# Secure Online Examination Architecture Based on Distributed Firewall

Chi-Chien Pan, Kai-Hsiang Yang, and Tzao-Lin Lee

*Department of Computer Science and Information Engineering,*
*National Taiwan University, Taipei, Taiwan, R.O.C.*
*E-mail: {d5526001, f6526004, tl_lee}@csie.ntu.edu.tw*

## Abstract

*Online (Web-based) examination is an effective solution for mass education evaluation. However, due to the incomplete of network security, students can communicate with each other, and we can't prevent the cheating. Therefore, keeping the security of a online examination has become an important issue. This paper focuses on how to implement a secure environment for online-examination in the general academic network environment without the need of special network topologies and hardware devices. It not only reduces the system administrator's load, but also enhances the system flexibility to fit every teacher's needs. We use (1) the distributed firewall techniques to control the network packets of all machines, and (2) the centralized security policy management to control the security policies for all machines. Beside the above mentioned , we also design some mechanisms to prevent the possible network attacks and cheating, which enhance the security of the online examination environment.*

## 1. Introduction

Many teachers prefer to conduct online examinations for their courses which are suitable for online examination, such as programming language, etc. This method could evaluate student's achievement, and helps teacher to give fair scores. However, due to the incomplete of network security, students could communicate with each other via the network without the permission by teacher.

During the online examination, all student computers need to connect to the examination server for getting the examination subjects, but some cheating behavior should be stopped, such as privately talking, referencing forbidden data, and answering for others, etc. It is very important to have some mechanisms for controlling all network behavior. Online examination could be hosted in many forms. Sometimes students are distributed to many remote sites, and it is impossible to control and monitor students' behavior, such as talking by phone or cellphone. Therefore, our research focuses on the general academic network environment: during the assigned time, students are gathered into the computer classrooms, taking the online examination under the forbiddance of talking to each other.

Usually the computer classrooms for online exami-nation are under open network environment and may have many different kinds of network topology. It is not easy to deploy additional devices such as firewall, proxy, and NAT server, etc. Some additional limitations exist for the computer classroom. (1) Because the computer classroom is a public place, we can't arbitrarily change the system configuration. (2) After finishing the examination, all configurations must immediately be restored as before.

In order to support using the system concurrently, the online examination servers can locate outside the classroom, usually at the lab. The examination servers must be able to reject the unauthorized connections from those machines which are not under control of our system. During the examination, all student machines can not connect to others except those allowed IP addresses and protocols. For those allowed destinations, student machines can transparently connect to them, without any extra configuration.

Conventional firewall is the basic protection of the enterprise network. It blocks unwanted connections to and from the network, but it can not filter traffic inside the Intranet. This is insufficient to meet our requirement.

Personal Firewall technique then made up the firewall shortage. It provides the capability to control each separate machine, prevents viruses, Trojan horses, and unauthorized sending data via network. However, it is also insufficient. It lacks an efficiently mechanism to update the security policy. To address the shortcomings of conventional firewalls and personal firewalls, the concept of a distributed firewall [1] has been proposed. In this scheme, security policy is still centrally defined, but enforcement is left up to the individual endpoints. By using the properties of distributed firewall, the centralized management rules and distributed control, we could implement one secure online examination environment.

In this paper, we introduce the details of constructing the whole secure online examination environment: section 2 lists the related researches and technologies in this area. Section 3 addresses the system architecture and operations. Section 4 outlines the security mechanism of the system to against some possible attacks. Section 5 describes the implementation details and related technologies. Finally, last section is the conclusion and suggestions for future work.

## 2. Related work

We firstly make a brief comparison with the conventional firewall, personal firewall and distributed firewall in order to design the whole architecture. There had been some technical literatures [2, 3, 4] address and focus in this field.

For the comparison with conventional firewall and distributed firewall: Conventional firewall relies on restricted topology and controls network devices to enforce traffic filtering. In this model, all the inside members are completely trusted and firewall can not stop the attacks from them. On the other hand, the distributed firewall is topology independence. With the distributed firewall, all machines are protected all the time. It also supports more detail control such as the application level control.

For the comparison with personal firewall and distributed firewall: Personal firewall lacks of the centralized security policy management mechanism. It is very inefficient and inconvenient for system administrators to update the rule. For the distributed firewall, it has the centralized policy management, and it is invisible and no user intervention required. For the technique about firewall, to establish the distri-buted firewall must combine many techniques of the conventional firewall and personal firewall, including the access rule design and the packet filtering technique etc. On the other hand, Windows platform is still the most popular client at the present time. To develop the distri-buted firewall under Windows contains many details, Vadim V.Smirnov did the analysis of the integrity and comparison for different personal firewall techniques under Windows platform [5]. Other techniques, such as Windows DDK [6], and the Network Driver Interface Specification (NDIS) are also needed.

## 3. Architecture

In this research, the system that we establish basically could be divided into three parts: teacher (Server), teaching assistant (Manager), and student (Client). The system structure is shown in Figure 1.

The client is used for students during the examination, and it is passively to accept the control only. There are three modes for client: green light, red light, and yellow light. Green light is under general situation, the machine works like usual and user can't feel the existence of the control system. Red light is the forbidden mode in the beginning of the examination. All network accesses are stopped under this mode, and user can't send any packet in addition to login to the Manager. Yellow light shows it is in the process of the examination. The light will change from red to yellow after all users login, at the same time the Manager sends Client the security policy, including the allowed IP addresses and ports about the Servers. All the unauthorized machines can't use the network. The client mode conversion model is shown in Figure2.

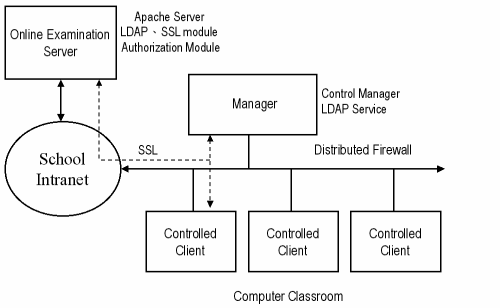


**Figure 1. System Structure**

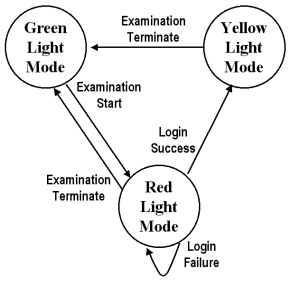


**Figure 2. Client Mode Conversion Model**

The main function of Manager is to control and monitor the whole process of examination. From the beginning of examination, it accepts the login messages from client, monitors the on-line situation, delivering the security policy to client, until the end of examination. The Manager stores user information into the LDAP server [7, 8] through the SSL connection. And then Server could retrieve the MAC, IP address, and username of each student, in order to filter the connection and prevent others from taking the examination.

The Server is mainly to provide the Web-based environment for the examination. Through the authorization module and secure connection to LDAP server, it could

get the information about students, and identify each student. The scenario of the system is as follows:

1. In general situation, the client shows the green light.
2. When it is time to start the examination, the Manager chooses the exact examination first, because there maybe some examinations at the same time. Manager obtains the key for this examination, and broadcasts to all machines for their response.
3. Client gets its key and replies some information to Manager, including MAC, and IP address etc.
4. Manager continues to broadcast and accepts the response in limit time, and will refuse the response when exceeding the limit time. According to response from machine, Manager could get the list of controlled machines, and sends the switch command to client for red light.
5. Student inputs the username and password to Client, then Client send the information to Manager for the authentication. Manager identifies it and dynamically generates a temporary ID and PASSWORD, which are different from the username and password. This method is mainly to prevent the connection to Server from outside machine. Then Manager sends them to client for the authentication on Server. At this time teaching assist also identifies each student in the classroom to prevent the cheating.
6. Manager stores the information including login IP, MAC, username, and the dynamically generated id, password pair into the LDAP server.
7. The examination starts, and Manager broadcasts the command to enable the control on all machines. The client program turns to the yellow light, and setups the allowed IP, protocols, and ports according to received security policy.
8. Client browses the web server via SSL connection, and has to input the id and password to take the exami-nation. In order to prevent some students from login for others, each client program forbids to login different username. If there is special need for doing so, it must be set up by Manager.
9. When the examination ends, Manager broadcasts the end command, all client turns into the green light.

For multiple examinations, each has its own encryption/decryption key, and the packet with different key will be ignored. Therefore they won't inference to each other.

## 4. Security Protection

The security design is the most important part in the distributed firewall. Because all control policy is sent through the network, the whole protection mechanism will break down if the transmission suffers the attacks such as duplication, forging and distorting etc. The security protection mechanism of distributed firewall is installed in the client, therefore the encryption/ decryption method and keys are very easily known. We adopted the asymmetric encryption/decryption algorithm with the public and private key. The length of key is also large enough in order to prevent the attack using the brute force method.

We reference PuTTY[9] source code, rewrite the memory management and fix some memory bug, to implement the 1024-bits RSA encryption/decryption mechanism [10] for the packet transmission. For the key generation and transmission, we setup all the key pairs of examinations in advance, like the PGP [11] method. Due to the examination classroom is under our control, it does not need to transmit the keys during examination, to avoid suffering the attacks.

In addition to the basic encryption/decryption method for the packets, we also design some mechanisms to prevent attacks:

1. We choose the ICMP echo reply packet format as the control packet format. The control commands are encrypted and then attached to the packet tails. It just looks like the general ping reply packet if you don't understand it or the key is incorrect, and it doesn't inference the operation of TCP/IP stack. For the hacker using sniffer program, the simple ICMP echo reply packet is not particularly outstanding. On the other hand based on the RSA encryption mechanism, we use the random bits to extend the content, the same control commands will become different packets after encryption. Therefore, hacker has no idea to do the analysis.
2. One-time password is used. For preventing the sniffer program to record all the packets, resending them to cause the system confusion, we design the one-time password mechanism. Each time the Client receives the command for changing mode, and it immediately generates a new password for next time, sending it back to Manager. If the commands from Manager with wrong password then Client ignores it. Therefore if someone records the previous packet and resends it, it will be dropped by Client because its one-time password already changed.
3. IP/MAC Spoofing: For preventing the IP and MAC spoofing, each packet contains its IP and MAC into the encrypted content in addition to the normal header. Therefore the mechanism could effectively solve the man-in-the-middle problem [12, 13].

## 5. Implementation

Because the Windows platform is still the most popular operation system, we choose the Windows as our implementation platform (Win98, Win2000, WinXP). The Apache Web Server[14] is chosen as the online exami-

nation server. OpenLDAP is as the directory service. Other developing tools include Visual C++ 6.0, Windows Device Driver Development Kit, Windows Resource Kit [15], and Windows Packet Capture Library [16] etc.

In order to prevent user arbitrarily unloading the distributed firewall, the control part of client program is developed as the device driver which residents in the system kernel and under the protection of operating system. The control part in the device driver layer just supports few I/O function calls, for example input the username and password only, and send back the current mode etc. For safety reason, it can't support uninstall function for client interface.

We make use of the NDIS Intermediate and NDIS Hooking techniques to implement the packet filtering function. In the Manager part, we use the packet driver interface WinPCap [16] to transmit packets and connects the OpenLDAP server by SSL mechanism for storing user information. For the design of Server, due to the Web form of examination, we implement Apache module to retrieve the student information from the OpenLDAP server, and authenticate the student. By considering the security, the control packet format is extended from the ICMP echo reply format. Figure 3 shows its format and related details.

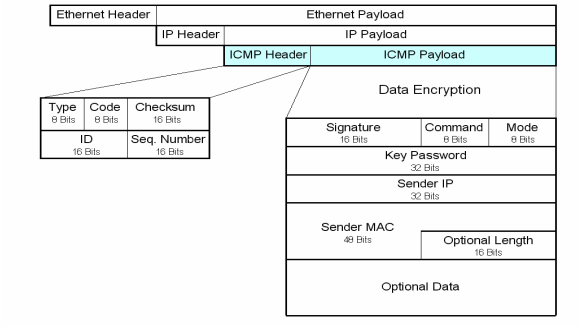


**Figure 3. Basic Network Packet Format**

Packet is divided into ICMP Header and Payloads. In the Header, we use type 0, which means Echo Reply, and the special code, 0x99, as the identification of our control packet. In the Payload, the 'Signature' field contains two characters used to make sure whether the packet is correctly encrypted, and otherwise the packet will be ignored. The 'Command' field is the command code. The 'Code' is the client mode. The 'Key Password' is the 32-bit one-time password. The 'Sender IP' and 'MAC' fields come from the IP header and Ethernet header, and are used for protecting the packet.

## 6. Future Work

In this paper, we investigate the distributed firewall technique on constructing a secure reliable online examination environment. However, it is just a beginning. After actually testing and measuring, we believe that there are still many topics need to be continuously researched and developed in the future:

(1) Security audit logging, reporting and alerting

We can enhance the system audit function by monitoring the behavior of manager, client, and server. If some security events happened, it could be handled immediately. And if the students cheat, the related logs are the substantial evidence.

(2) Enforcing security policy

The current access control functionality of our distributed firewall is governed by packet filter rules. We can enhance our firewall by combining lower layer access control with upper layer application functionality, and we can set the policy for some specific applications.

(3) Improving security between client and manager with digital certificate .

(4) Support for other platforms.

## 7. Reference


[1] Sotiris Ioannidis, Angelos D. Keromytis, Steven M. Bellovin, and Jonathan M. Smith, "Implementing a Distributed Firewall", ACM Conference on Computer and Communications Security, Athens, Greece, November 2000.

[2] Steven M. Bellovin, Distributed Firewalls, November 1999. <http://www.research.att.com/~smb/papers/distfw.html>

[3] Daniel Wan, Distributed Firewall, May 2001, <www.giac.org/practical/gsec/Daniel_Wan_GSEC.pdf>

[4] Wei Li, Distributed Firewall, December 5th, 2000. <www.cs.helsinki.fi/u/asokan/distsec/documents/li.ps.gz>

[5] Vadim V.Smirnov, Firewall for Windows 9x/NT/2000, <http://www.ntkernel.com/articles/firewalleng.shtml>

[6] Microsoft Windows Driver Development Kits, <http://www.microsoft.com/whdc/ddk/winddk.mspx>

[7] OpenLDAP Project, <http://www.openldap.org>

[8] Ellen Smith, 'Securely Implementing LDAP', SANS Institute, July 2001.

[9] PuTTY: A Free Win32 Telnet/SSH Client, <http://www.chiark.greenend.org.uk/~sgtatham/putty/>

[10] Cetin Kaya Koc, High-Speed RSA Implementation, RSA Laboratory, Nov. 1994, <ftp://ftp.rsasecurity.com/pub/pdfs/tr201.pdf>

[11] The International PGP Home Page, <http://www.pgpi.org>

[12] Bhavin Bharat and Bhansali, 'Man-In-the-Middle Attack - A Brief', SANS Institute, Feb. 2001.

[13] Robert Wagner , 'Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks', SANS Institute, Sep. 2001.

[14] The Apache Software Foundation, <http://www.apache.org>

[15] Microsoft Windows 98 Resource Kit, <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/win98/reskit/win98rk.asp>

[16] WinPcap: the Free Packet Capture Architecture for Windows, http://winpcap.polito.it/