Available online at www.sciencedirect.com

SciVerse ScienceDirect

AASRI Procedia 3 (2012) 335 – 340

AASRI Procedia

www.elsevier.com/locate/procedia

2012 AASRI Conference on Modelling, Identification and Control

Design Method for Virtual Network Attack and Defense Platform

Wang Fangnian[a], Peng Gang[a], Che Wanfang[b], Niu Cong[c], Bai Yun[b,d*], Zhu Genbiao[b]

[a] *Air Force Airborne Academy, Guilin 541003, China*
[b]*Key Lab of Complex Aviation System Simulation, Beijing 100076, China*
[c]*Beijing Institute of Technology, Beijing 100081, China*
[d]*Air Force Engineering University, Xi'an 710055,China*

Abstract

A design method for network attack and defense simulation platform is discussed in this paper. Firstly the component and function of the platform are analyzed. Then Visio second development method is used to construct the virtual network topology. The parsing of virtual network topology is also researched and the relative flow sheet is described. Lastly an example is carried out to test performance of the platform. Simulation results show the effectiveness of the proposed method.

Key words: Virtual network; Attack and defense simulation; Visio second development

1. Introduction

At present, the security of network and information closely related to network security devices is increasingly important, so it is particularly important for the skilled operation of network security devices. However, since the majority of network security devices take on duty, it is hard to implement offensive and

* Corresponding author. Tel.: 18611404006; fax: +0-000-000-0000 .
E-mail address: yunbai13@hotmail.com.

doi:10.1016/j.aasri.2012.11.053

defensive drilling and testing. Virtual network attack and defense simulation platform is to construct an attack and defense system with theoretical knowledge, reasonable structure, and suitable for the study of security management for the above requirements. Network attack and defense simulation combat environment is constructed to help security managers to raise the overall level of safety management, and enhance network and information security[1-2]. Design of network attack and defense simulation platform is of great significance to study the security of the network devices.

A design method of virtual network attack and defense simulation platform is constructed in this paper. The composition and function of the platform is analyzed. The establishing and parsing of virtual network topology is researched based on the Visio secondary development method, and the simulation is also presented.

2. Overall design of virtual network attack and defense simulation platform

Virtual networks and devices are used to simulate the real ones in the network attack and defense simulation platform. Its main functions contain generation of network topology, configuration of network security device, implementation of network attacks, attack detection, attack records and statistics. The virtual network device and topology are displayed in a graphical interface, and the functions of various devices are simulated through some special properties and methods, which is propitious to carry through network attack and defense simulation. The composition of network attack and defense simulation platform is shown in Figure 1(a).

The main function of network attack server is the implementation of network attacks. Attack methods selected from the attack database are used to attack the target device for testing.

Network defense simulation server is mainly composed of network data capture, network topology parsing, virtual network device and virtual network database. During simulation, the virtual network topology is established according to the actual situation, and the virtual network device should be configured according to the actual parameters of each device. The data transmission in the virtual network is determined by the network topology and device configuration. Each virtual device contains processes of data receiving, data processing and logging. Data arriving at each device should be tested with the particular rules of the device. The legitimate data will be transmitted properly while the illegitimate one will be discarded.

3. Creation and parsing of the virtual network topology

The creation of a virtual network topology is necessary for the construction of virtual network environment. There are various methods for the creation of a virtual network topology. The secondary development of drawing software technology is one of the most effective methods. It can simplify the development of the graphics editing module, and the capabilities of devices can also be carried out in the programming software. So Visio secondary development technology is used in the creation of virtual network topology.

3.1. Visio secondary development technology

Microsoft Office Visio 2003 ActiveX Control (Visio drawing control) can provide the full function for Visio application as an embedded component through the Visio object model. Visio drawing control can be driven by events or codes in the host application. In addition, the Visio drawing control provide chart production environment in the context of the application user interface for users[3].

The Visio drawing control components provide the function of the Visio application object model. It can be embedded in the development of the host application using the Microsoft Visual Studio.NET, Microsoft

Office XP and Microsoft Office container (such as Microsoft Office Word 2010, Microsoft Internet Explorer 5.0 and other Microsoft ActiveX container). The control will display the shape of the drawing screen after added to the host application. The Visio drawing control allows developers to extend custom applications and solutions. Visio components can be driven by the user drawing operation or host application events and data through providing programming capabilities, as well as control access to the full Visio object model. The architecture of Visio drawing control in application[3] is shown in Figure 1(b).

Diagram development with Visio is in an intuitive way. Both a topology diagram and a detailed technical drawing are available through combination of the program predefined graphics, and graphics can be modified or created to adapt to different business and requirements.

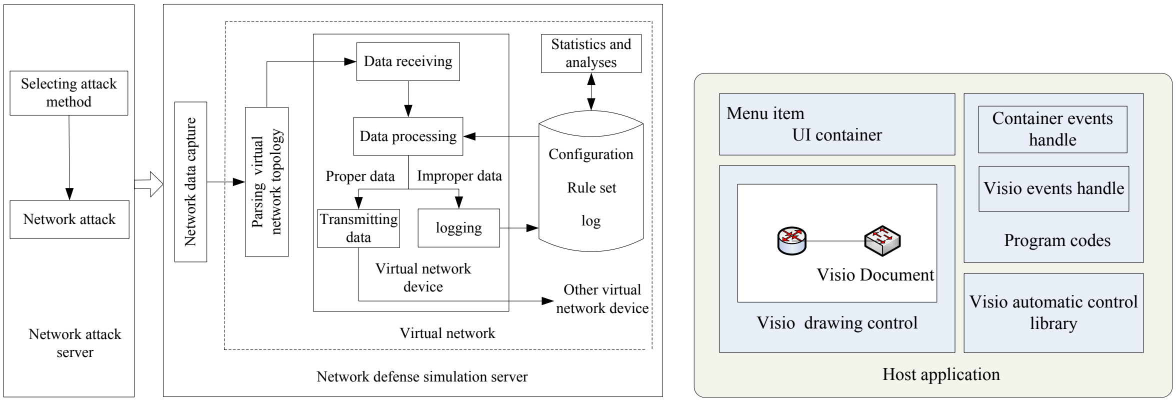


Figure 1: (a) Composition of network attack and defense simulation platform, (b) Architecture of Visio drawing control in application

3.2. Creation of virtual network topology

Network topology edit provides environment for users to build a virtual net-work. Equipment selection, connection, configuration and network testing can be simulated in this experimental environment.

The device model in the toolbox can be dragged to add a network device in the network attack and defense platform. When a network device is added to the virtual network, a dialog box will be popped up asking to enter the basic information of the device. The network device will be displayed in the network topology drawing interface if the information is proper. The user can operate the related devices through the right mouse button. For the router, the user can add some routing paths to the existing routing table; for the firewall, the user can edit the firewall rules, and then add it to the firewall rule table.

When the required devices for network drilling are all added to the operating platform, network connection between devices can be established. Visio secondary development technology is used for the generation of virtual network topology, which can make use of the powerful drawing capabilities of Visio drawing. The process of virtual network creation with Visio secondary development technology can be divided into the following sections[4]:

- Establishment of the mold

The virtual network device is called drawing cell, and the toolbox where the drawing cell is placed is called the mold in Visio. Each drawing is a Shape, and each Shape has a corresponding Shape sheet. There are two important tables in the Shape sheet: one is the User Defined Cells, the other is the Custom Properties. Properties of simulation devices can be set through the two tables.

In the Establishment of the mold, the drawing cell symbol is mapped out in the drawing area firstly. Then, the Shape Sheet spreadsheet is used to set properties for the drawing cell. Finally, the completed drawing cell will be dragged to a new mold, which can be saved with a new name.

- Control on the drawing cell with C#.NET

The control on the drawing cell with program contains two aspects: one is obtaining information of the drawing cell; the other is writing information to the drawing cell and controlling the state. The function shape.getCells() is used to obtain information of the drawing cell, and the specific values selected from Shape sheet should be determined in accordance with the relevant parameters. For example, if there is a row called "firewall name" in the Custom Properties table of the Shape sheet and the value of "value" wants to be obtained, the information should be written as follows:

shape.getCells ("Prop.Firewall Information").getResultInt ("value", 0).

The row is obtained in shape.getCells ("Prop.Firewall Information"), and the value of "value" column is obtained in getResultInt ("value", 0).

The process of writing information to the drawing cell is similar to that of obtaining information, for example:

shape.getCells ("Prop. Firewall Information"). FormulaU = "1".

The value of "FormulaU" is "1", which indicates the firewall is running.

The drawing cell and data can be separated through properties configuration. The data is stored in the database, and can be associated with the drawing cell by a unique identification.

- Definition of events

The corresponding menu should be popped up when the mouse right-click the virtual device components in order to input and modify the data of the device. So the right-click events of the Visio drawing control should be defined in the design of drawing cells. The codes of mouse handling event[5] are shown in Figure 2(a).

When the drawing cell corresponding to each device is dragged to the drawing control from the mold and connection between devices is constructed, the mapping of network topology is completed. After the completion of network topology, rules of the network security devices should be set to lay the groundwork for the attack and defense simulation. The rule setting mainly includes the router routing table and firewall filtering rules. A virtual network topology is established after the configuration of the virtual network security device.

When the drawing cell corresponding to each device is dragged to the drawing control from the mold and connection between devices is constructed, the mapping of network topology is completed. After the completion of network topology, rules of the network security devices should be set to lay the groundwork for the attack and defense simulation. The rule setting mainly includes the router routing table and firewall filtering rules. A virtual network topology is established after the configuration of the virtual network security device.

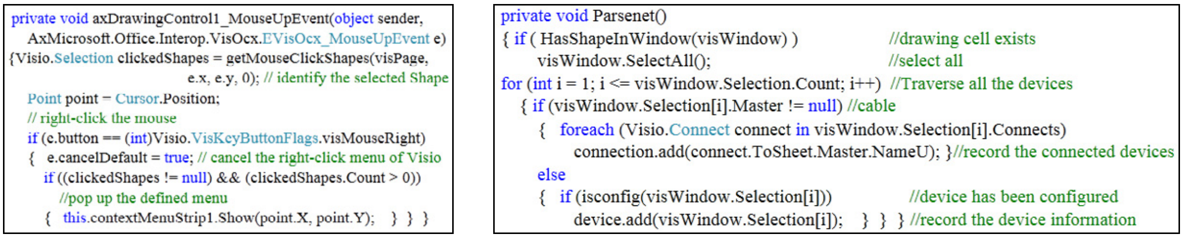
3.3. Creation of virtual network topology

After the establishment of virtual network topology, all network devices show only a simple graphical interface. The virtual network topology should be parsed to realize the simulation. The devices in the graphical interface and its connection relationship should be obtained. In the platform, the virtual network topology can be parsed by identifying the type of device and recording connection information of the cable. The process of the virtual network topology parsing is shown in Figure 3(a).

Traversing all the virtual devices is essential for the parsing of virtual network topology. The type of each device in the topology is determined firstly. If the device is network cable, the information of devices connected to it is recorded to the database, including the device type and name. Otherwise, the basic device information is directly recorded to the database, including device type, name, parameters and configuration.

Visio is a mature vector graphics system, and it is very convenient to obtain the topological relations between the drawing cells. Network cable connecting different devices is used to determine the connection between devices. The connection relationship of each device is written to the relevant attributes by Visio during drawing graphics. The From Connects set of Connects properties of devices is used to obtain the devices connected to current device, which is advantageous for the parsing of network topology[6]. The function ParseNet() is used to parse the virtual network topology, the codes of which are shown in Figure2(b).

All the information has been recorded to the database after creation and parsing of the virtual network topology. So all the simulation processes are transferred to the background simulation.



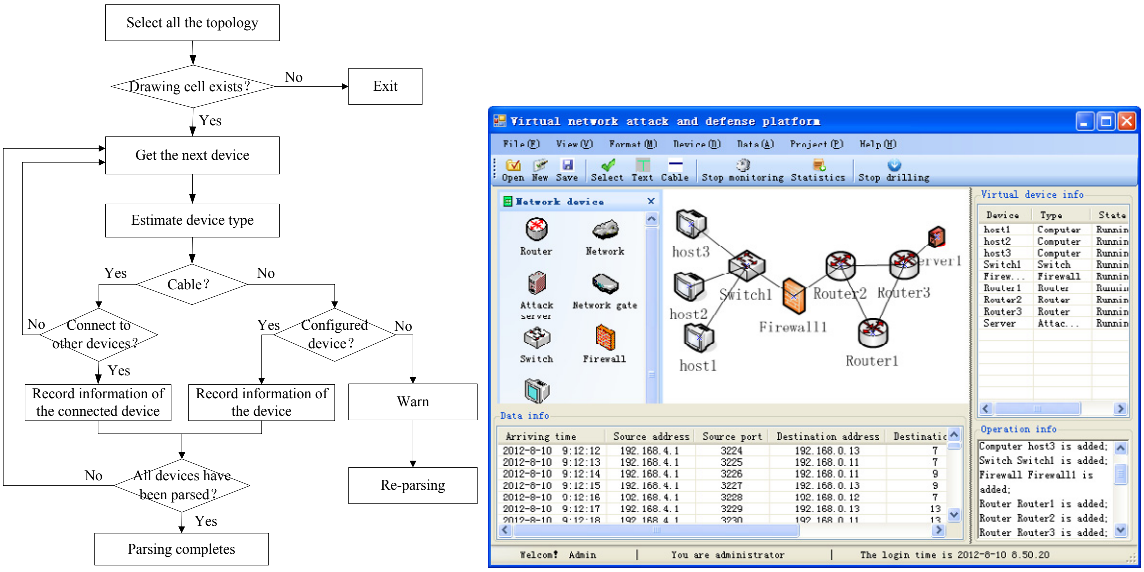
```
private void axDrawingControl1_MouseUpEvent(object sender,
    AxMicrosoft.Office.Interop.VisOcx.EVisOcx_MouseUpEvent e)
{Visio.Selection clickedShapes = getMouseClickShapes(visPage,
                              e.x, e.y, 0); // identify the selected Shape
    Point point = Cursor.Position;
    // right-click the mouse
    if (e.button == (int)Visio.VisKeyButtonFlags.visMouseRight)
    {   e.cancelDefault = true; // cancel the right-click menu of Visio
      if ((clickedShapes != null) && (clickedShapes.Count > 0))
         //pop up the defined menu
      {   this.contextMenuStrip1.Show(point.X, point.Y);   } } }
```

```
private void Parsenet()
{ if ( HasShapeInWindow(visWindow) )                 //drawing cell exists
      visWindow.SelectAll();                          //select all
for (int i = 1; i <= visWindow.Selection.Count; i++)  //Traverse all the devices
   { if (visWindow.Selection[i].Master != null) //cable
      {   foreach (Visio.Connect connect in visWindow.Selection[i].Connects)
            connection.add(connect.ToSheet.Master.NameU); }//record the connected devices
      else
      {   if (isconfig(visWindow.Selection[i]))              //device has been configured
            device.add(visWindow.Selection[i]);    } } } //record the device information
```

Figure 2: (a) The codes of mouse handling event, (b) Codes of ParseNet() function

4. Simulation results

The previous sections have conducted a comprehensive study for the architecture of network attack and defense simulation platform. An attack and defensive simulation example is established to test the platform in this section. The virtual network constructed in the platform is shown in Figure 3(b).



Arriving time	Source address	Source port	Destination address	Destinatic
2012-8-10 9:12:12	192.168.4.1	3224	192.168.0.13	7
2012-8-10 9:12:13	192.168.4.1	3225	192.168.0.11	7
2012-8-10 9:12:14	192.168.4.1	3226	192.168.0.11	9
2012-8-10 9:12:15	192.168.4.1	3227	192.168.0.13	9
2012-8-10 9:12:16	192.168.4.1	3228	192.168.0.12	7
2012-8-10 9:12:17	192.168.4.1	3229	192.168.0.13	13
2012-8-10 9:12:18	192.168.4.1	3230	192.168.0.11	13

Device	Type	State
host1	Computer	Runnin
host2	Computer	Runnin
host3	Computer	Runnin
Switch1	Switch	Runnin
Firew...	Firewall	Runnin
Router1	Router	Runnin
Router2	Router	Runnin
Router3	Router	Runnin
Server	Attac...	Runnin

```
Computer host3 is added;
Switch Switch1 is added;
Firewall Firewall1 is
added;
Router Router1 is added;
Router Router2 is added;
Router Router3 is added;
```

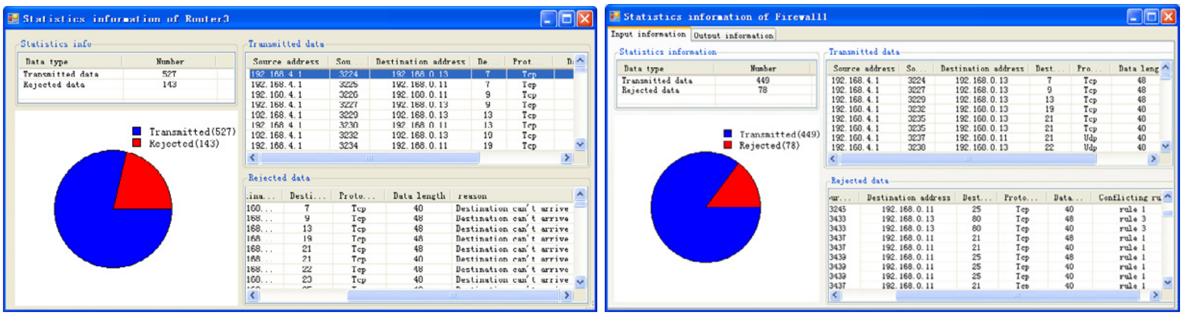
Welcom! Admin | You are administrator | The login time is 2012-8-10 8.50.20

Figure 3: (a) Parsing of virtual network topology, (b) The main interface of network simulation platform

Due to space limitations, the configuration of each network device is not shown. The statistics information of each device can be obtained in the simulation. Figure 4(a) and Figure 4(b) show the statistics information of Router3 and Firewall1, respectively.

It can be seen from the figure that whether the data of Router3 is transmitted depends on its routing table. Data in line with the routing table will be transmitted to the next device, while the improper data is rejected and logged. In the same way, data of Firewall1 compliant with the rules is transmitted, while the improper data is discarded.

Various simulations are conducted for comprehensiveness test of the platform, and the system function is analyzed through the statistics information of routers and firewalls. Simulation results show the virtual router can transmit data according to the routing table, while the virtual firewall can filter data with the filtering rules, which accord with the design objectives of the platform, and the desired purpose is achieved.



Statistics information of Router3

Statistics info

Data type	Number
Transmitted data	527
Rejected data	143

Transmitted data

Source address	Sou...	Destination address	De...	Prot...	D:
192. 168. 4. 1	3224	192. 168. 0. 13	7	Tcp	
192. 168. 4. 1	3225	192. 168. 0. 11	7	Tcp	
192. 160. 4. 1	3226	192. 160. 0. 11	9	Tcp	
192. 168. 4. 1	3227	192. 168. 0. 13	9	Tcp	
192. 168. 4. 1	3229	192. 168. 0. 13	13	Tcp	
192. 168. 4. 1	3230	192. 168. 0. 11	13	Tcp	
192. 168. 4. 1	3232	192. 168. 0. 13	19	Tcp	
192. 168. 4. 1	3234	192. 168. 0. 11	19	Tcp	

Rejected data

ina...	Desti...	Proto...	Data length	reason
160...	7	Tcp	40	Destination can't arrive
168...	9	Tcp	48	Destination can't arrive
168...	13	Tcp	48	Destination can't arrive
168...	19	Tcp	48	Destination can't arrive
168...	21	Tcp	48	Destination can't arrive
168...	21	Tcp	40	Destination can't arrive
168...	22	Tcp	48	Destination can't arrive
160...	23	Tcp	40	Destination can't arrive

Statistics information of Firewall1

Input information | Output information

Statistics information

Data type	Number
Transmitted data	449
Rejected data	78

Transmitted data

Source address	So...	Destination address	Dest...	Pro...	Data leng
192. 168. 4. 1	3224	192. 168. 0. 13	7	Tcp	48
192. 168. 4. 1	3227	192. 168. 0. 13	9	Tcp	48
192. 168. 4. 1	3229	192. 168. 0. 13	13	Tcp	48
192. 160. 4. 1	3232	192. 160. 0. 13	19	Tcp	40
192. 160. 4. 1	3235	192. 160. 0. 13	21	Tcp	40
192. 160. 4. 1	3235	192. 160. 0. 13	21	Tcp	40
192. 160. 4. 1	3237	192. 160. 0. 11	21	Udp	40
192. 160. 4. 1	3238	192. 160. 0. 13	22	Udp	48

Rejected data

ur...	Destination address	Dest...	Proto...	Data...	Conflicting ru
3245	192. 168. 0. 11	25	Tcp	40	rule 1
3433	192. 168. 0. 13	80	Tcp	48	rule 3
3433	192. 168. 0. 13	80	Tcp	40	rule 3
3437	192. 168. 0. 11	21	Tcp	48	rule 1
3437	192. 168. 0. 11	21	Tcp	40	rule 1
3439	192. 168. 0. 11	25	Tcp	48	rule 1
3439	192. 168. 0. 11	25	Tcp	40	rule 1
3439	192. 168. 0. 11	25	Tcp	40	rule 1
3437	192. 168. 0. 11	21	Tcp	40	rule 1

Figure 4: (a) Statistics of Router3, (b) Statistics of Firewall1

5. Conclusions

The composition and function of virtual network attack and defense simulation platform are analyzed in this paper. The creation of virtual network topology is achieved through the Visio secondary development technology and the parsing method of virtual network topology is also researched. Finally, the platform is tested by network attack and defense instances. Simulation results show that the main function of the virtual network attack and defense simulation platform is realized, and the design objectives are achieved.

References

[1] Wang, S., Wang, Z. Information system attack and defense. Beijing: Electronic Industry Press; 2007.

[2] Wu, X. Design and implementation of network attack and defense simulation environment. Xi'an: Xidian University; 2005.

[3] MSDN Library for Visual Studio. Microsoft; 2005.

[4] Zhu, H., Lei, M., Gao, S. Application of Visio secondary development technology in the electrical engineering teaching graphics. Journal of Electrical & Electronic Education; 2006.

[5] Zou, J., Zhou, S., Xiang, X. C# enterprise-level development. Beijing: People's Posts and Telecommunications Press; 2006.

[6] Richard B. C# network application programming. Beijing: Electronic Industry Press; 2003.