VIRTUAL PRIVATE NETWORK: A VERITABLE TOOL FOR NETWORK SECURITY

Ekwe O. A[1], Iroegbu C[2]

[1]*Department of Electrical/Electronics Engineering, Mouau, Abia, Nigeria*
[2]*Department of Electrical/Electronics Engineering, Mouau, Abia, Nigeria*

Abstract

Due to the increase demand nowadays to connect to internal networks from distant locations, the important of establishing secure links across the network cannot be overemphasized. Employees often need to connect to internal private networks over the Internet which is by nature insecure, thus, security becomes a major consideration. This research is on the implementation of Virtual Private Network (VPN). Virtual Private Network(VPN) technology provides a way of protecting information being transmitted over the Internet, by allowing users to establish 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: Virtual *Private Network, Authorization, Authentication, Encryption, Internet.*

----------***----------

1. 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. But 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, and the new connection produces what seems to be a dedicated point-to point connection [2].

Virtual Private Network (VPN) is a generic term used to describe a communication network that uses any combination 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 [3].

Virtual Private Network employs encryption, encapsulation, authentication, authorization, and firewalls among other techniques. VPN has become the defacto standard for secure Internet communications, providing traffic integrity, confidentiality and authentication

2. BACKGROUND INFORMATION

As enterprises dabbled in e-commerce, it became clear that the internet was the practical and cost effective way to connect with customers and partners. The concept of connecting with external users came to be known as extranet. 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 [5]. 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 [6].

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 (as in firewall) using a router[7].

3. DESIGN METHODOLOGY, SIMULATION AND TESTING

Figure 1 shows a generalized Model of a VPN.

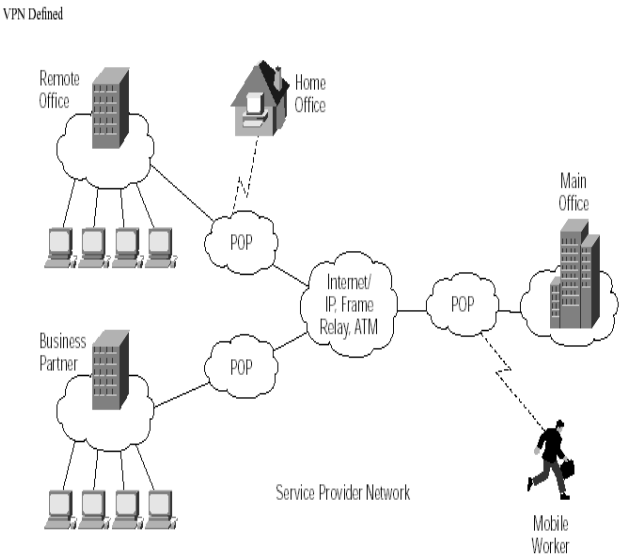

Fig-1: A VPN Model [3]

Figure 2 illustrates how to set up a VPN Tunnel between Gateways

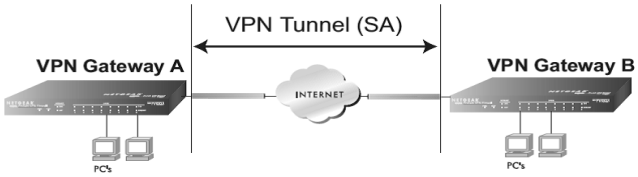

Fig-2: Setting Up a VPN Tunnel between Gateways

Figure 3 shows an X.25 Network model similar to one on which the data to be secured by this research runs.

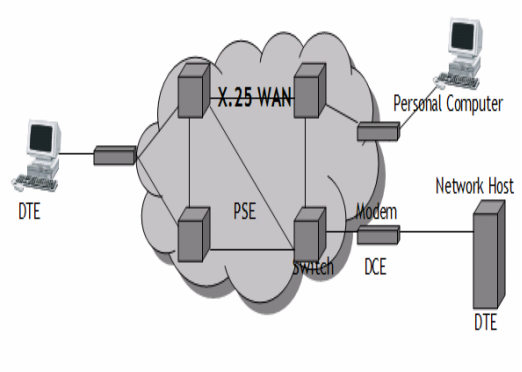

Fig-3: X25 Network Model

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 [6]. 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.

3.1 The Flowchart for the VPN Implementation

Figure 4 shows the flowchart for the VPN implementation.

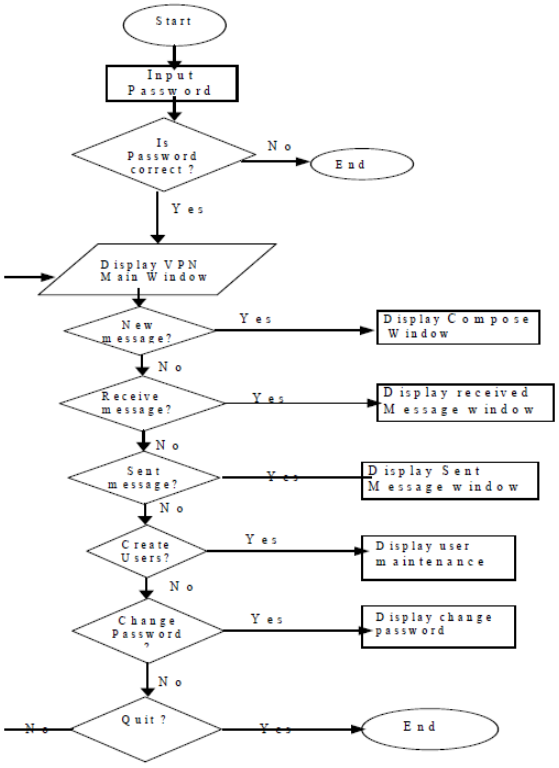

Fig-4: Flowchart of VPN implementation.

The message to be encrypted was juggled in such a way that the character at every sixth count in the message was used in conjunction with every second character in the ASCII count to form an encrypted version of the message. The design could take as much as 256 different input characters in the message

construction. The decryption process involved the reversal of the encryption process.

3.2 Symmetrical or Private Keys

The same key was used both to encrypt and to decrypt information, hence called a symmetrical key. This is the method adopted in this work. Symmetrical keys require users of a VPN to share the same key at each end of the connection. Because the key is shared, symmetrical keys are frequently referred to as shared secrets. Symmetric key encryption has a single key that is used by both communication partners. Figure 5 shows a symmetric key encryption and decryption method.

- When party A sends to party B, party A encrypts with the single symmetric key and party b decrypts with the same key.
- When party B transmits to party A, in turn party B encrypts with the single symmetric key and also party A decrypts with the same key.

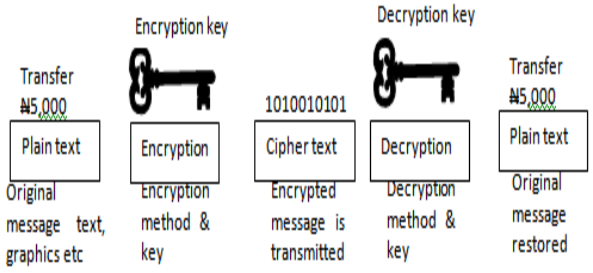

Fig -5: Symmetric key encryption and decryption [8]

3.3 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.

3.4 Authorization

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

4. RESULT ANAYSIS AND DISCUSSIONS

The result of a sample obtained from the Virtual Private Network implementation is shown in Figure 6 below.

Fig-6: Result obtained from the implementation of Virtual Private Network

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:

- Compose a message
- Checking his mail
- Create and delete user accounts
- Change user's passwords
- Exit the window.

5. CONCLUSIONS

Since the Internet offers no security for the data sent across it, the need of establishing a secure links across the network becomes inestimable. VPN provides a means of accessing a secure, private, internal network over insecure public networks such as the Internet. To achieve data security on the Internet, a combination of techniques namely: encryption, encapsulation, authorization, authentication, accounting, and spoofing were implemented in the Virtual Private Network.

REFERENCES

[1]. Ryan, Jerry. 2001. "A Practical Guide to the Right VPN Solution". The Applied Technologies Group. pp.5, 20, 21.
[2]. AXENT Technologies, Inc. 1998. "Everything You Need to Know AboutNetwork Security. Pg21.
[3].http://cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/vpn.htm
[4]. Chapman, D.B. and Zwicky, E.D. Building Internet Firewall, O' Reilly &
Associates, Sebastopol, C.A, 1995
[5]. CISCO. 2000. "Internetworking Technologies Handbook." pp. 1-2.
[6]. BNET. 2006. Louisville, KY. http://www.techguide.com

[7]. AXENT Technologies, Inc. 1998. "Everything You Need to Know About Network Security.
[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

BIOGRAPHIES

Engr. Ogbonna A. Ekwe is a highly motivated Electronic Engineer with a bias in Communications. He obtained his Bachelor of Engineering (B.Eng.) degree in Electronics Engineering at the University of Nigeria, Nsukka in 2005, and a Master's Degree in Electronic Communications and Computer Engineering from University of Nottingham, United Kingdom in 2011. He possesses many years of experience in different work environments with excellent team leadership qualities. Engr. Ekwe, O. A is presently lecturing in the department of Electrical/Electronic Engineering, Michael Okpara University of Agriculture, Umudike, Abia State, Nigeria. His research interest are in the areas of Interference management for cellular communication, Communication techniques for next generation cellular systems, Channel fading mitigation for fixed and mobile wireless communication systems, etc**.**

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