An Interactive Firewall Simulator for Information Assurance Education

Kenneth Williams and Huiming Yu

Abstract - **In this paper, we present an interactive firewall simulator to help students learn the intricacies of configuring a firewall to prevent attacks. The design principles of the simulator are to be competitive and fun to use while teaching the student the details of firewall configuration. The firewall simulator demonstrates how properly configuring a firewall allows normal network traffic while preventing various attacks. The instructor who can require configuration changes to the student's simulated firewalls controls the simulation. The firewall simulator has been designed and implemented in the Department of Computer Science at North Carolina A&T State University to enhance information assurance education. This simulator has been used in several courses with excellent results. The simulator has been distributed to the attendees of the 2008 Faculty Development Workshop on Cyber Games and Interactive Simulation and used in different colleges and universities**

Index terms **– firewall, firewall configuration, Information Assurance education**

I. Introduction

E-commerce and information availability play a very important role in today's modern society. People want around the clock access to information and their favorite websites. If a company's website were to go down for one minute, it could result in millions of dollars being lost. With the dramatic growth of e-commerce, wireless network and cloud computing, organizations and individuals require a certain level of privacy, integrity, confidentiality and availability. Therefore, security has become a major concern throughout the world. Increasing Information Assurance education and teaching knowledge of security techniques to students who major in computer science, information technology and management information system, and satisfying new expectations for Information Technology professionals has become a very urgent need [1, 2].

A firewall is a security tool that can be implemented in many environments to provide perimeter protection. Most commercial networks install a dedicated firewall device between their local intranet and the Internet to monitor traffic entering and leaving the network. To be effective, firewalls have to be properly configured. Proper configuration is neither immediately obvious nor static. It can be difficult to differentiate a good data packet from a potentially damaging packet.

We have taught Information Privacy and Security, Web Security, and Network Security courses for several years. According to students' feedback, after traditional lectures some of them have difficulty fully understanding the use and configuration a firewall. For many students an interactive education tool can help them to understand the functions of firewalls by getting hands-on and configuring a firewall step by step.

In order to enhance Information Assurance education we have developed an interactive firewall simulator in the Department of Computer Science at North Carolina A&T State University (NC A&T SU) to help students better understand the functions of a firewall and how to configure it, and to let students get hands-on experience. This simulator can be used in network security, Web security and other related courses by instructors in the classroom or by students outside the classroom.

In this paper, we discuss designs and implementation of the interactive firewall simulator, and present our teaching experience and lessons learned. In section 2 the objectives will be discussed and compared to other systems. The detail of the design considerations of the interactive firewall simulator will be presented in section 3. In section 4 functions of the simulator will be exhibited. In section 5 experimental results will be discussed. The conclusions will be given in section 6.

II. Background and Objectives

Firewalls are an import topic in Information Assurance and computer security. A number of educational firewall simulation systems have been previously developed. The goal of some systems [5][6] is to provide the student with a statistically supported understanding of a firewall's effectiveness. The configuration of the firewall in these systems is fixed by the simulation and not defined by the student. These systems give the student an understanding of network and firewall load, but provide very little training on the configuration of a firewall. Several systems [8][9][10] make use of virtualization for security simulations. Virtualization is effective for providing each student virtual resources, including firewalls, that the student can deploy to secure a network. Since each system is isolated, they do not benefit from any interaction between the students.

CyberCIEGE [7] is an interactive game designed to teach computer and network security concepts. It provides the student with a wide range of security threats and possible solutions. It also requires the student to provide security within a limited financial budget. Firewall configuration within CyberCIEGE is done at a high level without defining the details of what specific packets are to be filtered.

The objectives of the interactive firewall simulator presented here is to provide students with an interactive competitive system to help them better understand the concepts of firewall configuration and operation. Students are required to configure a simulated firewall using Cisco-like commands to prevent other students from attacking them. Students who have a basic understanding of firewalls can easily learn to use the system. Lab activities using the firewall simulator can be completed within an hour. The simulator can be used in any network or security course.

Manuscript received March 1, 2011; revised March 27, 2011. This work was supported in part by the U.S. National Science Foundation.

The authors are with the Computer Science department of North Carolina A&T State University, Greensboro, NC 27411 (phone: (336) 334-7245, fax: (336) 334-7244, email: williams@ncat.edu and cshmyu@ncat.edu

III. Design Considerations

Teaching students how to properly configure a firewall can be challenging. Most schools do not have commercial firewall systems available for the students to use nor do they have the capability to generate reasonable benign and attack traffic. To assist in teaching students how to configure a firewall, we designed and implemented a firewall simulator. This interactive learning simulator allows students to configure a virtual firewall to protect a virtual network. The major design considerations are:

- Teach students about firewalls – The primary goal of the firewall simulator is to teach students about the purpose and operation of network firewalls. Students need to understand that a firewall is not just a box you plug into your network. A firewall must be configured properly to be effective. The goal of the firewall simulator is to give students experience in configuring firewalls for a variety of situations.
- Be fun – An ideal assignment is so interesting that the students want to do it. Students are more likely to learn the material if they are interested in doing the assignment.
- Be competitive – Competition adds excitement and interest. In the real world, there appears to be a continuing competition between hackers trying to break into systems and system administrators working to defend them. In the simulation, students operate in both the defensive and offensive roles. If a student does not correctly configure their firewall, the other students will vigorously attack any weakness.
- Changing requirements – The most secure system is one that is disconnected from the network. While secure, this is not very useful. The optimal solution in configuring a firewall is to balance the needs of the users with the need to maintain security. The simulator requires the student allow certain specific network traffic to pass through the firewall. Like in the real world, requirements frequently change. The firewall simulator presents the students with changing specifications requiring them to change the configuration of their firewall.
- Completion in an hour – Many courses only have an hour for the students to work on an interactive lab. The lab was designed so that a group of twenty to thirty students can complete it within a 50 minute period.
- Major vendor syntax – There are many different firewalls available with many different systems for configuring them. To be effective, the configuration system for the simulator has to allow fine control over the many possible options. We chose to use the firewall configuration syntax defined by Cisco Systems [3, 4]. The configuration text file allows the student to see their full configuration at a glance, which is often obscured by GUI configuration systems that flip through multiple windows.
- Run on any system – The simulator does not require a dedicated lab, network isolation and any special hardware. It can be run in a lab of normal computers without interfering or endangering other users. To make the simulator available to many people and to avoid operating system peculiarities, the simulator is designed to run on a wide variety of systems. It is written as Java applets running in a browser with a Java application running on a web server.
- Be configurable – The simulator presents several different tasks and configuration changes to the students. To avoid having to change the program to change the number and type of tasks, the program reads two XML configuration files. These configuration files define the changes students will have to make during the simulation and define the actions students can take against other student's configuration.

IV. Functions of the Firewall Simulator

The simulator allows participants to configure their own simulated firewalls using Cisco-like syntax. Students can take benign or malicious actions against other players to score points. A benign action could be attempting to read the virtual public web server on another player's network. If the other player's firewall does not allow this permissible activity, the first player scores a point while the other player loses a point. A malicious action would be a network attack where the other player's firewall must prevent the action to avoid losing points.

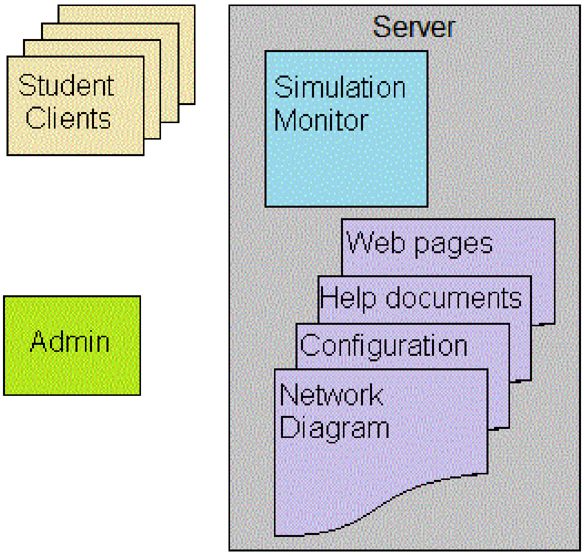
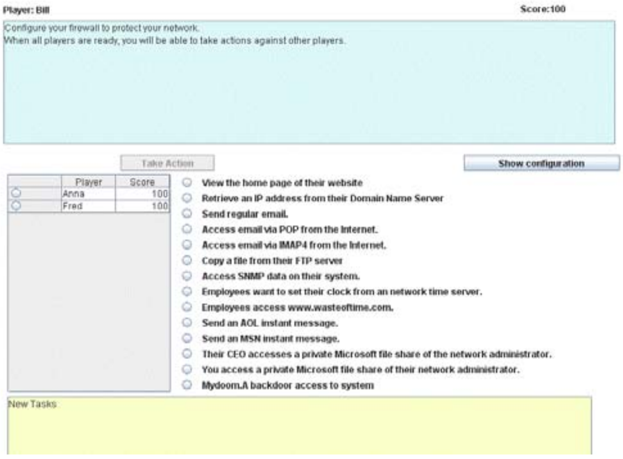


Fig. 1. Firewall simulator architecture

The general architecture of the firewall simulator is shown in figure 1. The student participants run a Java applet that is executed in their browser. There is also an administrator's console applet that allows the instructor to control aspects of the simulation. A Java application runs on the web server to facilitate communication between participants and to determine the results of any actions taken between participants. The web server holds the web pages containing the applets, instructional help files, diagrams of the simulated networks as well as XML formatted simulator configuration files.

When students view the firewall simulator webpage, they are required to enter their name. After this, they see the screen shown in figure 2. Their name is displayed at the top along with their current score. Scores start at 100 and can go up or down depending on how well the student configures their firewall and the level of actions taken against them. The names and scores of the other students participating in the simulation appear in the list on the left. Next to the names is a list of simulated actions the students can take against other players' networks. Many of the actions do not have any impact until a configuration change is required. For example, the sending of instant messages through the firewall should be initially prohibited until a new task requires the student to change their firewall configuration to allow them. To take an offensive action against another participant, the student selects their victim from the list of players, picks the action to be taken and then clicks the "Take Action" button. A student must wait a minute before repeating the same action against the same student. This gives the victim a chance to correct their firewall configuration before another attack from the same student.



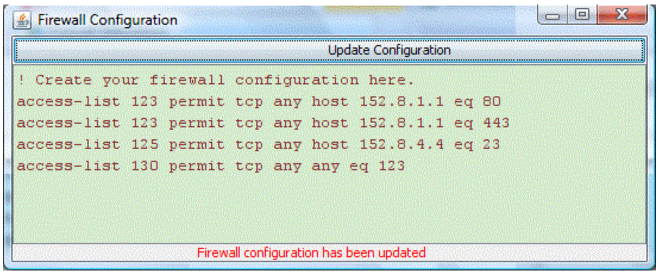
Configure your firewall to protect your network.
When all players are ready, you will be able to take actions against other players.

	Player	Score
○	Anna	100
○	Fred	100

- ○ View the home page of their website
- ○ Retrieve an IP address from their Domain Name Server
- ○ Send regular email.
- ○ Access email via POP from the Internet.
- ○ Access email via IMAP4 from the Internet.
- ○ Copy a file from their FTP server
- ○ Access SNMP data on their system.
- ○ Employees want to set their clock from an network time server.
- ○ Employees access www.wasteoftime.com.
- ○ Send an AOL instant message.
- ○ Send an MSN instant message.
- ○ Their CEO accesses a private Microsoft file share of the network administrator.
- ○ You access a private Microsoft file share of their network administrator.
- ○ Mydoom.A backdoor access to system

Fig. 2. Firewall simulator student client

The text area at the top of the screen displays messages to the student. When a student takes an action against another student, a notice appears in the message area telling each student of the success or failure of the action and if any points have been awarded or deducted. New tasks or required configuration changes are announced in the lower text area. When a student clicks the "Show configuration" button, he or she will see a small separate window displaying their firewall's configuration, as shown in figure 3. This window is displayed simultaneously with the other messaging window. In the configuration window, the student can enter the Cisco-like configuration statements to define his or her firewall. When the student believes his or her configuration is correct, he or she presses the large "Update Configuration" button at the top. The system will check their configuration for syntax errors. If any errors are detected, a detailed message will display at the bottom of the screen. When the configuration is syntax error free, the student's simulated firewall is updated.



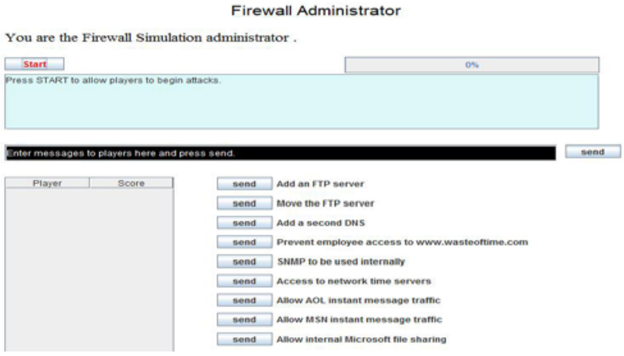
```
! Create your firewall configuration here.
access-list 123 permit tcp any host 152.8.1.1 eq 80
access-list 123 permit tcp any host 152.8.1.1 eq 443
access-list 125 permit tcp any host 152.8.4.4 eq 23
access-list 130 permit tcp any any eq 123
```

Firewall configuration has been updated

Fig. 3. Simulated firewall configuration screen

There is an instructor's web page, shown in figure 4, that controls the simulation. The instructor can start and stop a simulation session, add new configuration requirements and broadcast messages to the students. When students initially log onto the simulation, they may configure their simulated firewalls, but they are not allowed to take actions against other students. When all students in the lab are ready to participate, the instructor clicks "Start" to unlock the "Take Action" feature. The administrator can select from a list of configuration changes. Enabling a change sends an explanatory message to the students and requires the students to make a change to their firewall configuration. The students have 45 seconds to update their firewall before other students can take any action against them relating to this configuration change. A "speedometer" on the administrator's page shows the level of activity as the actions per second. When student activity starts to drop, the administrator can require another configuration change.

After initially configuring their firewall, students actively engage in taking actions against other students. Students learn that their firewall is improperly configured when the system informs them that another student has scored points against them. Changes in configuration requirements keep the student busy considering the appropriate configuration for their firewall. Rapid feedback enhances the learning environment.



You are the Firewall Simulation administrator .

Press START to allow players to begin attacks.

Enter messages to players here and press send.

- send Add an FTP server
- send Move the FTP server
- send Add a second DNS
- send Prevent employee access to www.wasteoftime.com
- send SNMP to be used internally
- send Access to network time servers
- send Allow AOL instant message traffic
- send Allow MSN instant message traffic
- send Allow internal Microsoft file sharing

Fig. 4. Administrator's controls

V. Experimental Results

The Interactive Firewall Simulator has been used in several classes at North Carolina A&T State University including Networked Computer Systems, Information Privacy and Security, Applied Network Security, and Security Management for Information Assurance. Students gave very positive feedback.

We also demonstrated the Interactive Firewall Simulator in the 2008 Faculty Development Workshop on Cyber Games and Interactive Simulation. The workshop took place from June 22 to June 28 at University of North Carolina at Charlotte. Eighteen faculty members, who came from different universities and colleges, attended the workshop. In an evaluation survey of those who attended the workshop, the firewall simulator received some of the highest ratings. The firewall simulator was made available to the workshop participants and several of them have used it at their universities.

VI. Conclusion

We designed and implemented an Interactive Firewall Simulator that provides a friendly interactive tutorial, step by step demonstrations of firewall configuration and how firewall works. Students can use the simulator to configure a firewall, to simulate an attack, and to prevent attacks. This simulator helps students better understand the concepts of firewalls, firewall configuration, and functions of firewalls.

Students’ feedback reflected that it was a very friendly, helpful and easy to use simulator. The level of excitement generated by the competitive nature of simulator is obvious to the instructors. By using this simulator students can quickly learn and practice configuring a firewall, and get hands-on experiences. This Interactive Firewall Simulator can be used in any classes involving network security techniques. The simulator source code and executables are available for instructors at http://williams.comp.ncat.edu/firesim/

REFERENCES

[1] A. Conklin, “Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course”, *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*, January 2006.

[2] E. Al-Shaer, A. El-Atawy, and T. Samak, “Automated Pseudo-live Testing of Firewall Configuration Enforcement”, *Proceedings of IEEE Journal on Communication*, Vol. 27, 2009.

[3] R. Tibbs, and E. Oakes, “Firewalls and VPNs: Principles and Practices”, Prentice Hall, 2006

[4] Cisco IOS Firewall Configuration Examples and Technotes. [Online]. Available: http://www.cisco.com

[5] J. Garrido and T Bandyopadhyay, “Simulation Model Development in Information Security Education”, *InfoSecCD '09 2009 Information Security Curriculum Development Conference*, Kennesaw, GA, Oct. 2010

[6] M. Ye and K. Sandrasegaran, “Teaching about Firewall Concepts using the iNetwork Simulator”, *Information Technology Based Higher Education and Training, 2006. ITHET '06. 7th International Conference,* Ultimo, NSW, July 2006

[7] C. Irvine, M. Thompson, K. Allen, “CyberCIEGE: gaming for information assurance”, *IEEE Security & Privacy,* vol. 3, no. 3, May-June 2005

[8] X. Wang G. Hembroff, R. Yedica, “Using VMware VCenter lab manager in undergraduate education for system administration and network security”, *Proceedings of the 2010 ACM conference on Information technology education*, Midland, MI, October 2010

[9] J. Hu, D. Cordel, C. Meinel, “A Virtual Laboratory for IT Security Education”, *Proceedings of the Conference on Information Systems in E-Business and EGovernment (EMISA),* Luxembourg, Oct 2004

[10] K. Stewart, J. Humphries, T. Andel, “Developing a virtualization platform for courses in networking, systems administration and cyber security education”, *Proceedings of the 2009 Spring Simulation Multiconference*, San Diego, CA, 2009