IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-4, Special Issue-6, Aug 2016 E-ISSN: 2347-2693

A Comparative Study of Security in E-commerce: Review

Sumanta Chatterjee[1*] and Krishnayan Gupta[2]

[1]*Computer Science and Engineering Department, JIS College of Engineering, India*
[2] *Computer Science and Engineering Department, JIS College of Engineering, India +*

Available online at: www.ijcseonline.org

Received: Jun/26/2016 Revised: July/12/2016 Accepted: July/26/2016 Published: Aug/12/2016

***Abstract*—** The goal of e-commerce system is to provide secure connections between customers and the company with other parties acquiring personal information. But in the various stages of e-commerce an individual or company is a victim of unwanted attacks or threats. Here, the investigation is done on the security concerns among different e-commerce websites. Matters such as privacy, security and threats, impersonation, forged identity etc. is also looked upon. The different threats are brought forward with maximum efforts done onto how it can be reduced.

***Keywords*—** client threats,channel threats, server threats, SSL/TLS, SET, 3d Secure

I. INTRODUCTION

E-commerce connects buyers and sellers over the Internet as they conduct business interactions. Though it can be incredibly convenient and productive when you are successful, it is also accompanied by risks.

Attackers can steal information during the course in the e-commerce transactions. The importance of secure networks cannot be overstated and it is important to think critically when designing e-commerce system.

The three major components by which to view a security system:

1. Attackers
2. Mechanism
3. Security Features

II. THE ATTACKERS

They have an incentive to acquire money by stealing the personal information of customer. If an attacker can obtain a buyer's credit card information during an online transaction he can then use it to make his own purchases later

III. THE MECHANISM

There are two Protocols that have been used to provide security in online transactions:

[1] The Secure Sockets Layer or SSL.
[2] The transport layer security or TLS.

A. TLS is the successor of SSL

These protocols are used by virtually all companies today to establish secure connections with their customers.

SSL and TLS consist of many different components:

[1] Public key cryptography
[2] Hash functions
[3] Data encryption
[4] Message authentication

These components are all used in the **handshake phase** which is a series of messages between the customer and the company. The end result at the handshake phase is a secure connection based on a shared secret key between the customer and the company.

From here the two parties proceed to the data transfer phase were sensitive details such as credit card information can be transmitted with confidence.

It can be found that the browser establishes an SSL TLS connection with the web page by looking for HTTPS in the URL instead of just HTTP. This "s" stands for Secure and with most browsers a symbol usually appears to the left of the URL to indicate that the connection is secure.

In Google Chrome a green-lock is displayed, in Safari a grey box with the word HTTPS is displayed along with the lock. Information about the connection description can be obtained by clicking on these icons.

Handshake Phase is an automated process of negotiation that dynamically sets parameters of a communications channel established between two entities before normal communication over the channel begins. It follows the physical establishment of the channel and precedes normal information transfer.

The handshaking process usually takes place in order to establish rules for communication when a computer sets about communicating with a foreign device. When a computer communicates with another device like a modem, printer, or network server, it needs to handshake with it to establish a connection.

B. E-commerce Threats:

1. **Client Threats:**
   - Malicious code: Virus, Worms, Trojan horse.

- Active Content: Java applet, ActiveX Controls, JavaScript, VB Script
- Unauthorized Access
- Server authentication threat (Fabrication)
- Phishing
- Theft & Fraud

2. **Communication channel Threats:**
- Confidentiality threat (Interception)
- Integrity threat (Modification)
- Availability threat (Interruption)
- Packet Sniffing

3. **Server Threats:**
- DoS (Denial Of Service)
- DDoS (Distributed Denial of Service)
- Client authentication threat (Fabrication)
- Database threat
- Common Gateway Interface (CGI) threats

Computer Virus & Computer Worm:
A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infection.
A worm is similar to a virus by design and is considered to be a sub-class of virus. Worms spread from computer to computer but unlike virus, it has capability to travel without any human action.
Unauthorized access:
Trojans are malicious programs that perform actions that have not been authorized by the user. These actions can include:

1. Deleting data
2. Blocking data
3. Modifying data
4. Copying data
5. Disrupting the performance of computers or computer networks

Impacts of Trojans:
i. **Backdoor** - A backdoor Trojan gives malicious users remote control over the infected computer.
ii. They enable the author to do anything they wish on the infected computer – including sending, receiving, launching, and deleting files, displaying data, and rebooting the computer.
iii. Backdoor Trojans are often used to unite a group of victim computers to form a botnet or zombie network that can be used for criminal purposes.

Protection from Trojan & Backdoor:
1. Stay away from suspect websites/web links: Avoid downloading free/pirated software's' that often get infected by Trojans, worms, virus and other things.
2. Surf on the cautiously: Avoid connecting with and/or downloading any information from peer-to-peer (P2P) networks, which are most dangerous networks to spread Trojan Horses and other threats. P2P networks create files packed with malicious software, and then rename them to files with the criteria of common search that are used while surfing the information on the web. It may be experienced that after downloading file it never works and hence there is a threat that although the file has not worked something may have happened to the system. The malicious software deploys its gizmos and the system is at serious health risk. Enabling spam filter "ON" is a good practice but is not 100% foolproof, as spammers constantly develop new ways to get through such filters.
3. Install antivirus/Trojan remover software: Now day's antivirus software(s) have built-in feature for protecting the system not only from virus and worms but also from malware such as Trojan Horses. Free Trojan remover programs are also available on the Web and some of them are really good.

C. Phising:

Phishing is a type of deception designed to steal your identity (i.e. a kind of ID Theft). In Phishing schemes the phisher tries to get the user to disclose valuable personal data such as credit card numbers, passwords, account data and other information by convincing the user to provide it under false pretenses. E-mail is the popular medium used in the Phishing attacks and such E-Mails are also called Spams.
How to avoid being victim of phishing attack:
1. ***Keep antivirus up to date:*** Important aspect is to keep antivirus software up to date because most antivirus vendors have signatures that protect against some common technology exploits. This can prevent things such as a Trojan disguising the web address bar or mimicking the secure link (i.e., HTTPS)
2. ***Do not click on hyperlinks in Emails:*** It should always be practiced that in case an E-Mail has been received from unknown source clicking on any hyperlinks displayed in an Email should be avoided. This may lead to either the link taking the victim to the website created by the phisher or triggering a Malicious Code installation on the system. Instead, to check the link, manually retyping it into a web browser is highly recommended
3. ***Take advantage of anti-Spam software:*** Ant-spam software can help keep phishing attacks at a minimum. A lot of attacks come in the form of spam and by using anti-spam software many types of phishing attacks are reduced as the message never end up in the user's mailbox.
4. ***Verify https (SSL):*** Ensure the address bar displays "https://" rather than just "http://" along secure lock icon than has been displayed at the bottom right-hand corner of the web browser while passing any sensitive information such as credit cards or bank information. One may like to

check by double clicking the lock to guarantee the third party SSL certificate that provides the https. Always ensure that the webpage is truly encrypted.

5. ***Use anti-Spyware software:*** Keep Spyware down to a minimum by installing an active Spyware solution such as Microsoft anti-Spyware and also scanning with a passive solution such as Spybot. If for some reason the browser is hijacked, anti-Spyware software can often detect the problem and provide a fix..

6. ***Firewall:*** Firewall can prevent Malicious Code from entering into the system and hijacking the browser. Hence, a desktop (software) such as Microsoft's built-in software firewall and or network (hardware) firewall should be used. It should be up to date in case any cyber security patches have been released by the vendor

7 ***Use backup system images:*** Always keep a backup copy or image of all systems to enable to revert to a original system state in case of any foul play.

8. ***Do not enter sensitive or financial information into Popup windows*****:** A common Phishing technique is to launch a bogus popup window when someone clicks on a link in a Phishing Email message. This window may even be positioned directly over a legitimate window a netizen trusts, Even if the popup window looks official or claims to be secure, entering - sensitive information should be avoided because there is no way to the security certificate.

9. ***Secure the host's file***: The attacker can compromise the hosts file on desktop system and send a netizen to a fraudulent site. Configuring the host file to read only may alleviate the problem. But complete protection will depend on having a good desktop firewall such as Zone Alarm that protects against tampering attackers and keeps browsing safe.

10. ***Protect against DNS Pharming attacks:*** This is a new phishing attack that does not Spam you with E-Mails but poisons your local DNS server and redirect your web requests to a different website that looks similar to a company website (e.. eBay or PayPal).

D. DOS & DDOS.

A denial-of-service attack (DoS attack) or distributed denial-of-service (DDoS attack) is an attempt to make a computer resource (i.e. information systems) unavailable to its intended users.

DoS Attack:

In this type of criminal act, the attacker floods the bandwidth of the victims or fills his E-Mail box with Spam mail depriving him of the services he is entitled to access or provide Although the means to carry out, motives for and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent the Internet site or service from functioning efficiently or at all, temporarily or indefinitely. The attackers typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, mobile phone networks and even root name servers (i.., domain name servers). Buffer overflow technique is employed to commit such kind of criminal attack known as Spoofing. The term IP address Spoofing refers to the creation of IP packets with a forged (spoofed) source IP address with the purpose of concealing the ID of the sender or impersonating another computing system. A packet is a formatted unit of data carried by a packet mode computer network. The attacker spoofs the IP address and floods the network of the victim with repeated requests. As the IP address is fake, the victim machine keeps waiting for response from the attacker's machine for each request. This consumes the bandwidth of the network which then fails to serve the legitimate requests and ultimately breaks down.

The United States Computer Emergency Response Team defines symptoms of DoS attacks to include:

1. Unusually slow network performance (opening files or accessing websites);
2. Unavailability of a particular website;
3. Inability to access any website;
4. Dramatic increase in the number of Spam E-Mails received (this type of DoS attack is termed as an E-Mail bomb).

The goal of DoS is not to gain unauthorized access to systems or data, but to prevent intended users (i.e. legitimate users) of a service from using it. A DoS attack may do the following:

1. Flood a network with traffic, thereby preventing legitimate network traffic.
2. Disrupt connections between two systems, thereby preventing access to a service.
3. Prevent a particular individual from accessing a service.
4. Disrupt service to a specific system or person.

DDoS Attack:

An attacker could take control of your computer by taking advantage of the security vulnerabilities or weaknesses. He/she could force your computer to send huge amounts of data to a website or send Spam to particular E-mail address. The attack is distributed" because the attacker is using multiple computers DoS attack.

A DDoS attack is a distributed DoS wherein a large number of zombie systems are synchronized to attack a particular system. The zombie systems are called secondary victims and the main target is called primary victim.

How to Protect from DoS/DDoS Attacks:

Computer Emergency Response Team Coordination Center (CERTCC) offers many preventive measures from being a victim of DoS attack.

1. Implement router filters. This will lessen your exposure to certain DoS attacks.
2. If such filters are available for your system, install patches to guard against TCP SYN flooding.

3. Disable any unused or inessential network service. This can limit the ability of an attacker to take advantage of these services to execute a DoS attack.
4. Enable quota systems on your OS if they are available.

Tools for detecting DoS/DDoS attacks:

1. ***Zombie Zapper:*** It is a free open source tool that can tell a zombie system flooding packets to stop flooding.
2 ***Remote Intrusion Detector (RID)*** It is a tool developed in "C" computer language which is a highly configurable packet snooper and generator. It works by sending out packets defined in the config.txt file, then listening for appropriate replies.
3. ***Security Auditor's Research Assistant (SARA):*** It gathers information about remote hosts and networks by examining network services. This includes information about the network information services as well as potential security flaws such as incorrectly set up or configured network services, well known bugs in the system or network utilities system software vulnerabilities listed in the Common Vulnerabilities and Exposures (CVE) database and weak policy decisions.
4. ***Find DDoS***: It is a tool that scans a local system that likely contains a DDoS program. It can detect several known DoS attack tools.
5. ***DDoS Ping***: It is a remote network scanner for the most common DDoS programs.

IV. SECURITY FEATURES

❖ Digital certificate

In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document that uses a digital signature to bind a public key with an identity – information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.

- Issued by trusted third parties known as Certificate Authorities (CAs)
- Used to authenticate an individual or an organization
- Digital Certificates are usually given for a period of one year
- They can be revoked
- It is given at various security levels.
- Digital Certificates can be issued by anyone as long as there are people willing to believe them.
- Digital Certificates are part of the authentication mechanism. The other part is Digital Signature.
- For ex-digital certificates in mobile applications

Contents of a typical digital certificate:

i. **Serial Number**: Used to uniquely identify the certificate.
ii. **Subject:** The person or entity identified.
iii. **Signature Algorithm:** The algorithm used to create the signature.
iv. **Signature:** The actual signature to verify that it came from the issuer.
v. **Issuer**: The entity that verified the information and issued the certificate.
vi. **Valid-From:** The date the certificate is first valid from.
vii. **Valid-To:** The expiration date.
viii. **Key-Usage**: Purpose of the public key (e.g. signature, certificate signing).
ix. **Public Key**: The public key.
x. **Thumbprint Algorithm**: The algorithm used to hash the public key certificate.
xi. **Thumbprint**: The hash itself, used as an abbreviated form of the public key certificate.

A. Non-Repudiation:

There are situations where a user sends a message and later refuses that he/she had sent the message. Non-repudiation does not allow the sender of a message to refute the claim of not sending the message.

Non-repudiation can be provided by digital signature using a trusted third party.

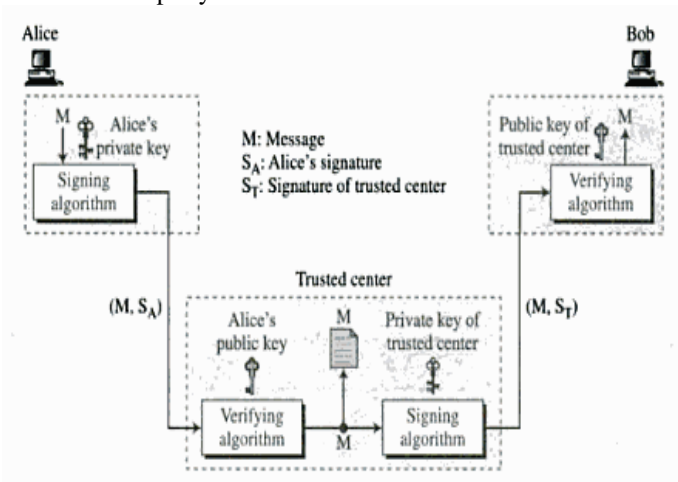


Fig 1. *Using a trusted center for nonrepudiation*

B. Difference between Digital Certificate and Digital Signature:

A digital signature is used to verify a messages authenticity. It is basically an encrypted hash of the message (message digest). The recipient can check if the message was tampered with by hashing the received message and comparing this value with the decrypted signature. To decrypt the signature, the corresponding public key is required.

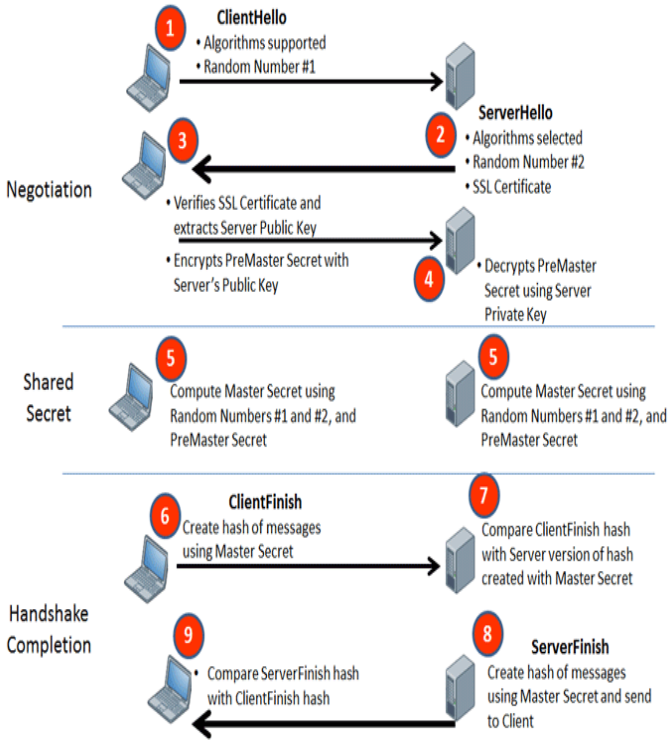
A digital certificate is used to bind public keys to persons or other entities. If there were no certificates, the signature could be easily be forged, as the recipient could not check if the public key belongs to the sender. Thus, digital certificate is used to verify public keys authenticity.

C. SLS/TLS

The idea is to provide security services for transaction on the Internet. For example when a customer shops online, the following security services are desired:

1. The customer needs to be sure that the server belongs to the actual vendor, not an imposter. The customer does not want to give an imposter her credit card number (ensuring server authentication). Likewise the vendor needs to authenticate the customer (ensuring client authentication).
2. The customer and the vendor need to be sure that the contents of the message are not modified during transition (ensuring message integrity).
3. The customer and the vendor need to be sure that an imposter does not intercept sensitive information such as credit card number (ensuring confidentiality).

These are ensured by a transport layer security protocols. The SSL (Secured Socket Layer) and the (Transport Layer Security), TLS is similar to SSL and in fact TLS is the successor of SSL. TLS is actually an IETF (Internet Engineering Task Force) version of the SSL.



Secure Electronic Transaction (SET):

SET was a protocol devised by MasterCard and Visa jointly for secure credit card payments on the Internet. However, it failed to gain attraction in the market.

SET incorporates the following features:

- Confidentiality of information
- Integrity of data
- Cardholder account authentication
- Merchant authentication

SSL vs. SET:

In SSL, data is exchanged securely. However the customer provides critical data such as credit card details to a merchant and hopes that the merchant does not misuse them. This is not possible in SET as the merchant does not know the customer's credit card number; the customer provides these details to a payment gateway.

In SSL a merchant believes that the credit card really belongs to the customer and that it's not a stolen card. However in SET this is very much unlikely, even if it happens, the merchant is safe, since the payment gateway ensures that the customer is not committing fraud.

However to prevent a customer from using another person's credit card number; a new protocol called 3-D Secure is used. It is enhancement to SET. It was developed by Visa and now even Master Card supports it.

SET vs. 3-D Secure:

The main difference between SET and 3-D Secure is that any customer (i.e. a cardholder) has to first enroll on the issuer bank's Enrollment Server. So during a transaction when the merchant receives the payment instruction, it forwards it to the issuer bank. The bank requests the cardholder for their user-id and password that were generated during the Enrollment process. It then verifies against its 3-D secure enrolled users database. Only after the user is verified successfully the issuer bank informs the merchant to accept the card payment. This ensures that no a person cannot user another person's credit card details

REFERENCES

[1] Niranjanamurthy M and Dharmendar chchar. " The Study of e-commerce sewcurity Issues and Solutions " International Journal of Advanced Research in Computer and advanced engineering. Volume -2, Issue -7 . Pages (5-7), July 2013.

[2] L.Byron."Study on Electronic Commerce and Security", International Journal of Advanced Research in Computer and advanced engineering. Volume -1, Issue -5 . Pages (5-7), July 2012.

[3] Dr.Nada.M.A.Al.Slamy."E-Commerce Security",International Journal of Computer Science and network Security", Volume-8, No-5. May 2008.

[4] Website- www.academia.edu/9273437/A_Comparative_Study_o

f_Secure_Electronic_Transaction_Mechanisms_for_E-Commerce.

[5] Mark S Ackerman and Donald T Davis Jr. " Privacy and Security Issues in E-Commerce ". Review Chapter of the new Economy Handbook, in press.

[6] Jarnail Singh."Review of E-Commerce Security Challenges",International Journal of Innovative Research in computer and Communication Engineering. Volume-2, Issue-2. February 2014.

AUTHORS PROFILE

Mr.Sumanta Chatterjee is presently working as an Assistant Professor of JIS College of Engineering, Kalyani, Nadia, West Bengal. He has worked 2 years in the Industry and 5 years in the Academic Sector. He completed his M.Tech degree in Computer Science and Engineering and B.Tech degree in Information Technology from West Bengal University of Technology.

He is recently working on the emerging research field "E-Commerce ".He has made significant contribution on the research field "E-Commerce". He has published more than 15 research papers. He is a member of International Association of Computer Science and Information Techn-ology (IACSIT) and also a member of International Association for Engineers (IAENG).

Mr. Krishnayan Gupta is a final year UG student of Computer Science and Engineering from JIS College of Engineering, Kalyani, Nadia, West Bengal. He has previously published a paper on "E-commerce" in ICICCT 2016, New Delhi.

