET officially becomes the internet and moved from a government research project to an operational network. During the 1980s, the hackers and crimes relating to computers were beginning to emerge. The 414 gang are raided by authorities after a nine-day cracking spree where they break into top-secret systems. The Computer Fraud and Abuse Act of 1986 was created because of Ian Murphy’s crime of stealing information from military computers [4]. In the 1990s, the internet began to become available to the public. The World Wide Web was born. Internet security has become a monumental problem. Franklin and McDaniel suggest that sophisticated hackers are stealing hundreds of millions of dollars each year, in addition to the inefficiency costs incurred by businesses and individuals [2, 4]. Further, these authors suggest that one well-designed attack could easily destroy a business’ operations or cripple an industry or the electricity grid for several days or weeks.

III. NETWORK SECURITY TOOL AND IMPLEMENTATION

To lessen the vulnerability of the internet network there are many products available. These tools are VPN, IPSec, Anti-Malware Software and scanners, Secure Socket Layer, intrusion-detection, security management and firewalls.

3.1 VPN (Virtual Private Network)

Virtual Private Network technology provides a way of protecting information being transmitted over the Internet, by allowing users to establish a virtual private “tunnel” to securely enter an internal network, accessing
resources, data and communications via an insecure network such as the Internet. This involves a combination of some or all of these features; namely: encryption, encapsulation, authorization, authentication, accounting, and spoofing [5].

![Figure 1: VPN Network Model.](image)

3.2 IPSec

IPSec enables a system to select and negotiate the required security protocols, algorithm(s) and secret keys to be used for the services requested. IPSec provides basic authentication, data integrity and encryption services to protect unauthorized viewing and modification of data. It makes use of two security protocols, AH (Authentication header) and ESP (Encapsulated Security Payload), for required services [6].

![Figure 2: IPsec connection.](image)

3.3 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 [7]. 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.

3.4 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 determining whether attacks are been launched. Some IDS systems just monitor and alert of an attack, whereas others try to block the attack.
3.5 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.

3.6 Encryption

Encryption provides privacy, which is called confidentiality. Both terms means that message can be transmitted without fear of being read by adversaries.

3.7 Cryptography

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

3.8 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.

IV. SUMMARY OF RECENT INTERNET NETWORK SECURITY THREATS, DATE AND ITS AREA OF ATTACK.

Below is the summary of recent threats, date and its area of attack [8].

<table>
<thead>
<tr>
<th>NAME OF THREAT</th>
<th>DATE DISCOVERED</th>
<th>TARGET SYSTEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Morris</td>
<td>Nov.2, 1988</td>
<td>VAX and SUN-3 running Blerckly UNIX</td>
</tr>
<tr>
<td>Melissa</td>
<td>Mar. 26, 1999</td>
<td>System running Unpatched Microsoft IIS</td>
</tr>
<tr>
<td>Code Red 1</td>
<td>Jun.19, 2001</td>
<td>Microsoft windows 2000 and other systems with IIS 4.0</td>
</tr>
<tr>
<td>Nimda</td>
<td>Sep.18, 2002</td>
<td>System running Microsoft window 95, 98, NT and 2000 with IIS</td>
</tr>
<tr>
<td>SQL Slammer</td>
<td>Jan.25, 2003</td>
<td>System running Microsoft window SQL</td>
</tr>
<tr>
<td>BOT Roster 1</td>
<td>Nov. 3, 2005</td>
<td>System running and network servers</td>
</tr>
<tr>
<td>Nyxem version D</td>
<td>Jan.2006</td>
<td>System running and network servers</td>
</tr>
<tr>
<td>Bot Roast 11</td>
<td>Nov.29, 2007</td>
<td>Microsoft windows 2000 and other systems with IIS 4.0</td>
</tr>
<tr>
<td>Conficker</td>
<td>Apr.4, 2009</td>
<td>System running and network servers</td>
</tr>
<tr>
<td>Stuxnet</td>
<td>Jun, 2010</td>
<td>System running Microsoft windows</td>
</tr>
<tr>
<td>Lulzraft</td>
<td>Apr., 2011</td>
<td>System running and network servers</td>
</tr>
<tr>
<td>FORTS3V3N</td>
<td>May 4, 2012</td>
<td>Network servers</td>
</tr>
<tr>
<td>iThug</td>
<td>Feb. 18, 2013</td>
<td>Microsoft windows and network servers</td>
</tr>
</tbody>
</table>

Table 1: Summary of recent internet network security threats, date and its area of attack

V. ANALYSIS AND CONCLUSION

From the result in Table 1, it is evident to say that the most prevalent internet security threats are Morris, Melissa, Nimda, SQL Slammer, BOT Roster Nyxem Version D, Bot Roast, Conficker, Stuxnet, Lulzraft, FORTS3v3N, iThug, while Virtual Private Network (VPN), IPSec, Anti-Malware Software and scanners, Secure Socket Layer, intrusion-detection, security management, firewalls, encryption and cryptography mechanisms has been identified as a veritable means of securing Internet Network Systems.

In this research, the implementation of Internet Network security has been reviewed with a combination of different security technique tools.
REFERENCES


Aru, Okereke Eze is a lecturer in the Department of Computer Engineering, Michael Okpara University of Agriculture, Umuahia, Abia State, Nigeria. His research Interests include Computational Intelligence, Security system design, Expert systems, Design of Microcontroller and Microprocessor based system, digital systems design using microcontrollers, Electronic and Communication Systems and other computer related subjects.

Okonba Brown is a Postgraduate Student of Electrical/Electronic Engineering, Michael Okpara University of Agriculture, Umuahia, Abia State, Nigeria. Her research interests include Electronic and Digital Systems, Data Communication, etc.