TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

Bachelor's Thesis

Control E-Commerce Security

Yucheng Wu

Turku University of Applied Sciences
Degree Program in Information Technology
December 2009

TURKU UNIVERSITY OF APPLIED SCIENCES

ABSTRACT OF THESIS

Abstract

Degree Programme: In Information Technology	
Author: Yucheng Wu	
Title: Control E-commerce security	
Specialization line: Data Communication	Instructor: Vesa Slotte Language Correction: Kalliopi Skarli
Date: December 2009	Total number of pages: 40
Electronic commerce has been very popular in the recent years. However, security is one of the barriers, which affects the development of E-commerce. How should merchants of E-commerce solve this problem and maintain a secure environment for their customers? How do customers protect their confidential data when they are shopping on-line? This thesis discusses various common attacks, and presents the protection solutions according to those attacks. Because attacks may take place on the customers and the sellers site, the method of defense has been discussed from these two sides. Furthermore, this thesis has provided the basic plan for developing an E-commerce site, which includes E-commerce security policies design and disaster recovery plan. The goal of this thesis is to provide the basic security knowledge of E-commerce for merchants and customers, and help them to confidently run a safe E-business and conduct shopping online safely.	
Keywords: E-commerce, security	
Deposit at: Library of Turku University of Applied Sciences	

Foreword

Although E-commerce is a young business model, it is not anymore new for us. The same applies to Security of E-commerce. It is still developing since attackers will always find new ways to attack. It will be helpful to find out basic strategies for SMEs to protect their E-commerce system.

This work is my Bachelor's thesis at Turku University of Applied Sciences, under the supervision of Mr. Vesa Slotte. I would like to thank first of all my parents for their continuous support from the start of my study as well as my all professors and good friends.

I was waiting for this moment to thank people with whose support and encouragement I managed to complete my Bachelor's Degree and write this document.

Yucheng Wu

Contents

1. Introduction to E-Commerce Security

Security in the virtual world of the Internet is even more confusing than in the real world we inhabit [1]. The world of the Internet has been built by various protocols, rules, and software applications, however, all of these elements may exist bugs, which may be the threat of Internet users. Especially, nowadays, the applications and systems are designed complicated to provide attractive functions, but the more complicated applications and systems produce the less secure E-environment.

1.1 Definition of E-commerce

E-commerce is electronic commerce, which is purchasing and selling products or service over electronic network, such as Internet. E-commerce provides a platform for difference business models, it includes business to business and business to consumers and even consumers to consumers. There are amount of retails or companies build their own web site to join E-commerce, E-commerce brings a lot of benefit to their business.

1.2 E-commerce security overview

Security plays a significant role in the business field, so it is necessary to understand how to keep a safe E-commerce environment. Firstly, let us take a look at different members of an E-commerce network. Actually, we may divide those members to four major parties or actors. The first one is shoppers who visit a web site and choose the product or service they want to order, and making a purchase. The second one is a merchant who is running his/her business on servers. There are many kinds of software that need to be installed on the server, and most of software is bought from the third party, which is the last legal player in an E-commerce network. The fourth party are attackers who are the dangerous to the whole E-commerce network. Based on the above introduction of the parties involved, it is easy to see that malicious hackers threaten the whole network.

There is an old Chinese saying that you will never be defeated if you know everything about your opponents, so thinking as an attacker is one way to protect E-commerce. This document will explain how malicious hackers attack an E-commerce system, how should

administrators protect an E-environment by using different methods, and what precautions should be taken to prevent an attack.

Figure 1.2 briefly displays the methods the hackers use in an E-commerce network. The thesis will explain the attack methods according to Figure 1.4 and propose the defence methods as well.

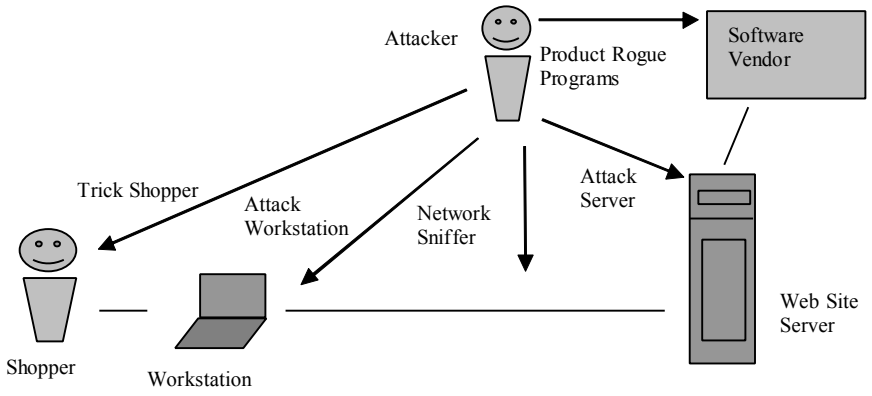

Figure 1.2 Target points of E-commerce topology

2. Attack Method

Figure 1.2 clearly displays the main target points in an E-commerce network. In this section, we will discuss the basic attack methods malicious hackers may use. Those attack methods will provide the essential security knowledge to both merchants and shoppers.

2.1 Tricking shoppers

Tricking shoppers is the easiest and most profitable attack method in E-commerce. Basically, attackers trick shoppers to acquire their personal information, such as password, the challenge questions' answer, bank account and so on. The most common method used by attackers is the social engineering attack. Attackers may firstly obtain shoppers' trust by calling or sending Emails to them, and then attackers start to ask for the shoppers' personal information. Having acquired this personal information, attackers may be able to steal shoppers' money from their E-bank account. The other method is using network technology to redirect shoppers to visit a bogus web site, which may look same as the original one shoppers want to visit. Once shoppers login to this fake web site, the web server will remember all of the shoppers' information. Later, attackers may use those shoppers' user names and passwords to login to the real web site and steal their money. For example, shoppers want to go shopping online, and the address of web shop is www.ebay.com, attackers may mislead shoppers to login to the web site www.ebuy.com. The content of this fake web site might look exactly same as EBay site in order to lead the victims enter their personal information and save it.

2.2 Guessing passwords

Guessing passwords is the other method attackers might use. However, it requires that attackers must be familiar with some certain shoppers' personal information, such as shoppers' birthday. This personal information is often to be set as the shoppers' password. Guessing passwords requires a lot of work, so attackers design some software to guess passwords. The software will try different combination of numbers and letters until the correct password is found, so the attackers could directly login to shopper's account. For

example, a dictionary attack is one kind of guessing password software. The password-cracking program takes a word from the dictionary file and tries the word as a password to access a computer [2].

2.3 Attacking the workstation

Attacking the workstation is another option to attack shoppers, therefore, the attackers need to find a weakness on the shoppers' computers. Unfortunately, weak points always exist in a workstation since there is not any perfect system in the world which means that all systems have vulnerabilities. Due to this reason, the attackers may access shoppers' systems after they have found vulnerabilities successfully. SANTAN is the one of popular scan port software, which could help attackers to detect the entrance of the shoppers' workstation. Upon entry, the attackers scan all of shoppers' files and systems to gain their password, or other confidential data.

2.4 Sniffing the network

During a shopper’s visit to a web site, the communication between the shopper’s s and server’s workstation is started. In this communication, both sides will exchange data with each other. However, the network communication is different from human communication; one side of communicator will break information into small pieces, which we call packages before sending data, and the other side will reconstruct them to read the complete information. Normally, attackers will choose a place, which is close to the shopper’s side or web site to sniff information. If a sniffer is set in the middle of the link between shoppers and sites, it is impossible to collect complete information. For instance, a Chinese local shopper wants to order a product from a web shop located in Turku south of Finland, the Chinese shopper's workstation will send an order message, which may be divided to several packages to the Finnish web server. This Chinese workstation might send first five packages through a Russian station to Turku, and other packages routing from Sweden to Turku. In this case, if a sniffer is set only in Russia means this attacker will lose all other packages except the first five. With these five packages, the attacker can probably not

analyze what information has been delivered. That is why attackers normally set the sniffer as close as possible to the shopper's or the server's side and this notifies shoppers and web site administrators that the sniffer might be located very close to them.

2.5 DoS attacks

Denial of Service is one effective attack method to impact servers, and it is shortly referred to as DoS. The aim of this attack is to deny victim(s) access to a particular resource. Based on this definition, DoS attack includes many different ways. UDP flood, ICMP flood and Smurf attacks are the most representative examples of DoS. Firstly, we take a look at the UDP flood attack. Attackers apply chargen service, which can test the connection of network devices, to occupy the bandwidth of web server, since chargen service will send character streams to a destination until the destination closes the connection. In this case, attackers send a special form of request to the first victim. This special request has a modified source address and port number. This spoofed address and port number mislead the first victim to sending all chargen traffic to the second victim's echo port. Echo service will forward all data back to sender. On its way, endless data will travel in the between the first victims and the second victims.

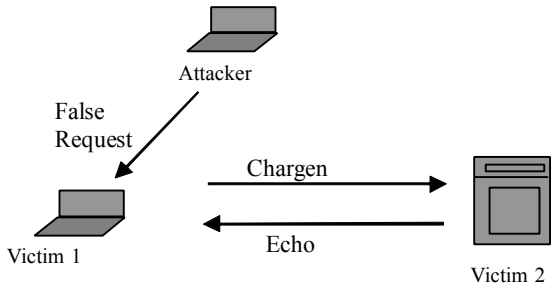

Figure 2.5.a UDP Flood

Secondly, the SYN attack is another example to be discussed. Before explaining the SYN attack, it is necessary to understand how TCP establishes connections using the three-step handshake. The three-step handshake is the way TCP provides a reliable connection between shoppers and servers. Firstly, the shopper side sends a SYN message as a request message to the server side. The server responds with a SYNACK (SYN acknowledgement)

to inform the shopper side. In the end, the shopper side will reply with an ACK (acknowledgement) after receiving a SYNACK message from the server side. A SYN message contains the basic information of the shopper side, so the server side will keep that information until shopper sends an ACK message. If the shopper does not reply with any messages after receiving the SYNACK, server side will keep shopper side information after some timeouts. Furthermore, the server usually has a limited amount of memory to store SYN information from shoppers. Basically, the SYN attack utilizes the feature of the three-step handshake to occupy the server's memory in order to deny the access to real shoppers. Attackers send a number of SYN messages with a spoof source address to a target server, and the fake source address leads the server replying with SYNACK messages to the destination, which might even not exist. This means that the server has to store SYN messages in certain places until timeouts, and those SYN messages may consume all the memory of storing the SYN message.

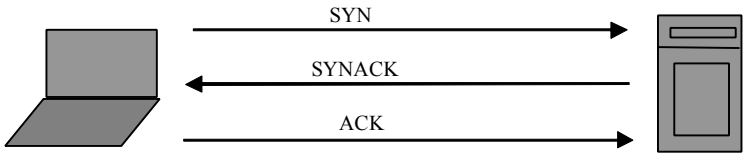

Figure 2.5.b TCP tree-step handshake

Smurf is one type of DoS attack as well and it generates a huge amount of traffic to the victim's network by using broadcast ping messages. Firstly, the attackers broadcast an ECHO_REQUEST message to the whole network, so that all hosts of network will reply to ECHO_REPLY message after having received an ECHO_REQUEST. Because the attackers modified the source address of the target victim, so all hosts will forward ECHO_REPLY messages to the final victim. The huge amount of ECHO_REPLY messages will block the network.

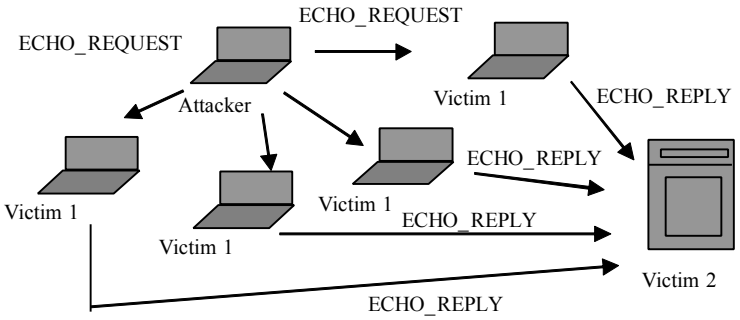

Figure 2.5.c Smurf attack

Since these examples are only attacks by a small group of malicious resources, the server side may still have enough bandwidth or memory to offer to real shoppers. In this case, the attackers design other action to occupy more resources of bandwidth or memory. Let us take the DDoS (Distributed Denial of Service) attack to see how it works. There are several steps to implement a DDoS attack. Firstly, the attackers need to infect some work stations, which can be located in different places as their slaves, so those slaves will wait for the attackers' command. Each of these slaves will control many other slaves to attack or occupy the final target servers' systems. The first layer slaves which are controlled directly by attackers will be called handlers. The slaves controlled by handlers are called agents. This kind of attack construction will help the attackers to consume a lot of target network resource. If the target server blocks or discovers one set of agents, the attackers only need to change to a new handler who controls a new set of agents.

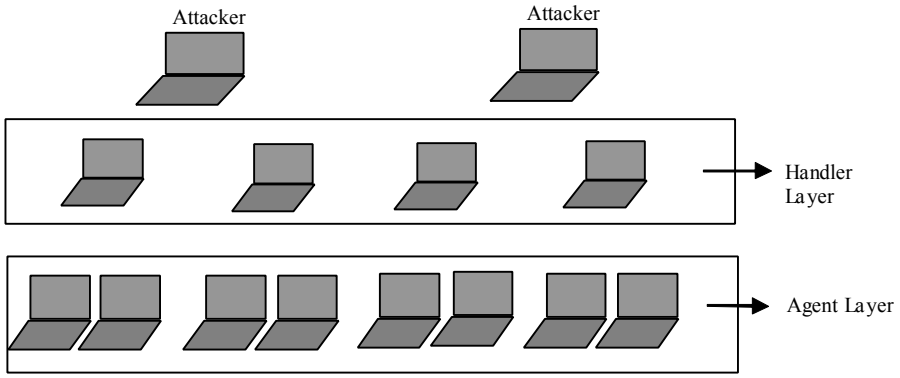

Figure 2.5.d Distributed Denial of Service network

2.6 Attack by known bugs

This attack method can be used on both of the shoppers' workstations and the merchants' system. The attackers firstly use available tools to verify which software the target workstation/server is using. After that, the attackers need to find patches of the software and analyze which bugs may not be fixed by administrators. With those unfixed bugs, the attackers may exploit the system.

2.7 Buffer overflow

If an attacker has gained access into the root of site, it means all of the E-commerce users' information is gained. The buffer overflow is the most common method used by the attackers to access the servers' kernel.

Buffer overflow: Over 70% of vulnerabilities that have been recorded have a buffer overflow in the exploit somewhere [3]. Let us see how this buffer overflow works. Actually, a buffer is the place which temporarily stores data, and each buffer has a limited space. When attackers set overwritten data into a buffer which does not have sufficient space to keep the data, the extra data will overflow into an adjacent buffer, which may contain other data. In this case, those data stored in the adjacent buffer will be replaced by overwritten data. Once the system invokes the data, which are stored in the adjacent buffer, those overwritten data will be executed. Normally, attackers will design those overwritten data in order to gain access into the root of system after system has been running overwritten data.

Figure 2.7 Buffer overflow

2.8 Attack from HTML code

There is no doubt that most of the web sites include HTML documents. This Section explains how malicious hackers find sensitive information from HTML code, and how they could use SSI commands to control the web server. Furthermore, this Section discusses the disadvantages of embedding unknown applets into a web site.

2.8.1 Information in HTML

Shoppers can read HTML codes from the browser which means that if HTML codes contain sensitive information, an attacker might benefit from it. Take the Firefox browser for instance, users can find HTML code by clicking ***View*** and selecting ***Source***, or pressing Ctrl and u at same time. The following example will illustrate how an attacker verifies the sensitive information from HTML codes.

```
<!— Note to developers, please use the following directory structure  /inet/html /inet/cgi-bin  /inet/dev —>
<HTML>
<HEAD>
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=windows -1252"> <META NAME="GENERATOR"
CONTENT="Microsoft FrontPage 4.0">
<META NAME="ProgId" CONTENT="FrontPage.Editor.Document"> <TITLE>Welcome</TITLE>
</HEAD>
<BODY>
<P>Welcome to our Web site</P>
<P><IMG BORDER="0" SRC="file:///C:/inet/brick.jpg"></P>
</BODY>
</HTML>
<! — Further information can be acquired from the Administrator at (555)555-5555, ext. 1234 or via email at
mcross@microsolved.com—>
```

Program 2.8.1 [4] Target HTML code for attacker

The highlighted parts show the sensitive information in the HTML source. The first line of highlight is the note from the administrator, explaining the directory structure. HTML documents are stored under the directory of /inet/html, the CGI (Common Gateway Interface) script is located in /inet/cgi-bin, and the web site is saved in the /inet/dev. The second highlight part displays the structure of directory as well. In the endcome the administrator's notes which contains the administrator’s contact information. In this example, it reminds web administrators to review all the posted web pages of HTML codes and remove or change the sensitive information if it is found. Furthermore, administrators have to configure proper permissions to the directory on their site as well, so visitors can not access the directory.

2.8.2 Server Side Includes (SSI)

SSI is the command controlling the web server, which can be embedded into HTML codes. This is another security problem has to be addressed. Firstly, let us take some examples to see how attackers utilize SSI.

```
Example 1
The current time is <!-#echo var="DATE_LOCAL"->

Example 2
<!-#include file="email.htm"->

Example 3
<!-#exec cgi=" /cgi-bin/test.pl"->
```

Program 2.8.2 [5] Target HTML code for attacker

The sign (#) indicates to the web server that the following code is the SSI command. In Example 1, "echo" is the command, which requires that a web server prints certain data to the client browser. The code of "var=" leads the server to find a variable which is called DATE_LOCAL, so the web server will print current local time to client browser. By changing the variable, the attackers may utilize the echo command to print the information they need. For instance, the attackers can modify the variable of example 1 to DOCUMENT_URI, which is other common variable in SSI, and DOCUMENT_URI displays to the attackers current document names and path. In the second example the "include" command tells the web server to invoke another file into the HTML documents, so that shoppers will see the text or pictures from the "email.htm" file in this case. If an administrator does not set proper permission of sensitive documents, an attacker will use the "include" command to find the content of those documents, which may include the shoppers' credit card number or other information. The command "exec" executes the program on the system or runs the shell scripts' file. The attackers may control the web server by using this command with another technique. If a web site does not need this command, its administrator could disable it by selecting "IncludesNOEXEC" option.

These examples are the most common attacking methods using SSI commends, so an administrator has to be aware of setting permissions properly if the web site applies the SSI function. Most web servers turn on SSI function automatically, so the web sites should turn

off this function when they do not need it. Network administrators could use a firewall to block SSI if it is impossible to disable it from the web server.

2.8.3 Java, JavaScript, and ActiveX

Java is a programming language developed by Sun Microsystems, and it is often used to make applets. These applets can be embedded into HTLM codes, and they will run on the shoppers' system when shoppers download the HTLM codes to their computers' memory. These applets may become the attackers' targets. The attackers can distort the Java program and set a computer worm into the program. When the shoppers are visiting the web site, they download HTLM documents, which contain viruses to their computers' memory and those worms are stored into the shopper's system. The result of this attack affects the shoppers' computers, but it does not affect the web server. But shoppers will realize which web site this virus comes from after their system has been damaged. The consequence will decrease the credit reputation of a web site. ActiveX work quite similarly to Java applets; it is embedded in HTML documents and runs applets after the shoppers have downloaded them into their computers' memory. The difference between Java and ActiveX is that Java can be run on virtually any operating system, including Windows, Linux, and Macintosh, whereas ActiveX components are distributed as compiled binaries, so they will only work on the operating system for which they were programmed [6]. Basically, ActiveX is originally only working with Internet Explorer. Due to this security issue, Microsoft has published a component named Authenticode for verification of ActiveX controls. When a web page attempts to install an ActiveX control, Authenticode verifies the publisher of a digital signature in order to make sure the original code has not been modified by attackers. How about JavaScript? JavaScript is a programming language which can be executed on the client browser and it allows instant validation of the form data. This feature of JavaScript is convenient for the shoppers. But JavaScript may contain malicious codes as well, especially, the codes written by unknown parties.

Is it possible to reduce this kind of rogue applets? The answer is positive. First of all, programmers need to read the code of each applet before they apply it in the HTML code.

Programmers need to understand the whole codes of the applets and ensure that the code can be trusted. Otherwise, they should not use those applets rashly. Secondly, merchants can choose applets and ActiveX components, which are created by well-known companies. For instance, Microsoft offers many code samples on their web site, which administrators could use on the E-commerce web site. The shoppers need to read those information boxes, which prompt users to install the ActiveX control. Shoppers may disable the functions of Java, JavaScript, and ActiveX from their browsers' option. Figure 2.8.3 displays an example how to disable Java, and JavaScript in the Firefox browser.

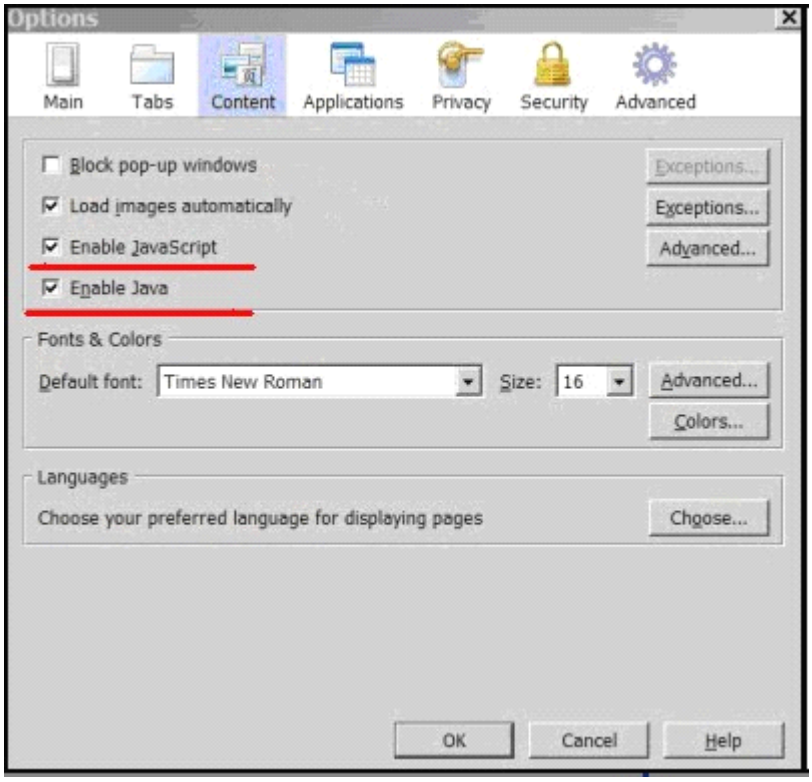

Figure 2.8.3 Firefox Options to enable/disable JavaScript and Java.

3. Defense

This section will demonstrate how to keep a secure E-commerce environment. The security work does not only belong to merchants but also to shoppers. The cooperation of merchants and shoppers should be seamless, so that attackers may not easily find the bugs to attack. According to the mentioned attack methods, this chapter will discuss how to protect an E-commerce network work properly. Figure 3 shows the basic defense methods.

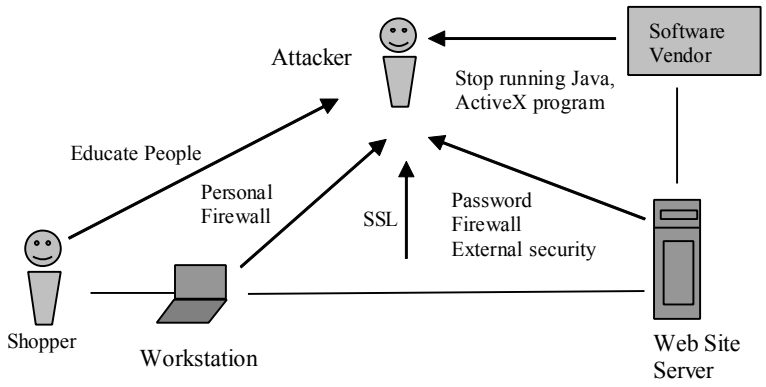

Figure 3 Defense topology and methods

3.1 Education

Educating shoppers is one of good way to decrease the tricking attack. However, this kind of education is not easy, since we could see there are still many customers tricked by very common social engineering attacks. That is why educating shoppers is not a short-term task. Merchants have to remind customers to set a secure password and change them regularly so that the information will not leak to attackers.

3.1.1 Keep password safety

Password is authentication used to verify the shoppers' identification, so it is significant to store personal password safely. Shoppers may have many different passwords for different web sites, so it is necessary to record which a password is used for which web site. However, it is not smart to write a password on a sticky note and stick on an obvious place ,

since the password might be seen by thieves as well. If passwords have been saved in the computer, it is necessary to encrypt that file, which contains the password, in case attackers may telnet into the shoppers' computers to steal important information. Furthermore, merchants need to remind shoppers about changing their password after a certain period.

3.1.2 Being aware of attacker tricks

Shoppers have to be always aware of those attackers who utilize social engineering techniques to trick shoppers and to gain the shoppers' personal information. Furthermore, media could explain the most common methods with which attackers spoof shoppers, and teach shoppers some basic methods to avoid being tricked. For example, it is important that shoppers do not tell any personal information through phone, Email or on-line program.

3.2 Setting a safe password

The most users select their password from their familiar things such as birth day, children's name, or pet's name. However, an attacker could pick up personal information such as children's name, spouse's name, birthday and even more. It is important that shoppers choose a strong password to login their account. What makes a strong password? Length is one of factor, and containing a variety of character is the other factor. When a shopper registers an account from a web site, it is a good idea to ask the shopper to have a password of a minimum length, and use a variety of characters. If shoppers cannot come up with a good password, merchants may guide shoppers using a safe password generator which we can find from many web sites, such as http://www.pctools.com/guides/password/. Shoppers may create 50 different passwords at once and choose one of them in case the generator web site may know the password.

3.3 Managing Cookies

When shoppers open an account in a web shop, they may use a cookie to store their passwords, Email addresses, account numbers and so on, so shoppers do not need to enter this information again when they login to the web site again. Basically, websites also use cookies to manage shopping carts and authenticate users [7]. The feature of cookies

provides convenient service to shoppers, but it also provides a chance for an attacker to steal information. Once shoppers apply cookies, the certain information shoppers enter into the web site will be recorded into the shoppers' hard disk. Once attackers access the shoppers' computer, they may scan the cookies' file and find the shoppers' personal information. How can the shoppers avoid this issue? The easiest way is to stop using cookies, and most users can reconfigure their browsers to turn off cookies.

3.4 Personal firewall

Installing a personal firewall is one way to protect the shoppers' work station. A personal firewall is an application which controls network traffic to and from a computer. While it is different from a conventional firewall, a personal firewall only works on the computer which has a firewall application installed. After a personal firewall has been installed, it will control the incoming and outgoing traffic according to the security policies. Furthermore, a personal firewall provides an intrusion detection system which is designed to detect unwanted attempts at accessing, manipulating, and/or disabling computer systems.

A personal firewall has some basic features which might help shoppers:

1. Shoppers can decide which programs can and cannot access the local network.
2. It can hide the shoppers' computers from port scans by not responding to unsolicited network traffic.
3. It can monitor if there are any applications sniffing the shoppers' data.
4. It can protect against Trojan accessing the shoppers' computers from the Internet.
5. It can provide information of a destination server which is communicating with the shoppers' work stations.
6. It can scan the shoppers' computers when the shoppers turn on computers to avoid malicious and other unwanted programs.

It is necessary to install a firewall for shoppers, and the shoppers have to update their firewall frequently. Because bugs may exist in the application firewall as well, installing new patches will decrease attacks.

3.5 Encryption and decryption Algorithm

Before explaining the secure transferring method, there are a couple of algorithms that need to be mentioned. They are the symmetric-key algorithm and the asymmetric-key algorithm. The symmetric-key algorithm only uses one key to encrypt and decrypt data. The symmetric-key algorithm computes hundreds to thousands times faster than the asymmetric-key algorithm. The asymmetric-key algorithm includes two keys which are the public key and the private key. The public key is used to encrypt data and a receiver decrypts the data with the private key.

3.6 Digital signatures

A digital signature is similar to a personal signature and it verifies two important things pieces of information in electronic communication. First, it checks whether the message comes from an original sender. Second, it verifies if the message has been changed after it was sent. How does a digital signature work in an E-commerce system? Firstly, a web site will use a one-way hashing algorithm to create a fixed length message digest from the data, which is going to be sent. After that, the message digest will be encrypted by the web site's private key in order to get digital signature. Figure 3.6.a shows the steps to create a digital signature.

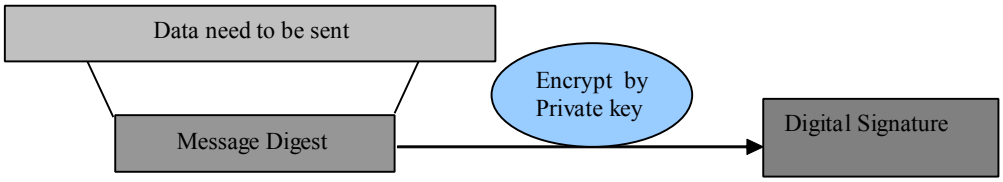

Figure 3.6.a Steps to create a digital signature

The created digital signature will be sent together with the data, which has to be sent to the shoppers. When the shoppers receive the digital signature and the data, they will decrypt the digital signature with a public key to obtain the first message digest, which we call digest1 here. At same time, the shoppers calculate the second message digest (called digest2) by using same method as the web site, so the second message digest is calculated from the received data. By comparing digest1 and digest2, the shoppers will know if this

message has been changed or not. If digest1 is the same as digest2, the shoppers will accept the digital signature as a legal one. The shoppers will discard the distorted message when the digest1 is different from digest2. Figure 3.6.b illustrates the whole process of digital signature verification.

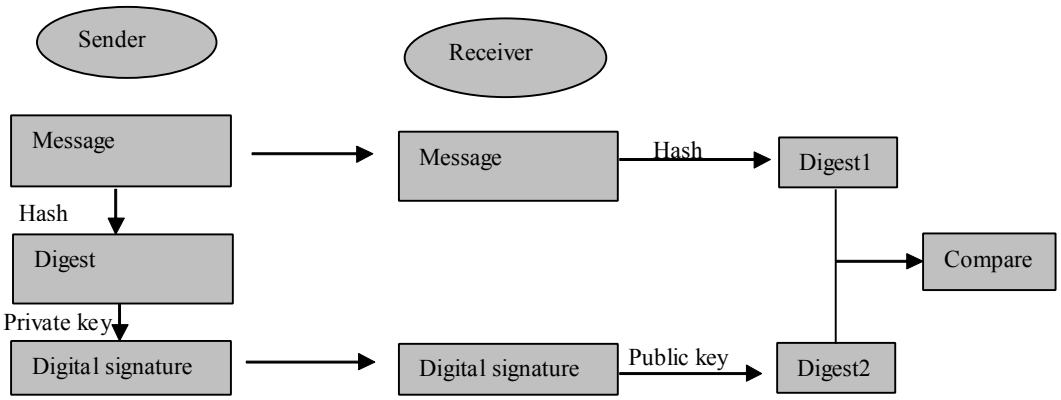

Figure 3.6.b Authentication of the message using a digital signature

3.7 Digital certificate

While a digital signature cannot solve the problem of attackers spoofing shoppers with a fake web site which we can call "man-in-the-middle" attack to gain shoppers' information, digital certification is one solution to this kind of attack. What is a digital certificate? A digital certificate is actually an electronic file that uniquely identifies communication entities on the Internet [8]. Merchants can apply this certification from the certificate authority which is the third party that shoppers can trust. Actually, a digital certificate is like an ID card issued by the police office, and most people trust the police stamp. A typical digital certificate includes the signature of a CA (certificate authority) as well so that people could use the CA's public key to decrypt the signature and verify if they trust this digital signature and this digital certificate. Furthermore, a digital certificate is not permanent, so it is necessary to see if this certificate is still valid. If the certificate is valid, the customers' browsers will check whether this issuer is in the trusted list of CA. For example, users may see those trusted authorities list on the Mozilla browser. Figure 3.7 shows what the list looks like.

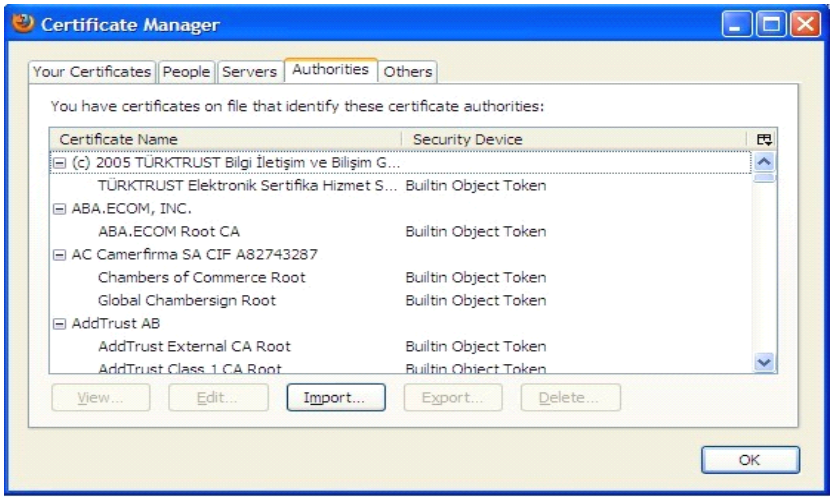

Figure 3.7 The list of authorities of the Mozilla Firefox browser

The checking work normally has been carried out automatically by the users' browsers, so that the users do not need to check it by themselves.

3.8 Secure Socket Layer and Transport Layer Security

Transport Layer Security (TLS) and its predecessor SSL are security protocols that encrypt data transferring between the shoppers' workstation and the sites' servers and prevent third party listening and tampering.

Secure Sockets Layer is a protocol designed to work, as the name implies, at the socket layer, to protect any higher-level protocol built on sockets, such as telnet, ftp, or HTTP [9]. A good example of applying SSL is HTTPS. Https:// indicates that users are connecting to a secure web server. For instance, when Finnish customers go to the Nordea bank site to login to their bank account, they will see a secure web site connection address: https://solo1.nordea.fi/nsp/engine?language=en&country=FI .

How does SSL/TLS work? The SSL/TLS client and server communicate by a handshaking procedure. Figure 3.8 illustrates the steps through which SSL/TLS achieves a secure conversation.

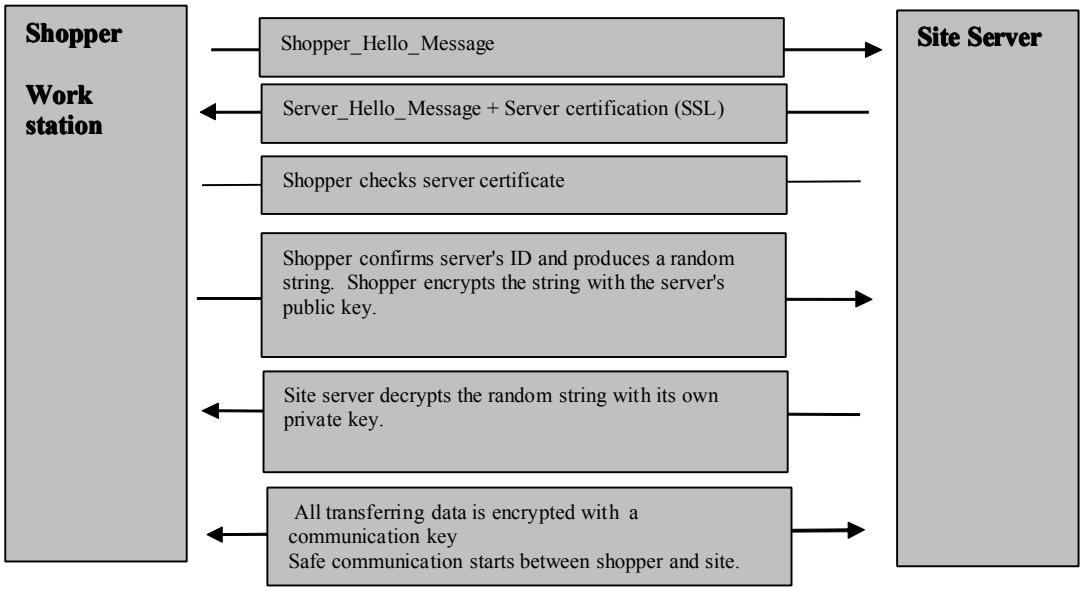

Figure 3.8 SSL conversation steps

Firstly, a shopper sends a "Hello" message to start conversation, and this message includes the list of cryptology algorithms which shoppers are supported. The site receives the message and replies with a server_hello message. The server_hello message contains the suitable algorithm chosen from the list and its site's digital certificate. In the same way as we mentioned in the digital certificate section, the shopper verifies the digital signature to make sure if this certificate can be trusted. After the site of identification has been confirmed, the shopper site will generate a random string and encrypt it with the public key received from the site. The encrypted random string is sent to the site and it will be decrypted by the site's private key. In this way, no one can sniff and tamper this random string. The algorithm of the symmetric-key will be used after both sides have the same random string. The random string will be taken as the key to encrypt and decrypt the later message, which will be transferred between the shoppers and the web site. In brief, SSL and TLS apply both a symmetric-key algorithm and an asymmetric-key algorithm to ensure the security of the transmission.

3.9 Server firewall

A server firewall is a part of the network that is designed to block unauthorized access and intruder attacks. A common technique is to set up a demilitarized zone (DMZ) for an E-commerce network. The other common technique used in conjunction with a DMZ is a honey pot server. This section discusses how these two techniques are used into the E-commerce network.

3.9.1 Demilitarized zone (DMZ)

A DMZ is a network construct that provides secure segregation of networks that host services for users, visitors, or partners [10]. That means visitors only access the E-commerce network of DMZ, rather than the whole network. There are two most common approaches to design a DMZ network. One is a single firewall, the other one uses two firewalls to construct a DMZ. Figure 3.6.1.a and Figure 3.6.1.b display the topology of DMZ with a single firewall and double firewalls.

A single firewall has three interface connections to divide the network into: the external part, the DMZ part and the internal part. As mentioned, DMZ contains the server, such as the web server, which visitors located in the external parts can easily visit. The internal network involves the most confidential data which might be stored in the payment server and the authentication server. Basically, a single firewall needs to transfer a large amount of data and it examines if the data is going to transfer from internal network to the DMZ network, or from the DMZ network to an external network.

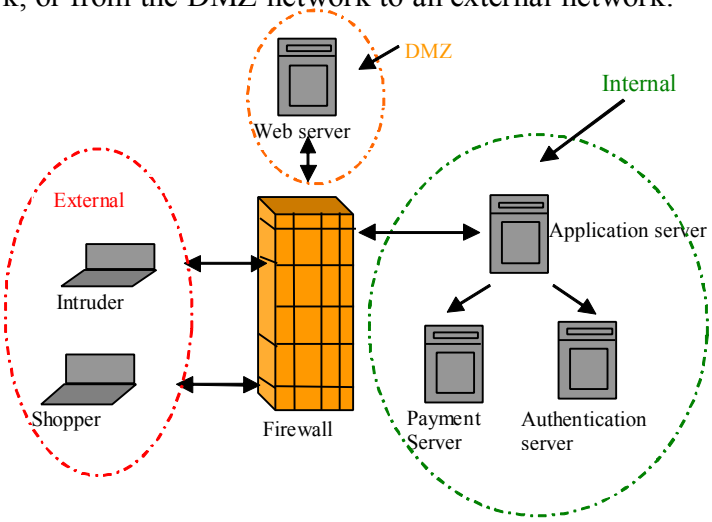

Figure 3.9.1.a Single firewall Separate DMZ

Compared with the single firewall, the model of double firewalls is more secure to protect confidential data. It offers two firewalls to separate DMZ and the internal networks. Figure 3.6.1 b shows what the topology looks like. The left firewall is called the "front-end" firewall which has been configured to allow incoming and outgoing traffic from the external network to the DMZ network.

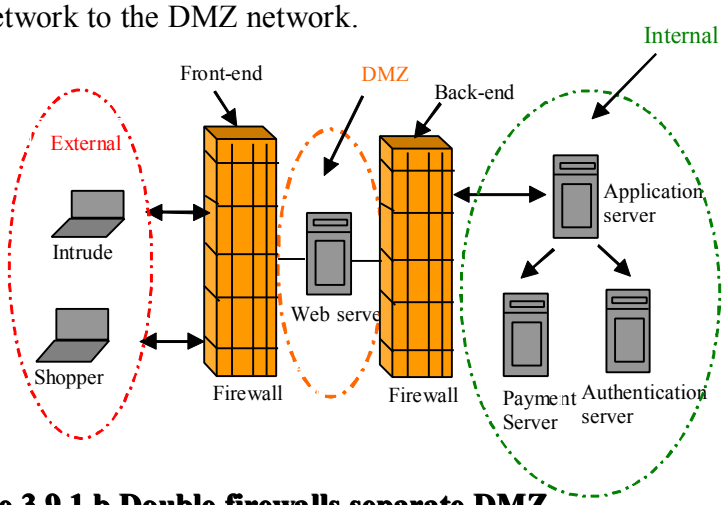

Figure 3.9.1.b Double firewalls separate DMZ

The other firewall called "back-end" firewall allows only certain trusted servers access, in order to keep the internal network security. Purchasing firewalls from two different vendors is recommended. Because different companies design firewalls differently, the bugs of firewalls may not be same. If the first firewall breaks down, attackers may need longer time to find the second firewall's bugs.

3.9.2 Honey pot

A honey pot is basically an unprotected system with no applied patches, operating system updates, or firmware updates that are used to attract, trap, and identify possible attackers [11]. It is divided into two categories which are virtual honey pots and real honey pots. The concept of a honey pot came about a couple of years ago, when network administrators needed to find out if anyone is sniffing their network.

Actually, a virtual honey pot is an emulator. It is very often that a virtual honey pot emulates as a FTP server, since the FTP server supports clear text transmission mode,

which may attract intruders to attack it. If anyone is sniffing or attacking a server's port, the emulator will record which port has been sniffed and attacked.

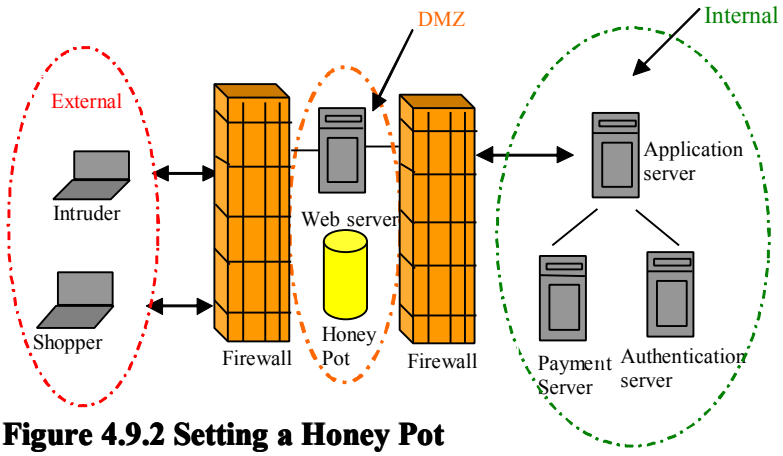

Figure 4.9.2 Setting a Honey Pot

Compared with a real FTP server, the virtual FTP does not contain any important information or even an operation system, so that attackers can not attack the rest of the network or even not steal any important information from the emulator. This is an advantage of the virtual honey pot, but it is a disadvantage as well, since professional attackers may easily realize they fall into a honey port. Because a virtual honey port is made by an emulator it may not execute any program after the attackers have tried different operation system commands. Moreover, the virtual honey pot only records limited attacking information, since it does not have the ability to discern newly devised attacks.

A real honey pot does not have this problem, because it is built on one or more than one real server(s). When attackers access a real honey pot, they may not easily verify that they fall in a trap. However, this does not mean the attackers will not perceive it. The attackers might suspect the weak protection for this server. However, once the attackers realize they are in the real honey pot, they might attack the rest of network through this real honey pot. The best solution is to combine the honey port with DMZ double firewalls solution, which is displayed by Figure 3.6.2.a. Although the attackers realize that they fall into a honey pot and try to attack other networks through the real honey pot, the second firewall will protect the internal work. The disadvantage of a real honey pot is that it is expensive to use for small enterprise, so merchants can choose the most suitable solution for their network.

3.10 Preventing DoS attacks

As previously mentioned, DoS attacks can be easily launched by anyone, from anywhere, at anytime, so is there any effective solution to prevent DoS attacks? Unfortunately, the answer is no, since each E-commerce network device has a different configuration and DoS attacks can be launched by unknown hosts or network. However, it does not mean administrators should only wait for DoS attacks. This section will discuss the basic methods to decrease DoS attacks in an E-commerce network.

One of most important action administrators need to take is controlling the inbound and outbound traffic of an E-commerce network. Normally, administrators may only concentrate on the inbound traffic. However, controlling the outbound traffic is significant, too. In DoS attacks, attackers use a distorted source address to hide themselves and lead slaves to do the dirty work. These spoof source IP addresses might be distributed to the devices of E-commerce network. Without controlling the outbound traffic, the internal devices of E-commerce network may become the attackers' slaves to attack others. In this case, network administrators could configure the firewall to deny those invalid source IP addresses, private and reserved source IP addresses from the internal network. A well-designed Access Control List (ACL) will control the traffic of egress and ingress. However, it is necessary to keep in mind that the capacity of ACL lists is limited. The more ACL lists implemented, the more time firewalls will take to filter traffic. Furthermore, administrators should disable IP direct broadcast on all systems so that we may decrease the Smurf attack. For example, the command of **no ip direct-broadcast** will disable the IP broadcast function of Cisco routers. Chargen and echo services are used in DoS attacks, too. These services are intended to test the network, so administrators can disable these kinds of services, which are not often used in an E-commerce network.

Monitoring the network may help administrators to react quickly when DoS attacks are launched. There are a few tools that can help and these are: The first one is Nmap, which is a security scanning tool that may help administrators to scan the entire network systems' UDP and TCP ports, so administrators may analyse if handlers or agents exist in the network. Find_ddos is another tool, which is used on a host to determine if DDoS attack

software is installed on the host. Zombie zapper is one of type of software to stop DDoS attacks. Basically, this software stops those flooding messages from zombie systems. Besides those basic free software tools, an Intrusion Detection System (IDS) should be introduced, as well. An intrusion detection system is a device, which is used to monitor network and system activities. If merchants have enough financial resources for network security control, then they can set suitable IDS on their E-commerce network and hosts. Well-designed IDS can display the conversations between client, master and agent. This information provides the evidence of DDoS attack to network administrators.

3.11 Updating patches

As we mentioned in the beginning of this section, patches may display the bugs existing in the system or software to the attackers. Updating patches can perfect the system and software, so that both the E-commerce network administrators and the shoppers should constantly install the latest version of patches for keeping a secure E-shopping environment.

3.12 Monitoring and analyzing security logs

Finding the weak points of an E-commerce system is also one of the defense strategies. Monitoring and analyzing security logs may achieve this defense goal. For instance, if there is anyone falling into a honey pot, the honey pot will record a security log to network administrators. It would be good that network administrators read those logs frequently and understand which points are the targets of the intruders, so that the administrators can update the system according to the bugs displayed on the log. Monitoring the entire E-commerce network will help administrators to react quickly when attacks start. For instance, administrators may monitor the network through Intrusion Detection System (IDS).

4. Site development

Web administrators have to keep in mind that developing a site constantly offers a stable web site to customers. This chapter discusses how to maintain and develop a secure and stable site.

4.1 Implementing security policies

The primary and most basic security tool of any organization is security policy. The security policy is the backbone of the entire operation because it defines the rules by which business is conducted [12].

4.1.1 Take Password policies as an example

What kind of policies should apply to E-commerce? Let us take password policies as an example to see how security policies maintain the security of E-commerce. Password policies ensure that passwords are sufficiently strong so that passwords cannot be easily guessed. The account lockout capability ensures that an automated scheme cannot make more than a few guesses before the account is locked. The normal password policies are displayed in the following text:

- Shoppers have three chances to enter a suitable password. The account will be locked after shoppers or attackers have input the wrong password three times.

- When shoppers set a password for their account, the password has to contain letters and numbers. The length of password should be more than 6 characters.

- Users are advised not to store their password only in plain text directly into database. Passwords should encrypted by one-way hash algorithm before saving into database.

4.1.2 Examples of other policies

A comprehensive security policy is actually made up of several individual policies, each of which target unique lateral aspects of the site's business processes. The individual policies work together to provide three basic assurances for the site: confidentiality, integrity, and availability of data [13]. Here follow some other individual policy examples that administrators may apply to the E-commerce system in order to manage and protect the system's security.

- The sensitive and confidential data needs to be encrypted during the transfer.

- Security experts can be employed to attack and analyze the E-commerce system regularly, so that the site administrators can update the system according to the found bugs.

- External security experts need to have verified appropriate processes and techniques of third party applications before installing them on the system.

Different policies should be created depending on the type of the E-commerce network. It is of utmost importance to apply the policy. Administrators do not only need to understand all the policies, but also to apply the policy in the real work. Furthermore, other departments of employees have to understand particular security policies according to their need.

4.2 Choosing suitable components and internet connection

It often happens that shoppers see a slow, unreachable, or not fully functional web site. What might cause that? One of the possibilities is that the network components do not handle sufficient volumes of network traffic. This section will discuss how merchants can use suitable components to work together and provide a stable working web site for shoppers.

4.2.1 Determining the overloaded device

An E-commerce infrastructure contains different components, which may include web servers, database server, financial transaction servers, DNS servers, and network equipments. If one of these devices works over their capacity, the whole web site may not work properly. Sometimes, the overload device will work as efficiently as the device being down, but sometimes the overload device will work very slowly. Depending on the status of the overloaded device, the web site will work slowly, or even not at all. The overloaded device is harder to troubleshoot than the device being down. For example, the most basic way administrators might use is a ping test to verify which device is not working. However, the ping test may not work for checking the overloaded device, since the overloaded device may still display "up" state from the ping test. To find an overloaded device, administrators need to understand each device's capacity and analyze which one is the current bottleneck in the whole network. As we know overloading is always associated with network throughput, CPU utilization, and what is in the RAM.

Firstly, how can we determine the load of a router? Take Cisco routers for instance, we could use **show interface** to see the description of a particular interface. For instance, the command will show the particular interface, which is running 100Mbps, full-duplex Fast Ethernet. In addition, an administrator could use the command **show process** to see the CPU utilization of the router. With description information, the administrator could decide if this router is suitable to work with other network components. Moreover, the web server is the most important component of the E-commerce network, so the administrator needs to consider if the web server has sufficient capacity to work with other devices. By checking the operating system of the web server, administrators may easily see a rough measurement of the overall load of a system. We are only taking two of the most popular server operating systems as examples. In a UNIX operating system, we may use the commands **uptime** and **top** to check load. Performance monitor provides a rough idea about what the load is and the task manager displays the CPU utilization to Windows users.

4.2.2 Managing Bandwidth

Bandwidth is one factor which may bottleneck an E-commerce network. When merchants buy an Internet connection from an ISP (Internet Service provider), they have to consider how much bandwidth the site normally needs. It is always good to find enough site bandwidth for customers, and the merchants do not need to pay much. There are two forms of bandwidth service merchants could choose. One is having the bandwidth delivered to the merchants' location, which means merchants will have their own connection line, which connects from merchants' site to the ISP directly. This form of service will be much more secure and convenient to the merchants. However, good service always costs more. For example, a common T1 Internet access is around $2,000 per month. How about the other option of service form? It is co-location which tends to be cheaper, but it is less convenient and secure. Since co-location allows many companies to share the cost of establishing bandwidth, the merchant pays much less than using his/her own line. How should merchants find a suitable connection for their E-commerce network? There many different software packages could monitor the usage of bandwidth, so analyzing the data may help merchants to make a decision. MRTG (Multi Router Traffic Grapher) is one free software which monitors and measures the traffic load on network links.

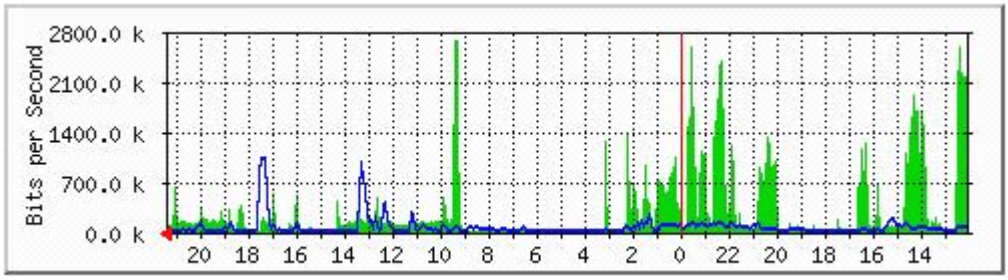

Figure 4.2.2 [14] A sample MRTG bandwidth graph

4.3 Disaster recovery plan

If a site administrator configures a secure firewall, updates the latest patch for OS, uses secure software, and manages the whole network according to security policies, what should the administrator do if one of the servers is still down? How can the administrator

find lost data from an unfixable server? A good disaster recovery plan may help the merchant to decrease that risk.

Basically, disaster can be classified in two broad categories which are: human-made disaster and nature disaster. Human-made disaster includes accidents, burglary, virus, intrusion, etc. Nature disaster is difficult to prevent, but with a disaster recovery plan, it is possible to decrease loss of data.

4.3.1 Backup rotation process

Since we never know when the server will be going down, and how much important data might be lost from a human made disaster, backup becomes a significant precaution, depending on the backup medium and how important the backup data are. Merchants could choose different methods to backup data.

A full backup is very easy to understand, as the name implies, all the data will be copied to the backup medium after a certain period. Administrators copy all the data every day to the backup medium, so if a server is going down, the administrators will use the previous day's backup to recover the system. For example, administrators backup all the data from the system to the backup medium on Monday. The next day, Tuesday, the administrators backup all the data which includes the data comes from Monday and Tuesday. In this way, there is maximum one day data lost by accident, and the whole recovery process will take place in a very short time. Of course, administrators may backup all the data in a period even shorter or longer than one day, depending on the backup plan. However, this method requires a lot of storage space media and time, since there are much data which may be repeatedly copied.

The incremental backup method solves the full backup disadvantage as it only records new data from the system to the backup medium. It saves much backup medium and time for site administrators, but it has some problems as well. For example, administrators use the incremental backup method to backup all the data on Monday as basic backup and the next day they only backup the new data which comes on Tuesday. The next day, the site

administrator only records new data comes on Wednesday but does not record the new data which comes on Tuesday. In this way, it requires a very short time to copy the data from the system to the medium, and saves much backup space When a server is down on Thursday, the administrators have to take backup data from Monday's record to Wednesday's record. If one of these days' backup is missing, this means that the recovery process will fail. Furthermore, this recovery process has to take a very long time to complete.

The differential backup is another method which combines those two methods. It contains two parts of data backup which are basic backup, and differential backup. For example, administrators copy all the data from the system on Monday, and they take these data as basic backup. On Tuesday, the administrators only copy the data which are different as basic backup. The same work will be done on Wednesday, so actually Wednesday backup contains the Tuesday backup and the new data coming from Wednesday but does not include the basic backup from Monday. If the server is going down on Thursday, administrators will need only two backup records which are the basic backup from Monday and the differential backup from Wednesday. In this way, merchants do not need to worry about the cost of the backup medium, and administrators could complete the recovery in a short time.

4.3.2 Off-site data protection

Off-site data is the strategy of sending critical data out of the main location, in order to decrease the risk of losing important data from nature disaster, human accident or system crash. Normally, administrators have two options to send backup data away from its original location. One is sending those removable backup media to another physical place than the administrators' office. The other way is uploading data to an online backup system. Carbonite [14] is one of the companies offering this kind of online backup service to customers. More information can be found at http://www.carbonite.com/.

4.3.3 Building a redundant line to the ISP

As previously mentioned, the data needs to be backed up so that the loss from disaster is decreased. What else should be backed up in an E-commerce network? If the connection between the web server and the ISP is going down, then customers can not visit the web shop. This is a bad situation for merchants, since troubleshooting may take very long time. In the meantime, merchants will lose many potential customers. Building a redundant line with another ISP is good precaution for this case. When the original ISP connection is down, the redundant connection will take over immediately and replace the original one. If merchants cannot afford two network service providers, they could install two physical lines going to the same ISP.

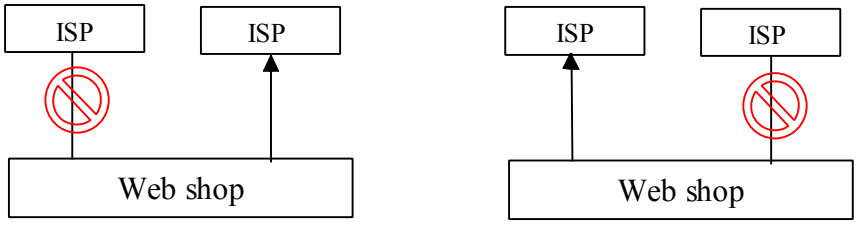

Figure 4.3.3 Redundant line

5. Conclusion

E-commerce security issues are related to different technical fields, so maintaining a secure environment is not only work belonging to technical administrators but also to merchants, service providers, shoppers, and everyone who participates in E-commerce. We have a lot of mature technologies to protect the security of E-commerce such as firewall, SSL, monitoring site program, and many more. But we still need to be aware of attackers since they may appear anytime and anywhere in our E-commerce system. The implementation of a well-conceived recovery plan is necessary, so that we will be able to quickly restore the system after an attack. When we have the knowledge of E-commerce security and all the security policies and plans have been designed, the implementation has to been done according to what technologies and plans we have. Otherwise, theory and plan will be only staying on the paper, and E-commerce will become a trouble maker rather than a good business platform.

References

[1]Russell, Ryan (Contributor); Huston, L. Brent (Editor). 2000. Hack Proofing Your E-Commerce Site: The Only Way to Stop a Hacker Is to Think Like One. Rockland, MA, USA: Syngress Publishing, p 29.

[2] Wang, Wallace. 2003. Steal This Computer Book 3: What They Won't Tell You About the Internet. San Francisco, CA, USA: No Starch Press, Incorporated, p176.

[3] Conway, Richard Cordingley, Julian. 2004. Code Hacking: A Developer's Guide to Network Security. Herndon, VA, USA: Charles River Media, p204.

[4] Russell, Ryan (Contributor); Huston, L. Brent (Editor). 2000. Hack Proofing Your E-Commerce Site: The Only Way to Stop a Hacker Is to Think Like One.Rockland, MA, USA: Syngress Publishing, p 211.

[5] Russell, Ryan (Contributor); Huston, L. Brent (Editor). 2000. Hack Proofing Your E-Commerce Site: The Only Way to Stop a Hacker Is to Think Like One. Rockland, MA, USA: Syngress Publishing, p 211.

[6] Cross, Michael. 2006. Developer's Guide to Web Application Security.

Rockland, MA, USA: Syngress Publishing, p 118.

[7] Schrenk, Michael. 2007. Webbots, Spiders, and Screen Scrapers. San Francisco, CA, USA: No Starch Press, Incorporated, p 47.

[8] Milutinovic, Veljko. (Editor); Patricelli, F. (Editor). 2002. E-Business and E-Challenges. Amsterdam, NLD: IOS Press, p 92.

[9] Milutinovic, Veljko. (Editor); Patricelli, F. (Editor). 2002. E-Business and E-Challenges. Amsterdam, NLD: IOS Press, p 108.

[10] Flynn, Hal. 2006. Designing and Building Enterprise DMZs. Rockland, MA, USA: Syngress Publishing, p 2.

[11] Crayton, Christopher. 2003. Security+ Exam Guide. Herndon, VA, USA: Charles River Media, p 121.

[12] Russell, Ryan (Contributor); Huston, L. Brent (Editor). 2000. Hack Proofing Your E-Commerce Site: The Only Way to Stop a Hacker Is to Think Like One. Rockland, MA, USA: Syngress Publishing, p 220.

[13] Russell, Ryan (Contributor); Huston, L. Brent (Editor). 2000. Hack Proofing Your E-Commerce Site: The Only Way to Stop a Hacker Is to Think Like One.

Rockland, MA, USA: Syngress Publishing, p 255.

[13] [www-document] Available at http://upload.wikimedia.org/wikipedia/commons/5/57/MRTG_Graph_from_My_Router_localhost_eth0-day.png (referred: 03.03.2010)

[14] [www-document]. Available at:

http://www.carbonite.com/ (referred: 03.03.2010)

[15][www-document]. Available at: http://www.ibm.com/developerworks/websphere/library/techarticles/0504_mckegney/0504_mckegney.html (referred: 03.03.2010)