iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** XII **Month of publication:** December 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Virtual Private Network Security

Nnochiri, I.U., M. Eng.,
Department of computer Science, Michael Okpara University of Agriculture, Umudike, Abia State, Nigeria

Abstract -This research is on the implementation of Virtual Private Network (VPN). Owing to the demand at the present time to connect to internal networks from distant locations, the significant of establishing safe links across the network became paramount. Workers frequently require connecting to internal private networks over the Internet which is by nature insecure; accordingly, security becomes a chief thought. Virtual Private Network (VPN) technology provides a way of protecting information being transmitted over the Internet, by allowing users to set up a virtual private 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.

Keywords: Internet Virtual Private Network, Authorization, Authentication, Encryption.

I. INTRODUCTION

As the Internet became more and more accessible and bandwidth capacities grew, companies began to put their Intranets onto the web and create what are now known as Extranets to link internal and external users [1]. However, as cost-effective and quick-to-deploy as the Internet is, there is one fundamental problem – security. Security which is primary to life and property is a method of protecting our information against disasters, system failure, and unauthorized access. Today, Virtual Private Network (VPN) has overcome the security factor in the network using special tunneling protocols and complex encryption procedures, data integrity and privacy is achieved. Virtual Private Network (VPN) is a standard term used to illustrate a communication network that uses any mixture of technologies to secure a connection tunnelled through an otherwise unsecured or untrusted network. It uses public network paths but maintains the security and protection of private networks. Instead of using a dedicated connection, such as leased line, a "virtual" connection is made between geographically dispersed users and networks over a shared or public network, like the Internet. Data is transmitted as if it were passing through private connections [2]. Virtual Private Network employs encryption, encapsulation, authentication, authorization, and firewalls among other techniques.

II. BACKGROUND INFORMATION

As ventures dips into e-commerce, it became obvious that the internet was the convenient and cost valuable way to bond with clients and associates. The internet began as a concept in 1964, when the Rand Corporation of USA introduced the idea of Packet Switching Network (PSN). A PSN divides a message into packets of fixed size and routes them to the destination [3]. An example of this is the X.25 network. 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. In 1984, the ARPANET was shutdown but the remaining nodes and subnets connected to the network of computer world-wide remained, thus causing the internet to become a public network. And since it is a public network, there is no security on it [4]. One of the ways to achieve the needed security is the implementation of the Virtual Private Network, which employs encryption, encapsulation, authentication, authorization, and firewalls among other techniques to ward-off intruders by blocking or disallowing all traffic except messages from designated places or for a designated type using a router [5].

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 [6]

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 [7]. 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 [8].

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. 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 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 bidirectional 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. DESIGN METHODOLOGY, SIMULATION AND TESTING

Figure 1 shows a generalized Model of a VPN.

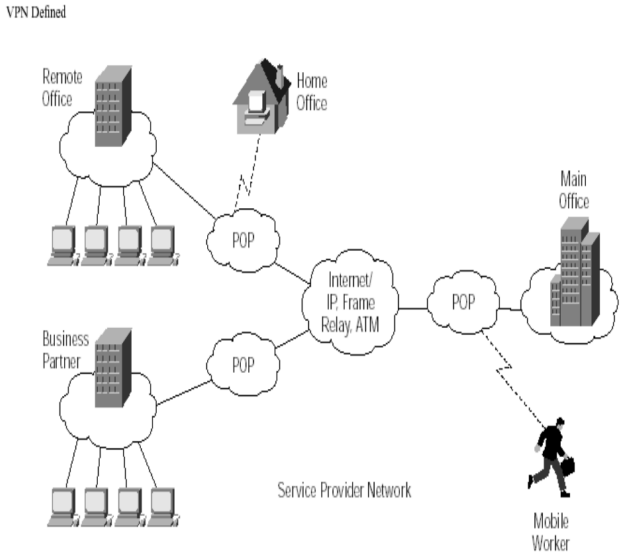


Fig-1: A VPN Model

Figure 2 shows an X.25 Network model similar to one on which the data to be secured by this research runs.

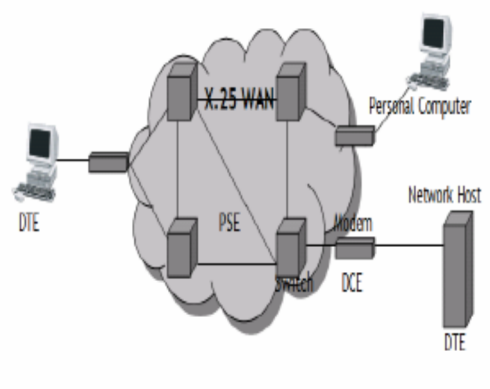


Fig-2: X25 Network Model

X.25 is an ITU-T protocol standard model for WAN communications designed to operate effectively regardless of the type of systems connected to the network and used in the public switched networks (PSNs) of common carriers, such as the telephone companies. Its devices fall into three categories: Data Circuit-terminating Equipment (DCE), Data Terminal Equipment (DTE), and Packet-Switching Exchanges (PSE). The VPN encryption program developed in this research was installed on the DTE at both ends (i.e. sender and receiver's personal computers). Data circuit-terminating equipments are communications devices, such as modems and packet switches that provide the interface between data terminal equipment devices and packet-switching exchanges, and are generally located in the carrier's facilities Packet-switching exchanges are switches that compose the bulk of the carrier's network. They transfer data from one DTE device to another through the X.25 public switched network.

A. 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.

B. Authentication

Authentication proves the sender's identity. If we get a message claiming to be from someone, we want to be certain that it is not really coming from someone else; we apply the concept of authentication. A common technique for authentication is for each side to "challenge" the other side by sending a random number. The challenger decrypted the returned value and if the decrypted value matched the original random number, the challenged party was treated as authentic. There are many forms of authentication; passwords authentication, authentication card, biometric authentication etc.

C. Authorization

Authorization allows the network to permit or deny a person access to a particular database or services.

V. RESULT ANAYSIS AND DISCUSSIONS

The program challenged a user to provide user name and password for authentication and authorization purposes. To maintain responsibility for message validity, the recipient of the message would need to decrypt the document using the sender's private key. If the encryption codes are the same when compared, the message is decrypted. After a total of three unsuccessful trials, the intending user is completely logged out and the VPN system platform is automatically exited, while for a successful login, the VPN main window menu is displayed, availing the user the opportunity to:

A. Compose a message
B. Checking his mail
C. Create and delete user accounts
D. Change user's passwords
E. Exit the window.

VI. CONCLUSIONS

This research work has examined internet network security. It has exploded various attacks and vulnerabilities of data over the internet network. As the Internet offers no security for the data sent across it, the need of establishing a secure links across the network becomes enormous.

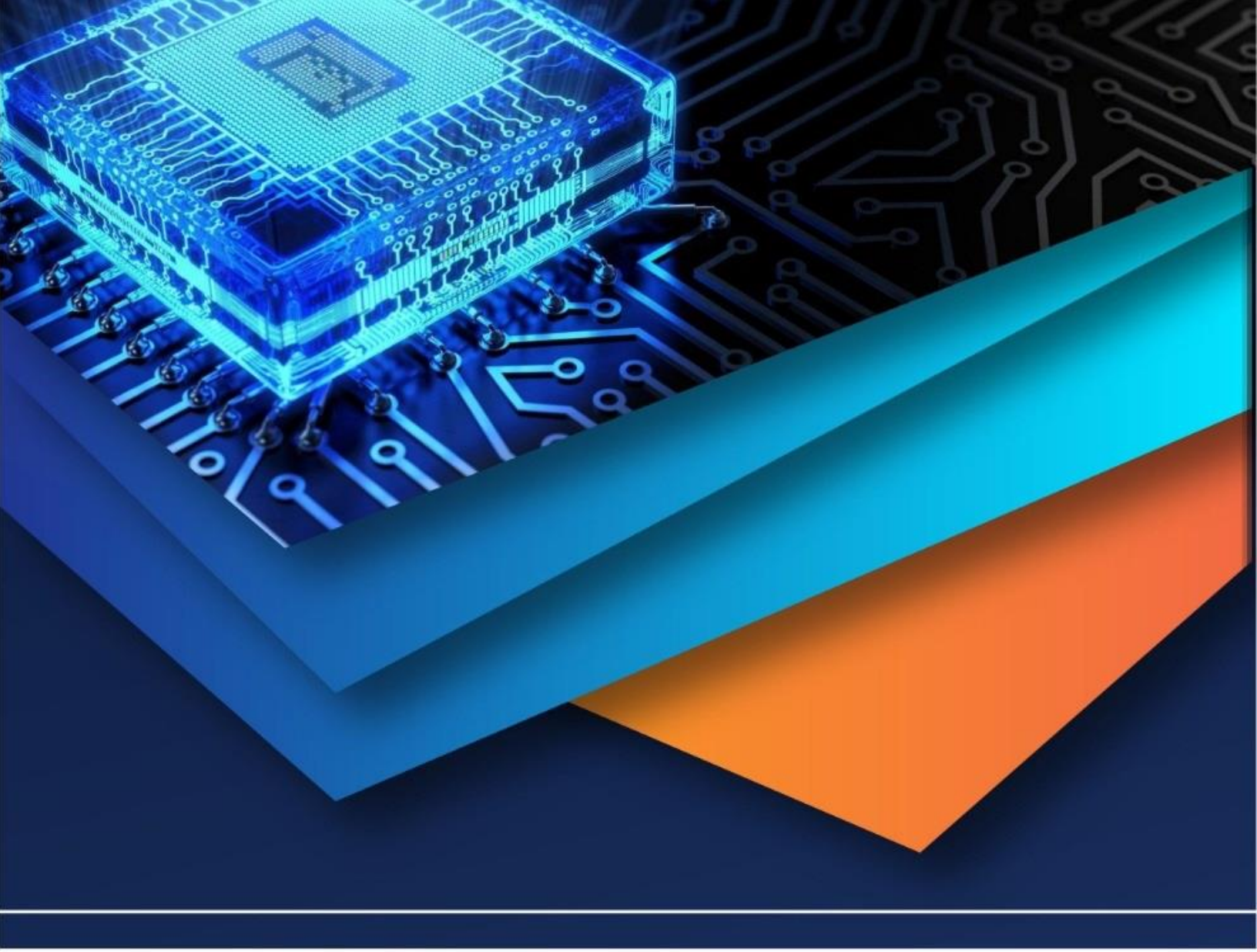
VPN provides a means of accessing a secure, private, internal network over insecure public networks such as the Internet.

REFERENCES

[1]. Ryan, Jerry. 2001. "A Practical Guide to the Right VPN Solution". The Applied Technologies Group. pp.5, 20, 21.
[2].http://cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/vpn.h tm
[3]. CISCO. 2000. "Internetworking Technologies Handbook." pp. 1-2.
[4]. BNET. 2006. Louisville, KY. http://www.techguide.com
[5]. AXENT Technologies, Inc. 1998. "Everything You Need to Know About Network Security.
[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 November 11, 2014, at http://discovery.csc.ncsu.edu/ICICS06/Keynote McDaniel.html
[7] http://www.cert.org/archive/pdf/DOS-trends.pdf
[8]. Aru, O., Iroegbu C., and Enyenihi, H. 'Analysis of Data Security Approach for Digital Computers'. International Journal of Modern Engineering Research, Vol. 3, issue. 6, Nov - Dec. 2013 pp-3449-3451
[9] http://www.cert.org/tec-tips/malicious-code-FAQ.htm

ABOUT THE AUTHORS

Engr. (Mrs) Ifeoma U. Nnochiri is a lecturer in the department of computer Science, Michael Okpara University of Agriculture Umudike, Abia State, Nigeria. She holds a Bachelor degree (B.Eng) and Master's degree (M.Eng) in Computer Science & Engineering. More so, she is at the point of completing her Doctorate degree (PhD) in the same field. Her areas of interest include artificial intelligence, fuzzy logic and neural network, Embedded Systems etc.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY