Asian Journal of Information Technology 6 (7): 785-792, 2007
ISSN: 1682-3915

Software Design for a Firewall Security System

F.I. Anyasi, A.K. Yesufu and J. Oriafo
Department of Electrical and Electronics, University of Ambrose Alli,
P.M.B 14, Ekpoma, Edo State, Nigeria

Abstract: This study highlighted the importance of security measures and therefore, takes a look at a practical solution to security lapses on networked systems. Existing computer systems that had only users authentication were examined and resolved to design software that can serve as a security measure to computers that are linked to one another and those connected to the Internet. The software (Program in Visual Basic 6.0) called a Firewall was developed. On implementation it was found that if a known Trojan is detected during communication, it kills and terminates the process, but if none found, it allow communication by confirming the information source.

Key words: Internet security, firewall approach, software design, securiy system, Nigeria

INTRODUCTION

Information is power. It is therefore ,a critical resource that should be protected with due respect to its confidentiality and value to any organization. In computer system technology, data security embodies the protection of data, program and any information, from unauthorized or accidental modification, damage, destruction or disclosure (Avikuim and Ranun, 1996).

Interest for and knowledge about, computers and network security is growing along with the need for it. This interest is in no doubt, due to the increase in the number of businesses that are migrating their sales and information channel to the Internet: As is well known, "The internet is a verse web of interconnected networks" (Chapman and Zwicky, 1995). The growth in the use of network computers in business, especially for e-mail, has also fuelled this interest. As organization and individuals start utilizing networks and the Internet, it is important for them to consider a security measure. Computer networks may be vulnerable to many threats along many avenues of attack including (Cheswick and Bellovin, 1994):

- Social engineering; where someone tries to gain access through social means (pretending to be a legitimate system user or administrator).
- War dialing; where-in someone uses computer software and a modem to search for desktop computer equipped with modems that answer, providing a potential path into a corporate network.
- Password guessing; the most common of which is "brute-force" attack where someone keeps trying possible combination of alphabets and/or figures until the required combination is accepted.
- Prying eyes of competitors and disgruntled employees.
- Eavesdropping of all sorts, including stealing e-mail messages files, passwords and other information over a network connection by listening in on the connection.

Many companies have lost millions of Naira due to security lapses in their network. Individuals are also presented with the post-mortems of security breaches in high profile companies in the news and are given the impression that some bastion of defense has failed to prevent some intrusion. Although we should know that no single mechanism or method will provide for the entire computer network security need of an organization, it is necessary that a form of security should be in place for any system connected to the Internet. A firewall should be designed between the networks. Firewalls are barriers at the gate to a network that filter the transmission of certain types of traffic according to security criteria (Joe and Dan, 1997). The research reported in this study was based on Info-tech, Mechelin Nig-. Ltd as a case study in 2004.

Firewall: We are used to the term "firewall" in other disciplines and in fact the term did not originate with the Internet. We have firewalls in housing separating, for example a garage from a house or one apartment from

Corresponding Author: F.I. Anyasi, Department of Electrical and Electronics, University of Ambrose Alli, P.M.B 14, Ekpoma, Edo State, Nigeria

another. Firewalls are barriers to fire, meant to slowdown its spread until the fire department can put it out (Oliver and Chapman, 1990).
Internet firewall has the following properties:

- It is a simple point between 2 or more networks through which all traffic must pass (choke point).
- Traffic can be controlled by and may be authenticated through the device and all traffic is logged there.

The first network firewalls appeared in the late 1980s and were later used to separate a network into smaller LANs.

The first security firewalls were used in the early 1990s (http://www.cisco.com/ipj, 1999). They were IP routers with filtering rules. The security policy was something like the following; allow anyone "in here" to access "out there". Also, keep anyone (or anything, I don't like) "out there" from getting "in here". These firewalls were effective, but limited. The next security firewalls were more elaborate and more tunable. Probably the first commercial firewall of this type, using filters and application gateways (proxies), was from Digital Equipment Corporation and was based on the DEC Corporate Firewall.

MATERIALS AND METHODS

Analysis of data and design: Data analysis seeks to analyze systematically the data input, data flow and information output within the context of a particular organization. The method is used to analyze, design and implement improvements in the functioning of an organization. Further more, system analysis and design is a series of processes systematically undertaken to improve business through the use of computerized information system. Before a new system can be designed and developed, it has to go through a cycle called the system development lifecycle. The proposed system has a life cycle as shown in Fig. 1.

The existing systems: InfoTech, Michelin Nig. Ltd, operates a Local Area Network (LAN). Different resources with particular reference to each Department of Michelin Port Harcourt are stored on the network. All staff of the company belonging to different departments can make use of the network resources in the day-to-day operation of the company. This LAN is connected to other LANs operated by the Michelin group. It is also linked to the Internet.

Description of the proposed system: The new system will contain a firewall and would work in a way that all systems on the network would have identification

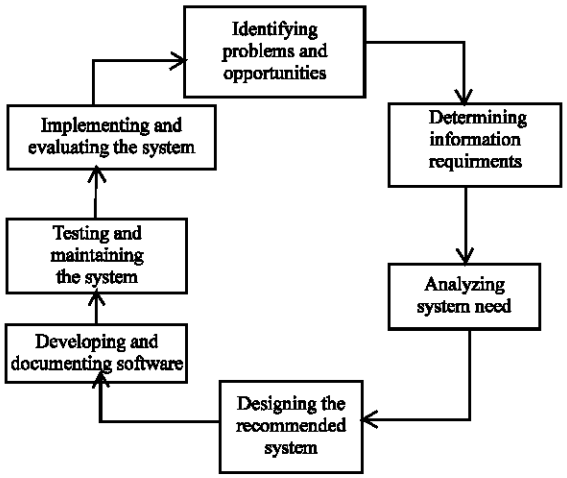

Fig. 1: System life cycle

numbers, so as to determine which system is accessing (communicating) the network resources at particular time.

The new system would also be designed to act as a verifier between users on the network and external users i.e., granting access to only external users that may have been registered to the network. It will also act as a watchdog, detecting the possible intrusions by most Trojans (these are programs that appear to be pleasant but are actually designed to break security or damage a system. A Trojan differs from a virus in that the damaging code is unable to replicate itself and spread to other programs). The new system is also able to;

- See current open ports on one's systems
- Save the attacks of Trojan to a log
- Manage Internet access and provide service for certain sites while other are blocked.

Produce management report from the log files.

Flow chart: Through the use of structural analysis techniques called flow-charting, the system analyst is able to put together a graphical representation of data movement through the program. The data flow approach emphasizes the logic underlying the system. By using combinations of symbols, the system analyst is able to create a pictorial view depicting data flow that eventually can provide solid system documentation. The above explanation is deployed in an attempt to design the system developed (Fig. 2).

Input design: The quality of the system input determines the quality of the system output. It is therefore, vital that input forms and screen be designed with this critical relationship in mind. This system is based on a network server connection. It's input is based on signals it receives during communication with modes on/off the

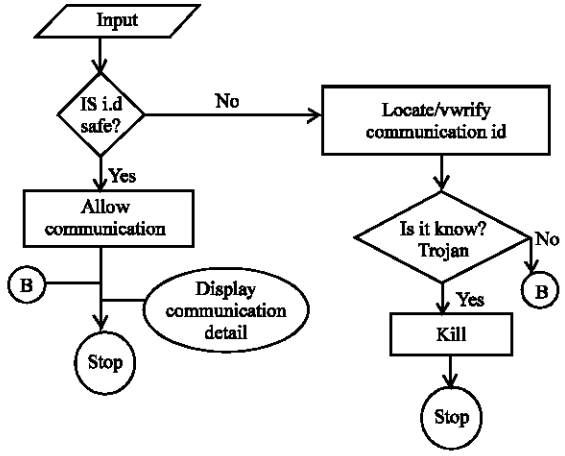

Fig. 2: Flow chart repersentation of the proposed system

network. Its communication channels are represented by data structures called sockets. A socket is identified by the following components:

- An address
- A port

The software (firewall) program receives input signal when computers on the network want to communicate. It simply receives the address port numbers e.t.c. And verifies if the communication is between systems on the network if so it allows communication otherwise it records the address of the system external to the network and checks the IP address in its databank. It then decides whether to allow or terminate communication.

Output design: Output information is delivered to user through the information system. Output can take many forms; the traditional hardcopy of printed reports and soft copy such as the Visual Display Unit (VDU) screens, microforms, audio output e.t.c. Users are reliant on output in order to accomplish their tasks and they judge the merit of the system solely by its output. Since the useful output is essential to gaining use and acceptance of the information system, this system was designed in a way that:

- The output serves the intended purpose
- The output fits the user
- The output can be saved on a log
- The output can be viewed
- The output rate can be delayed or increased

In this case, since the firewall is built on the server only, the system administrator has the most access to the output. The system administrator can view the output; delay the scan port in the parameters options. This system is also expected to generate some menus screen

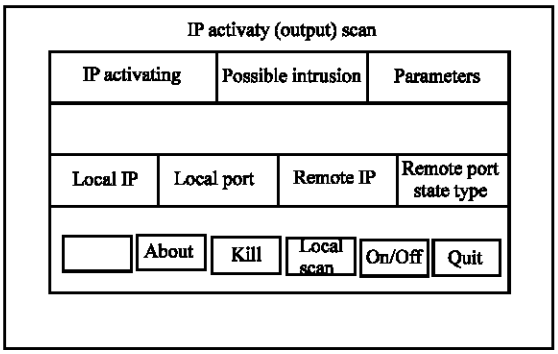

Fig. 3: Output main menu

display etc, depending on the mode being activated at any particular time. The system is designed with the user in mind i.e., it is user friendly. This is in the sense that it is highly interactive, easy to use, menu driven to make the user's job easier.

The output main menu (screen) is as shown in Fig. 3.

Choice of programming language: The programming languages used is Visual Basic 6.0. Visual Basic (VB) programming is basically in 2 steps; the visual programming step and the code-programming step.

During the visual programming step, one designs programmable forms using tools that come with the VB package. These visual tools allow one to design programs (forms) on as one wants/sees basis. i.e., one basically produces forms as one wants them to appear. In the code programming steps, one write codes using text editors. These codes are created for executing the visual forms.

This programming language offers the above-mentioned aids, it is easy to use and is currently one of the newest and most widely used programming languages.

RESULTS AND DISCUSSION

Users documentation: This study has been designed with the user in mind. It is designed such that a novice can operate it.

Table 1: Command buttons and their functions

	Command	Function
1	Kill	Terminates or disconnects communication
2	About	Describes the program and its author
3	Local scan	Scan for local system
4	ON/OFF	Removes or shows the scanning rate
5	Quit	Ends the program
6	Command	Function
7	Reset	It resets the list
8	Clear list	It clears the list of intrusion
9	Save log	Saves the current list
10	Scan delay	Increase/decrease the scan rate
11	Alert	Introduces or removes a beep sound

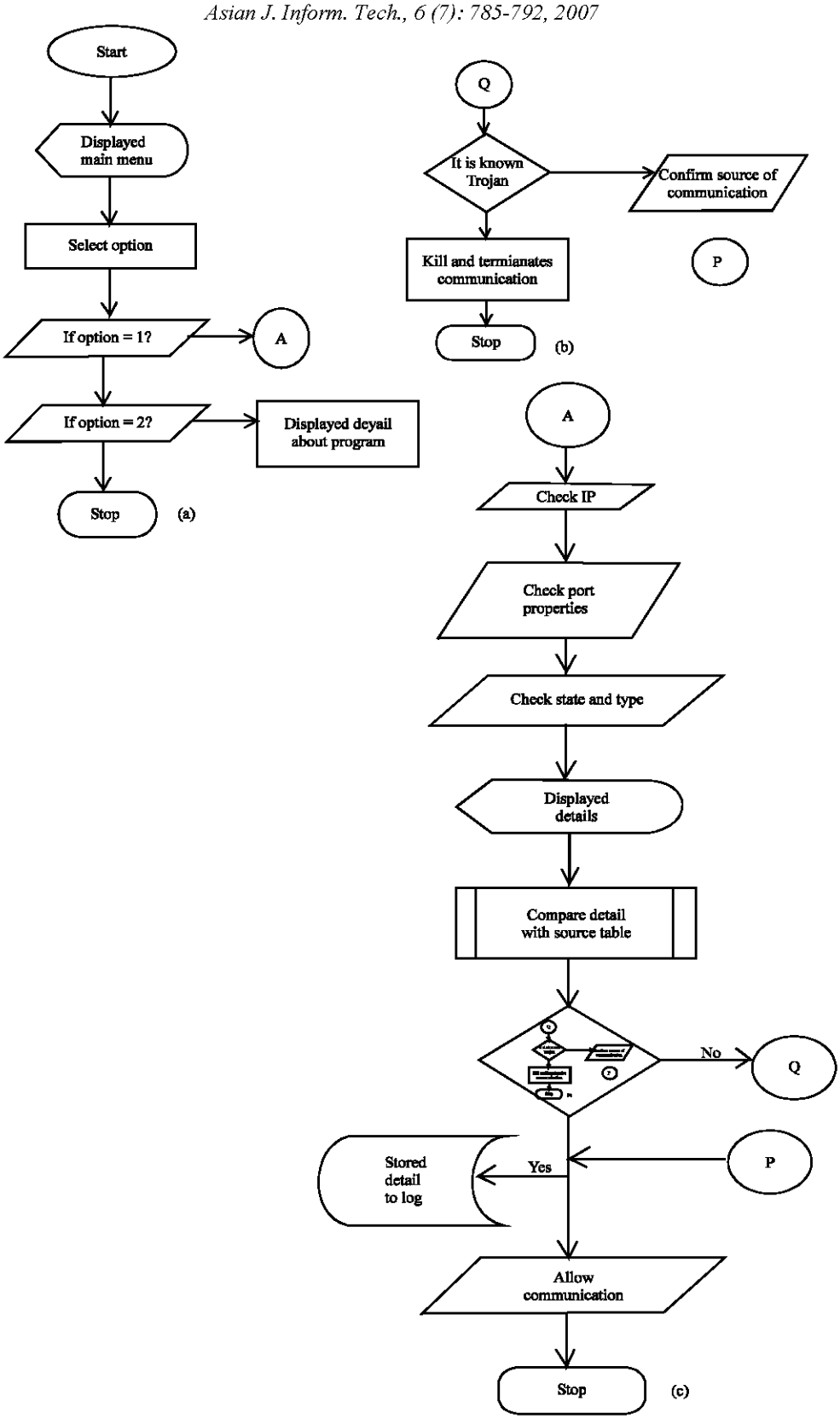

Fig. 4: Logic flow charts: (a) The flow chart for the display menu. (b) Flow chart showing the procedure if a known trojan is found. (c) Flow chart showing the procedure for a virus free communication

The program is designed in a way that when it is executed, the main menu is displayed. This main menu contains three major menus titled
IP activities (Internet Protocol)
Possible intrusion
Parameters.

- In the Internet Protocol activities menu, the local IP, the local port number, remote port number, the system state and type are displayed in Table 1.

Each option is activated by pressing the number corresponding to the option, for example the kill option is activated by pressing 1, the Quit option is activated by pressing 5.

- Possible Intrusion menu-here a list of possible program is displayed. In this menu the user makes use of the following command button as shown in Table 1, items 6-9.

The command is activated by pressing the number corresponding to the option in the menu. For example the About option is called by pressing 2, while the Reset option is activated by pressing 7 e.t.c.

- Parameters menu-here the user can quit the program, set the speed of scanning, in set a beep to sound alarm when a Trojan is encountered. It contains the following command buttons as shown in Fig. 1, items 10-11.

The Alert command is activated by pressing 11; while the scan delay is called by pressing 10 e.t.c. These commands and others have been designed with tool tips to enable the user execute the programs. Figure 4 shows the logic flow charts for the executed program.

The program listing (source codes): The program for the executed program is as follows;

```
Private Sub cmdRefresh_Click()
    If cmdRefresh.Caption = "On" Then
        cmdRefresh.Caption = "Off"
        Timer1.Enabled = True
    Else
        cmdRefresh.Caption = "On"
        Timer1.Enabled = False
    End If
End Sub
Private Sub cmdReset_Click()
    shIndic.FillColor = vbGreen
    bIndicC = True
End Sub
Private Sub cmdSave_Click()
    Call Write_Log
End Sub
Private Sub Form_Activate()
    Call Affiche_Port
End Sub
Private Sub Affiche_Port()
    Dim lngSize As Long
    Dim lngRetVal As Long
    Dim i As Long
    Dim lvItem As ListItem
        On Error Go To End
    Erase Fire
    indtab = 0
    ListView1.ListItems.Clear
    '
    ' TCP
    lngSize = 0
    lngRetVal = GetTCPTable(ByVal 0 and, lngSize, 0)
    If lngRetVal = ERROR_NOT_SUPPORTED Then
        MsgBox "IP Helper not supported !"
        Exit Sub
    End If
    ReDim arrTCPBuffer(0 To lngSize-1) As Byte
Private Sub CheckIP_Click()
    Call Affiche_Port
End Sub
Private Sub cmdAbout_Click()
    Load frmAbout
    frmAbout.Visible = True
End Sub
Private Sub CmdClear_Click()
    List Attack.Clear
End Sub
Private Sub cmdKill_Click()
    Dim TCPTableRow As MIB_TCPROW
    Dim lngRetValue As Long
    '
    If Not ListView1.SelectedItem Is Nothing Then
        '
        TCPTableRow = TCPBuffer(ListView1.
    SelectedItem.Index)
        '
        TCPTableRow.dwState = MIB_TCP_STATE_
        Delete_TCB
        '
        lngRetValue = SetTCPEntry(TCPTableRow)
        '
        If lngRetValue = 0 Then
                    MsgBox "Kill terminated :-)",
                    vbInformation
```

```
    Else
        MsgBox "Impossible Kill  :-(",vbExclamation
    End If
        '
    'Call cmdGet_Click
        '
    End If
End Sub
Private Sub cmdLocal_Click()
    Call Control_Trojan_Local
End Sub
Private Sub CmdQuit_Click()
    Unload Me
    End
End Sub
    lngRetVal = GetTcpTable(arrTCPBuffer(0), lngSize, 0)

    If lngRetVal =  Error_success Then
        CopyMem lngRows, arrTCPBuffer(0), 4
       For I = 1 To lngRows
          CopyMem TcpTableRow, arrTCPBuffer(4 + (i-
1)* Len(TcpTableRow)),
Len(TcpTableRow)
          If Not ((CheckIP.Value = vbChecked) And
(GetIpFromLong(TcpTableRow.dwLocalAddr) = "0.0.0.0"
Or
(GetIpFromLong(TcpTableRow.dwLocalAddr)        =
"127.0.0.1")) Then
    With TcpTableRow
    ReDim Preserve fire(indtab)
    ' Source listview
Set lvItem = List View1. ListItems. Add (..GetIp From Long
(.dwLocalAddr))
            lvItem.SubItems(1)  =  GetTcpPortNumber
            (.dwLocalPort)
            lvItem.SubItems(2) = GetIpFromLong
(.dwRemotePort)
            lvItem.SubItems(3)  =  GetTcpPortNumber
            (.dwRemotePort)
            lvItem.SubItems(4) = GetState(.dwState)
            lvItem.SubItems(5) = "TCP"
            'Source table
            fire(indtab).local_ip = lvItem
            fire(indtab).local_port = lvItem.SubItems(1)
            fire(indtab).remote_ip = lvItem.SubItems(2)
            fire(indtab).remote.port = lvItem.SubItems(3)
            fire(indtab).state = lvItem.SubItems(4)
            fire(indtab).type = "TCP"

            indtab = indtab + 1
    End With
    End If
    ReDim Preserve TCPBuffer(i)
    TCPBuffer(i) = TcpTableRow
    Next i
End If
'UDP
lngSize = 0
lngRetVal = GetUdpTable(ByVal 0and, lngSize, 0)

    If lngRetVal = ERROR_NOT_SUPPORTED Then
            MsgBox "IP Helper not supported !"
            Exit Sub
    End If
    ReDim arrUDPBuffer(0 To lngSize-1)' As Byte
    lngRetVal = GetUdpTable(arrUDPBuffer(0),lngSize,(0)
    If lngRetVal = ERROR_SUCCESS Then
            CopyMem IngRows, arrUDPBuffer(0),4
            For i =1 To lngRows
            CopyMem UdpTableRow, arrUDPBuffer
            (4 + (i-1)*  Len(UdpTableRow))
            Len(UdpTableRow)
            If Not ((CheckIP.Value = vbChecked) And
    (GetIpFromLong(UdpTableRow.dwLocalAddr)     =
    "0.0.0.0" Or
    (GetIpFromLong(UdpTableRow.dwLocalAddr)     =
    "127.0.0.1")) Then
            With UdpTableRow
                    ReDim Preserve fire (indtab)
            ' Source listview
            Set lvItem = ListView1.ListItems.Add
    (..GetIpFromLong(.dwLocalAddr))
            lvItem.SubItems(1) = GetUdpPort Number
            (.dwLocalPort)
            lvItem.SubItems(5) = "UDP"
            ' Source table
            fire(indtab).local_ip = lvItem
            fire(indtab).local_port = lvItem.
    SubItems(1)
            'fire(indtab).remote_ip = ""
            'fire(indtab).remote_port = ""
            'fire(indtab).state = ""
            'fire(indtab).type = "UDP"
            indtab = indtab + 1
        End With
        End If
    Next i
End if
If FicTrojanOk = True Then
         'Call Control_Trojan_Local
         Call Test_Attack
    End If
End:
End Sub
```

```
Private Sub Form_Load
        Me.Show
        Me.Refresh
With nid
    .cbSize = Len(nid)
    .hwnd = Me.hwnd
    .uId = vbNull
    .uFlags = NIF_ICON Or NIF_TIP Or NIF_MESSAGE
    .uCallBackMessage = WM_MOUSEMOVE
    .hIcon = ImageList1.ListImages(4).Picture
    .szTip = "JoanneWall" and vbNullChar
End With
    Shell_NotifyIcon NIM_ADD, nid
    bIndic = True
    bIndicC = True
    Timer1.Interval = HScroll1.Value
    chkBeep.Value = vbChecked
    Call Read_Port
    FormFire.Status.SimpleText = "Trojans tested: " and
    Str(indport)
End Sub
Private Sub Form_QueryUnload(Cancel As Integer,
UnloadMode As Integer)
    Shell_NotifyIcon Nim_delete, nid
    Me.Refresh
End Sub
Private Sub HScroll1_Change()
    lbldelay = Str(HScroll1.Value)
    Timer1.Interval = HScroll1.value
End Sub
Private sub Timer1_Timer()
    Call Affiche_port
    If bIndicC Then
    shIndic.FillColor = vbGreen
Else
    shIndic.FillColor = vbRed
End If
If bIndic Then
    shIndic.Visible = True
    bIndic = False
Else
    shIndic.Visible = False
    bIndic = True
End If
End Sub
Private Sub Timer2_Timer()
    Dim tStats      As MIB_IPSTATS
    Static TStaticStats As MIB_IPSTATS
    Dim lRetValue      As Long
    Dim blnIsSent      As Boolean
    Dim blnIsRecv      As Boolean
    Private Declare Function RegOpenKeyEx Lib
"advapi32" Alias "RegOpenKeyExA" (ByVal hKey As
Long, ByVal lpSubKey As String, ByVal ulOptions As
Long, byVal samDesired As Long, ByRef phkResult As
Long) As Long
Private Declare Function RegQueryValueEx Lib
"advapi32" alias "RegQueryValueExA" (ByVal hKey As
Long, ByVal lpValueNAme As String, ByVal lpReserved
As Long, By ref lpType As Long, ByVal lpData As String,
ByRef lpcbData As Long) As Long
Private Declare Function RegCloseKey Lib "advapi32"
(ByVal hKey As long
Private Sub cmdOK_Click()
    Unload Me
End Sub
Private Sub Form_Load()
    Me.Caption = "A proposal of " and App.Title
    lblVersion.Caption = "Version" and App.Major and
"." and App.Minor and "." and
    App.Revision
    lblTitle.Caption = App.Title
End Sub
```

Testing: On installation of the designed software in the systems under review, it was found that a display menu as shown in Fig. 3 appears on the screen at the commencement of any activities. When a virus infected package was to be processed, the system refused communication and with depression of the KILL key, the process was terminated thereby eliminating the known virus.

CONCLUSION

A security system is neither immutable nor composed of policies that are perfect, final or everlasting. In other words, the importance of specific elements of security changes with time and is subject to influences such as technological advancement, new breach-in-method etc.

In this research, existing computer systems that had only user authentication were examined and resolved that this was grossly insufficient. The software (Program in Visual Basic 6.0) called a Firewall developed was able on implementation to detect a known Trojan during communication, thereby killing and terminating the process, but if non found, it allow communication by confirming the information source. The Firewall developed provided the best defense against intrusion, manipulation and damage to information stored in and transferred via networked computer systems.

In recognition of the fact that the success of any organization depends on how efficiently it manages its information, it is the researcher's hope that all organizations, no matter businesses would develop a Firewall such as this, to act as a reliable security tool.

It is recommended that any organization, large or small should take security issues as a priority. They should develop a security policy to ensure information management and control.

If an organization deals in communication or has a network that is linked to other networks or the Internet, it is strongly recommended that a kind of firewall be developed round the organization's network so as to act as a control.

REFERENCES

Avikuim, F. and V. Ranun, 1996. A Network Perimeter with Secure External Access. Proc. ISOC NDSS Symposium, 3: 35-41.

Chapman, D. and E. Zwicky, 1995. Building Internet Firewalls. ISBN 1-56592-124. O' Reily and Assoc., pp: 201-215.

Cheswick, W. and S. Bellovin, 1994. Firewalls and Internet Security" Repelling the Wily Hacker. ISBN 0201633574, Addison-Wesley, pp: 81-92.

http://www.cisco.com/ipj, 1999. Firewalls and Internet Security. The Internet Protocol J. (IPJ)., 2: 2.

Joe, C. and N. Dan, 1997. MCSC Training Guide: Network Essentials. ISBN 1-56205-749-9. New Riders. pp: 23-41.

Oliver, E. and R. Chapman, 1990. Data Processing and Information Technology. ISBN 1-870941-462, the Guernsy, pp: 215-218.