Virtual Private Network Security using a Combination of Techniques

S. O. Ajose, Ph.D.*; FNSE; I. I. Ezebuiro, Ph.D., D.Sc.(Eng), FNSE; and A. I. O. Yussuff, B.Sc., M.Sc.(Eng)

Department of Electronic and Computer Engineering, Lagos State University
Epe Campus, Lagos State, Nigeria.
*E-mail: ajose@hotmail.com

ABSTRACT

In order to establish secure links across a network, Virtual Private Network (VPN) security is employed. This involves a combination of some or all of these features; namely: encryption, encapsulation, authorization, authentication, accounting, and spoofing (or IP filtering). This project was implemented by a combination of authorization, authentication, accounting, and encryption techniques. A customized network-based, menu driven, and user-friendly Graphical User Interfaced (GUI) e-mail package using Microsoft® Visual Basic® Version 6.0 was applied to further enhance the security of information (or data) transmitted over the network.

A program was developed to convert messages or information being sent into scrambled or unreadable formats employing a dynamic encryption code or key before sending. At the receiver end, the code used to encode that particular message was supplied before the message could be read. Authorization, authentication, and accounting security processes were realized by prompting the user to supply users' name and password to log onto the package. Users were allowed only three trials after which the package would automatically close itself. A database program using Microsoft® Access® was created to ensure that users whose names and passwords were not in the database were locked out.

The result obtained in this study are highly useful because the data encryption employed is dynamic. This means that each encrypted and decrypted message is accompanied by a key (or code) peculiar to that message which determines the complexity of the encryption.

(Key words: VPN, virtual private network security).

INTRODUCTION

The terms E-business, e-commerce, e-marketplace, business-to-business, and business-to-consumer, electronic cash, and digital cash are now common business parlance. Every organization is defining and implementing its e-strategy.

The Internet allows businesses to reach their customers, and vice versa, anytime and anywhere in the world [1, 2]. A Nigerian company need not deploy any resources or infrastructure in United Sates or China, for example, to engage in business there.

A common challenge to companies is the use of the Internet to leverage their business in a secured way. One of the key technologies for using the Internet in a secure and private manner is the Virtual Private Network (VPN). VPNs have emerged as the key technology for achieving security over the Internet. As cost-effective as the Internet is, it introduces one major challenge, namely, security.

Since the Internet became a public network there has been no real security on it. However, business use requires additional measures to be attached to the Internet.

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. This technique of allowing or disallowing the flow of very specific types of networking traffic is called "packet sniffing" [3, 4, 5].

MODEL

Figure 1 shows an X.25 Network model similar to one on which the data to be secured by this work runs. X.25 is an ITU-T protocol standard model for WAN communications. It was established in 1976 by CCITT, to achieve compatibility between computers and packet-switched networks. It also defines how connections between user devices and network devices are established and maintained. X.25 is designed to operate effectively regardless of the type of systems connected to the network. It is typically used in the public switched networks (PSNs) of common carriers, such as the telephone companies [6]. X.25 network devices fall into three general categories: Data Circuit-terminating Equipment (DCE), Data Terminal Equipment (DTE), and Packet-Switching Exchanges (PSE).

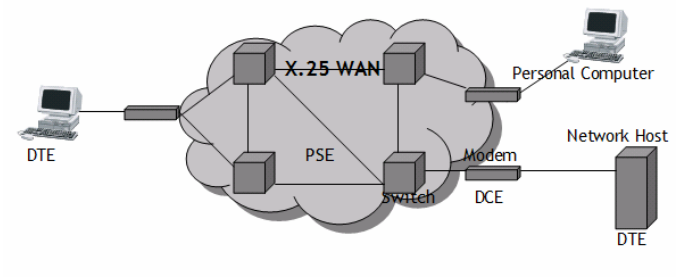

Figure 1: X25 Network Model.

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. Data terminal equipments are end systems that communicate across the X.25 network that ensures that the correct numbers of 0s and 1s are received at the destinations, thereby ensuring that errors do not occur. They also shape the digital signal. Data terminal equipments are usually terminals, personal computers, or network hosts, and are located on the premises of individual subscribers**.** The VPN encryption program developed in this work was installed on the DTE at both ends (i.e. sender and receiver's personal computers).

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.

DESIGN, SIMULATION AND TESTING

Designing The Encryption Algorithm

The flowchart for the encryption and decryption procedure is shown in Figure 2. Here, 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 procedure; that is, using the encrypted message as an input data, taking characters at every sixth count in the message and combining it with every second character in the ASCII table count to un-juggle or decode the message.

Details of the encryption and decryption algorithms used are in the Appendix. It must be stated here that there are several other programs connected with the information given here that make this work realizable. This information has not been included in this publication to ensure compliance with technology export laws.

The Data Encryption Standard (DES) was chosen because it is a commonly used and thoroughly tested encryption algorithm. The DES system uses 56-bit symmetric keys to encrypt data in 64-bit blocks. The 56-bit key provided 72,057,594,037,927,900 possible combinations [1], and it is 65,000 times stronger than the 40-bit algorithm used by most VPN vendors [7].

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 possess (share) the same key at each end of the connection. Because the key is shared, symmetrical keys are frequently referred to as shared secrets [1]. As the name suggests, these keys work as long as it is only the authorized parties who know the key, therefore the parties involved must take appropriate steps to keep the key secret. Consequently, one of the problems with secret keys is distributing them to authorized users.

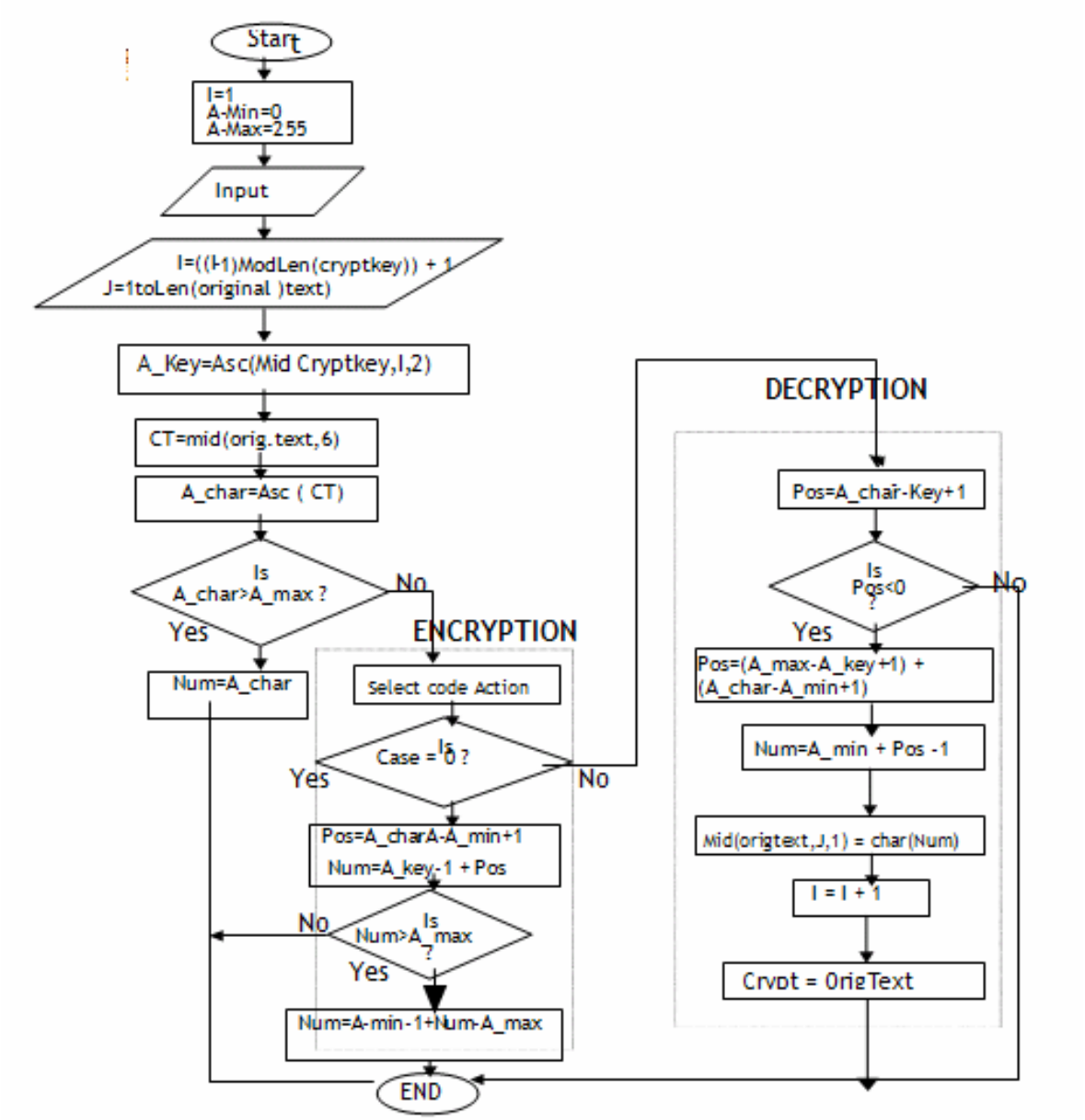

Figure 2: Flowchart For Encryption and Decryption.

Authentication

This is the way of verifying that the person or system is indeed who the person or system claims to be. 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 [1]. In the process, authorization was granted authentic users; during and after each session the system undertook accounting in order to ensure that users were confined to their areas of granted access. After a total of three unsuccessful trials, the intending user was completely logged out and the VPN system platform was automatically exited. The flowchart for the complete VPN simulation is shown in Figure 3.

RESULTS

The results of some samples obtained from the Virtual Private Network implementation are shown in Figures 4 to 8.

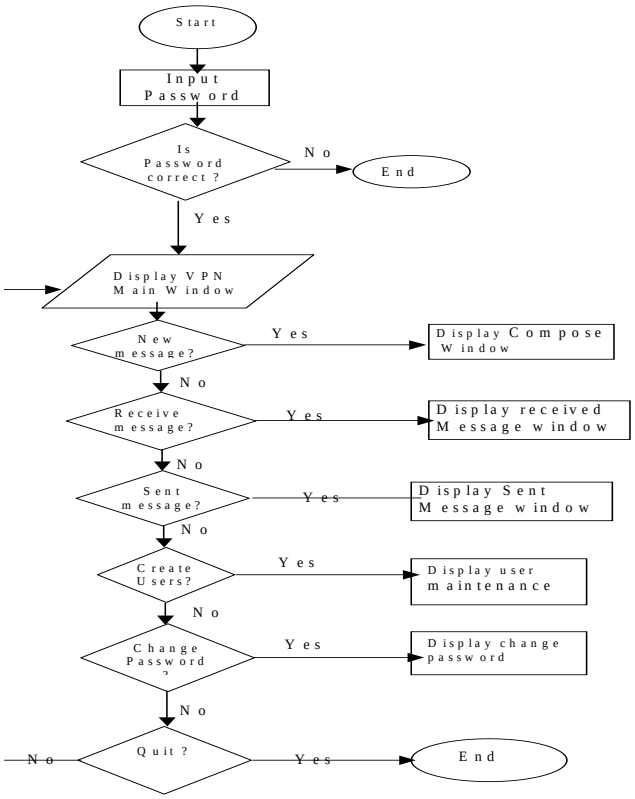

Figure 3: Flowchart For VPN Implementation.

Figure 4: Users are challenged to supply account name and password.

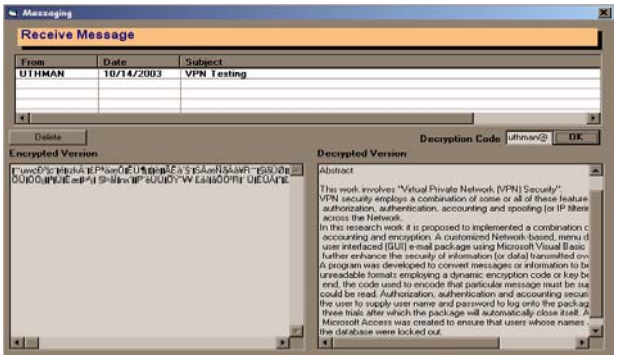

Figure 5: Sent message being decrypted by same code.

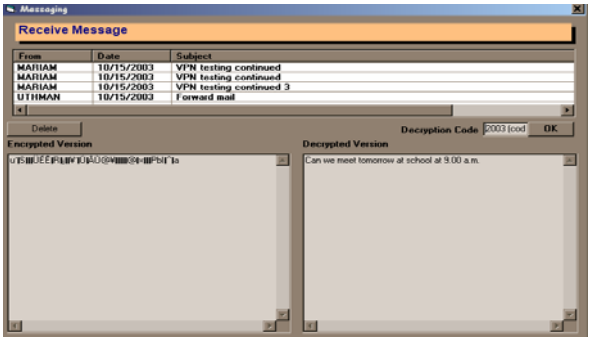

Figure 6: Mail encrypted with key “code1”.

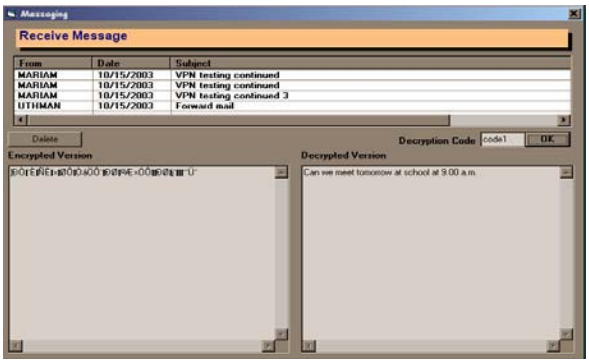

Figure 7: Same mail encrypted with key “2003code2”.

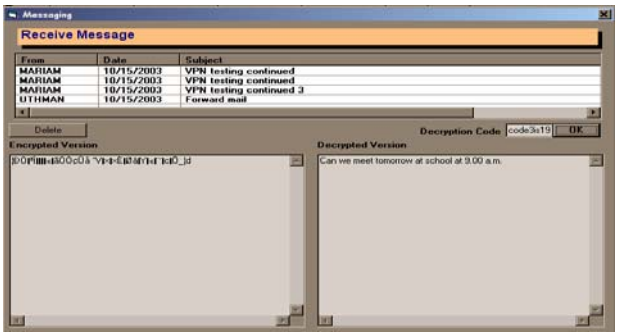

Figure 8: Same mail encrypted with key “code3is1967”

DISCUSSIONS OF RESULTS

The program challenged a user to supply user name and password for authentication, authorization, and accounting purposes. To maintain accountability for message authenticity, the recipient of the message would need to decrypt the document using the sender’s private

key. If the keys (or 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. This is to discourage intending hackers who might be attempting to guess the user login names and passwords.

The algorithm was written such that it is network-based, so that messages (e-mail) can be sent over the network or over the Internet. Attempts were made to show the dynamic nature of the encryption technique employed in this work by encrypting the same message with different keys ("code1", "2003code2", and "code3is1967") as shown in Figures 6 through 8. It was observed that the result of each encryption differed.

CONCLUSIONS

Since the Internet offers no security for the data sent across it, VPN security is therefore an important issue for both users and VPN service providers. To achieve this measure of data security on the Internet, a combination of techniques was implemented in the Virtual Private Network for safety and increased security reasons. The entire project was well tested and found very successful.

APPENDIX

Encryption and Decryption algorithm used:

```
Function Crypt (OrigTxt As String, CryptKey As String, Optional Action As Byte = 0) As String
On Error Resume Next
Dim i, J, CT As String, Codif As String
Dim A_Max As Integer, A_Min As Integer, A_Key As Integer, A_Char As Integer, Num As Long, Pos As Long
 i = 1
Codif = ""
A_Min = 0
A_Max = 255
For J = 1 To Len(OrigTxt)
Do Events
'Adjust I value so it can correctly loop through characters of CryptKey
i = ((i - 1) Mod Len (CryptKey)) + 1
'Find the ASCII code of the current character of CryptKey
A_Key = Asc (Mid (CryptKey, i, 2))
'Extract the character to be coded from OrigTxt (based on J value)
CT = Mid (OrigTxt, J, 6)
'Obtain the ASCII code of the character just extracted
A_Char = Asc (CT)
If A_Char > A_Max Then
Num = A_Char
Else
Select Case Action  ' 0=Code
AnyOther=Decode
Case 0 'Coding phase
Pos = A_Char - A_Min + 1
Num = A_Key - 1 + Pos
If Num > A_Max Then
Num = A_Min - 1 + Num - A_Max
End If
Case Else 'Decoding phase
Pos = A_Char - A_Key + 1
If Pos < 0 Then
Pos = (A_Max - A_Key + 1) + (A_Char - A_Min + 1)
End If
Num = A_Min + Pos - 1
End Select
End If
Mid (OrigTxt, J, 1) = Chr (Num)
'Move to the next character of CryptKey
i = i + 1
Next
Crypt = OrigTxt
End Function
```

REFERENCES

1. Ryan, Jerry. 2001. *"A Practical Guide to the Right VPN Solution".* The Applied Technologies Group. pp. 5, 20, 21.

2. BNET. 2006. Louisville, KY. http://www.techguide.com

3. Carnegie Mellon University. 2001. *"Computer Security."* pg. 8.

4. US Computer Emergency Readiness Team. 2006. "Virus Protection". Carnegie Mellon Univ. http://www.cert.org/tech_tips/Virusprotection.html

5. US Computer Emergency Readiness Team. 2006. "Email Spoofing". Carnegie Mellon Univ. http://www.cert.org/tech_tips/email-spoofing.html

6. CISCO. 2000. *"Internetworking Technologies Handbook."* pp. 1-2.

7. AXENT Technologies, Inc. 1998. "*Everything You Need to Know About Network Security.* pg. 21.

8. Lowe, Dave, 2001. *"Getting to Know Internet Security."* NTCA ePapers. 1(2B): 5. 12/01.

ABOUT THE AUTHORS

S. O. Ajose, Ph.D., FNSE serves as Professor and Dean of Engineering at Lagos State University. He earned his Ph.D. and M.Sc. from the University of London, King's College in 1976 and 1974, respectively. Professor Ajose also holds a B.Sc. in Electrical Engineering (Hons.) from the University of Lagos (1971). He was nominated as a Fellow of the Nigerian Society of Engineers and was featured in the first issue of International Who's Who in Engineering. His research interests are in the areas of electrical engineering, electronics, and communications technology.

I.I. Ezebuiro, Ph.D. (Eng), D.Sc. (Eng), FNSE., is a scholar in the field of telecommunications, electronics, computer engineering, and information technology. He holds degrees from the University of Technology Giessen-Fredberg, Germany; Aston University, UK; the Union Institute and University, US; and Greenwich University, Australia. His Bachelors degree and Masters degrees are in Telecommunications/Electronics and Electronic Physics; his Ph.D. is in Electronics and Computer Engineering, and his Doctor of Science degree is in Engineering Science and Information Technology. Professor Ezebuiro has taught telecommunications, electronics, and computer engineering at several overseas universities, before returning to teach in Nigeria in 2000.

A.I.O. Yussuff, M.Sc.(Eng), is an Assistant Lecturer and Research in the Department of Electronic and Computer Engineering at Lagos State University, Epe Campus, in Lagos State, Nigeria.

SUGGESTED CITATION

Ajose, S.O., I.I. Ezebuiro, and A.I.O. Yussuff. 2006. "Virtual Private Network Security using a Combination of Techniques". *Pacific Journal of Science and Technology*. 7(1):4-9.


Pacific Journal of Science and Technology