Survey on Internet Network Security Breaches as It Affects Computer Systems

Iroegbu. C .
Department of Electrical/Electronics Engineering,
Michael Okpara University of Agriculture,
Umudike, Abia State, Nigeria

Okonba. B. J.
Department of Electrical/Electronics Engineering,
Michael Okpara University of Agricuture,
Umudike, Abia State, Nigeria

***Abstract*— The purpose of this paper is to analyze Internet network Security breaches as it affects computer systems.**
As cost-effective and quick-to-deploy as the Internet is, there is one fundamental problem – security. Some of the "vehicles" that hackers use to conduct these illegitimate activities are Trojan horse programs , Backdoor and Remote administration , Unprotected Windows shares , Mobile Code , Cross-Site Scripting, Email Spoofing , Email-born Virus , Hidden File Extensions, Packet sniffing etc. To lessen the vulnerability of the internet network Security breaches, there are many products available. These tools include Encryption, IPSec, Identification and Access Anti-Malware Software, Secure Socket Layer, intrusion-detection, firewalls.

Keywords—Network; Internet; Computer; Security; Hackers.

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, therefore breach of data and information may lead to numerous legal disputes.
The three basic security concepts relevant to data (information) on the internet are confidentiality, integrity and availability. The concepts relating to the people who use that data (information) are authentication, authorization, and non-repudiation [1]. It is easy to gain unauthorized access to data in an insecure networked environment, and it is hard to catch the intruders. Confidentiality refers to preventing the disclosure of information to unauthorized individuals or systems. Data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle. Availability refers to the uninterrupted accessibility of the information systems required to store, process,

retrieve and transmit data and information [2]. When information is read or copied by some unauthorized person, the result is known as loss of confidentiality. Also when information is modified in unexpected ways, the result is known as loss of integrity, while when information is erased or become inaccessible, the result is loss of availability. To make information available to those who need it and who can be trusted with it, organizations use authentication and authorization. Authentication and authorization go hand in hand. Users must be authenticated before carrying out the activity they are authorized to perform. Security is strong when the means of authentication cannot later be refuted, the user cannot later deny that he or she performed the activity. This is known as non-repudiation [3].
This research has attempted to present various internet network security attacks and vulnerabilities as it affects computer systems. Those affected by such attacks include banks, insurance companies, government agencies, network service providers, utility companies, universities etc. The consequences of a break- in cover a broad range of possibilities: decrease in productivities, loss of money or staff man hour, loss of market opportunity, legal liability etc.

II. LITERACTURE REVIEW

The internet began as a concept in 1964, when the Rand Corporation of USA introduced the idea of Packet Switching Network (PSN) [4].
The physical implementation of the internet began in 1969 with a four-node network called the ARPANET, a project funded by Advanced Research Project Agency (ARPA) of the U.S Department of Defense .During this period, little thought was given to the security of data on the network[5].
In 1989, the ARPANET officially becomes the internet and a large amount of personal, commercial, military, and government information on networking infrastructures worldwide are linked together, thus Security issues becomes a concern . During the 1980s, hackers and crimes relating to computers were beginning to emerge. In 1982, the first computer virus appeared, Elk Cloner, displaying a short poem when an infected computer booted up for the 50th time. Since then, cybercriminals have created millions of viruses and other malware—email viruses, Trojans, Internet worms, spyware, keystroke loggers—some spreading worldwide and making headlines 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 were created because of Ian Murphy's crime of stealing information from military computers [6]. Today, the use of the World Wide Web and Web-related programming languages creates new

IJERT

opportunities for network attacks. Intruders can steal or tamper with information without touching a piece of paper or a photocopier. They can create new electronic files, run their own programs, and hide evidence of their unauthorized activities.

III. FORMS OF NETWORK ATTACKS

There are so many forms of network attacks, but here are some of the most common methods used by hackers to gain access to private computers [7]

A. Trojan horse programs:

Trojan horse programs are a common way for intruders to trick one into installing "back door" programs. These can allow intruders easy access to a computer without one's knowledge, change system configurations, or infect the computer with a computer virus.

B. Backdoor and Remote administration:

On windows computers, three tools commonly used by intruders to gain access to your computer are back Orifice, Netbus, and Subseven [8]. These back door or remote administration programs, once installed, allow other people to access and control your computer.

C. Denial of Service:

Another form of attack is called a denial-of- service attack. This type of attack causes a computer to crash or to become so busy processing data that one is unable to use it. In most cases, the latest patches will prevent the attack. It is important to note that in addition to being the target of a denial-service-attack, it is possible for one's computer to be used as a participant in a denial-of-service attack on another system.

D. Being an intermediary for another attack:

Intruders will frequently used compromised computers as launching pads for attacking other systems. An example of this is how distributed denial-of-service tools are used. The intruders install an "agent" (frequently through a Trojan horse program) that runs on the compromised computer awaiting further instructions. Then, when a number of agents are running from different computers, a single "handler" can instruct all of them to launch a denial-of-service attack on another system. Thus, the end target of the attack is not one's own computer, but someone else's-one's computer is just a convenient tool in a larger attack.

E. Unprotected Windows shares:

Unprotected Windows networking shares can be exploited by intruder in an automated way to place tools on large numbers of windows- based computers attached to the internet. Because site security on the internet is independent, a compromised computer not only creates problems for the computer's owner, but it is also a threat to other sites on the internet. The greater immediate risk to the internet community is the potentially large number of computers attached to the internet with unprotected Windows networking shares. Another threat includes malicious and destructive code, such as viruses or worms, which leverage unprotected Windows networking shares to propagate. One such example is the 911 worm. There is great potential for the emergency of other intruder tools that leverage unprotected Windows networking shares on a widespread basis.

F. Mobile Code (Java, JavaScript, and ActiveX):

There have been reports of problems with "mobile codes" (e.g. Java, JavaScript, and ActiveX). These are programming languages that let web developers write code that is executed by the web browser. Although the code is generally useful, it can be used by intruders to gather information (such as which web sites one visit) or to run malicious code on one's computer.

G. Cross-Site Scripting:

A malicious web developer may attach a script to something sent to a web site, such as a URL, an element in a form, or a database inquiry. Later, when the web site responds one's request, the malicious script is transferred to one's browser. One can potentially expose one's web browser to malicious scripts by following links in web pages, email messages, or newsgroup postings without knowing what they link to using interactive forms on an untrustworthy site viewing online discussion groups, forums, or other dynamically generated pages where users can post text containing HTML tags.

H. Email Spoofing:

Email "spoofing" is when an email message appears to have originated from one source when it actually was sent from another source. Email spoofing is often an attempt to trick the user into making a demanding statement or releasing sensitive information (such as passwords). Spoofed email can range from harmless pranks to social engineering ploys. Examples of the latter include email claiming to be from a system administrator requesting users to suspend their account if they do not comply email claiming to be from a person in authority requesting users to send them a copy of a password file or other sensitive information.

I. Email-born Virus:

Viruses and other types of malicious code are often spread as attachments to email messages [27]. The Melissa virus spread precisely because it originated from a familiar address and can be distributed in amusing or enticing programs. Many recent viruses use these social engineering techniques to spread.

J. Hidden File Extensions:

Windows operating systems contain an option to "Hide file extensions for known file types". The option is enabled by default. Multiple email-borne viruses are known to exploit hidden file extensions [9]. The first major attack that took advantage of a hidden file extension was the VBS/Love Letter worm, which contained an email attachment named "LOVE-LETTER-FOR-YOU.TXT.vbs". Other malicious programs have since incorporated similar naming schemes. Example include Down loader (MySis.avi.exe or

IJERT

QuickFlick.mpg.exe), VBS/Timofonica (TIMOFONICA.TXT.vbs). The files attached to the email messages sent by these viruses may appear to be harmless text (.txt), MPEG (.mpg), AVI (.avi) or other file types when in fact the file is a malicious script or executable (.vbs or .exe, for example).

K. Chat Client:
Internet chat applications, such as instant messaging applications and Internet Relay Chat (IRC) networks, provide a mechanism for information to be transmitted bi-directional between computers on the internet. Chat clients provide groups of individuals with the means to exchange dialog, web URLs, and in many cases, files of any type. Because many chat clients allow for the exchange of executable code, they present risks similar to those of email clients.

L. Packet sniffing:
A packet sniffer is programs that capture data from information packets as they travel over the network. That data may include user names, passwords, and proprietary information that travel over the network in clear text. With perhaps hundreds or thousands of passwords captured by the packet sniffer, intruders can launch widespread attacks on systems.

M. Disk Failures:
Availability is one of the three key elements of information security. Although all stored data can become unavailable-if the media it's stored on is physically damaged, destroyed, or lost-data stored on hard disks is at higher risk due to mechanical nature of the device. Hard disk crashes are a common cause of data loss on personal computers.

N. Power failure and surges:
Powers problems (surges, blackouts, and brown-outs) can cause physical damage to a computer, inducing a hard disk crash or otherwise harming the electronic components of the computer.

O. Physical theft;
Physical theft of a computer, of cause, result in the loss of confidentiality and availability, and (assuming the computer is ever recovered) makes the integrity of the data stored on the disk suspect.

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

Below is the summary of recent threats, year and its area of attack.

Table 1: Threats, year and areas of attack

NAME OF THREAT	DATE DISCOVERED	TARGET SYSTEM
Elk Cloner	1982	Apple II operating system.
EGABTR Trojan horse	1985	Files on the hard disk
Brain	1986	Floppy disk
Christmas tree worm	1987	User's address book.
Morris	Nov.2, 1988	VAX and SUN-3 running Blerckly UNIX
AIDS Trojan horse	1989	Computer's hard disk
polymorphic virus	1991	
Michelangelo panic	March 6 1992	Disks and PCs,
Hoax	1994	Hard drive
macro" virus,	1995	Microsoft Word.
Chernobyl	1998	BIOS
Melissa	Mar. 26, 1999	System running Unpatched Microsoft IIS
Palm virus	2000	Palm operating system
Code Red 1	Jun.19, 2001	Microsoft windows 2000 and other systems with IIS 4.0
Nimda	Sep.18, 2002	System running Microsoft window 95, 98, NT and 2000 with IIS
SQL Slammer	Jan.25, 2003	System running Microsoft window SQL
BOT Roster 1	Nov. 3, 2005	System running

IJERT

		and network servers
Nyxem version D	Jan.2006	System running and network servers
Bot Roast 11	Nov.29, 2007	Microsoft windows 2000 and other systems with IIS 4.0
Conficker	Apr.4, 2009	System running and network servers
Stuxnet	Jun, 2010	System running Microsoft windows
Lulzraft	Apr., 2011	System running and network servers
FORTS3V3N	May 4, 2012	Network servers
iThug	Feb. 18, 2013	Microsoft windows and network servers

V. PREVENTIVE TOOLS

To lessen the vulnerability of the internet network, some of the available preventive tools include:

A. Identification and Access:

The system uses this technique to verify that you have legitimate right and access. Depending on the techniques employed, the system uses one of the following or a combination to authenticate your identity. It uses what you have such as cards, keys, signatures or badges built into chips to identify you to the system. Also, the system can use what you know viz: pins, passwords and digital signatures to grant you access it can also use what you are that is your physical traits to identify and grant you access to the system.

B. Encryption:

This is a method of altering data so that it is not useable unless one change is undone. An example is the "Pretty Good Privacy" (PGP) a computer program written for encrypting computer massages that is putting them into secret codes. When data is encrypted, it is then scrambled to descript them, you must unscramble it.

C. Protection of Software and Data:

Corporate organizations train and educate their workers on the need for how to back up their disks and protect them against viruses and worms. The protective security procedure in this category include: control of access, firewalls, audit control and people control.

D. IPV6 Security and firewalling:

IP security (IPSec) specifications have been implemented widely with IPV6 between communicating hosts on local networks or an virtual private networks (VPNs), in which the internet serves as the communication channel between two private network. The IP security (IP Sec) extension leaders, IPV6 includes security features that provide cryptographic security services at the network layer which include; authentications, integrity, confidentiality, access control, Security Association (SA), security association database (SAD), security parameter index (SPI), Security policy database (SPD).

VI. CONCLUSION

Security which is primary to life and property is a method of protecting our information against disasters, system failure, and unauthorized access. After all, "prevention is better than cure". This research work has examined internet network security breaches as it affects computer systems. It has exploded various attacks and vulnerabilities of data over the internet network. Some of the "vehicles" that hackers use to conduct their illegitimate activities are Trojan horse programs, Backdoor and Remote administration , Unprotected Windows shares , Mobile Code , Cross-Site Scripting , Email Spoofing , Email-born Virus , Hidden File Extensions, Packet sniffing etc.

IJERT

REFERENCES

[1] Risk Management Guide for Information Technology Systems,NIST, US Deptt. Of Commerce
[2] ISACA, 2008, *www.isaca.org*
[3] CERT coordination center, CERT advisories and other security information, CERT/CC, Pittsburgh, P.A. Available on line: http://www.cert.org.
[4] Chapman, D.B. and Zwicky, E.D. Building Internet Firewall, O' Reilly & Associates, Sebastopol, C.A, 199 5
[5] "Internet History Timeline," www3.baylor.edu/~Sharon_P_Johnson/etg/inthistory.h tm.
[6] McDaniel, P. (2006, December 6). *Physical and digital convergence: Where the Internet is the enemy.* Eighth International Conference on Information and Communications Security. Retrieved April 24, 2009, at http://discovery.csc.ncsu.edu/ICICS06/Keynote McDaniel.html
[7] http://www.cert.org/adversories/CA-2014-05.html
[8] http://www.cert.org/archive/pdf/DOS-trends.pdf
[9] http://www.cert.org/tec-tips/malicious-code-FAQ.htm

BIOGRAPHY

Iroegbu Chibuisi received his B.Eng. degree in Electrical and Electronics Engineering from Michael Okpara University of Agriculture, (MOUAU) Umudike, Abia State Nigeria in 2010, and currently doing a Master of Engineering degree in Electronics and Communication Engineering, Michael Okpara University of Agriculture, (MOUAU) Umudike, Abia State Nigeria. He is a member of International Association of Engineers. His research interests are in the fields of wireless sensor networks, Electronic and Communication Systems design, Security system design, Expert systems and Artificial Intelligence, Design of Microcontroller based systems, Channel coding etc.

Okonba Brown .J received his B.Eng. degree in Electrical and Electronics Engineering from University of Portharcourt, Rivers State Nigeria in 2002, and currently doing a Master of Engineering degree in Electronics and Communication Engineering, Michael Okpara University of Agriculture, (MOUAU) Umudike, Abia State Nigeria. He is a member of Nigerian Society Engineers. His research interests are in the fields of, Electronic and Communication Systems design, Security system design, Network design etc.

IJERT