ISSUES OF PRIVACY AND SECURITY IN E- COMMERCE

Daya Shankar Singh
Assistant Professor, Department of Computer Science
Sunbeam College For Women Varanasi-221109, Uttar Pradesh, India
E-mail:- vnsdaya@gmail.com

Abstract

From few decades back use of Internet is dramatically increased. With the increment of interest of Internet users, commercial organization also changed their business approaches and makes the business transactions online. This digital business approaches is known as E-Commerce.

85 percent of net surfers shop online and the majority of those shoppers prefer shopping online for reasons like saving time and avoiding crowds.

The people involved in digital business are facing the challenge of issue of privacy and security day to day. The users, merchant and banks are passing through the various types of threats in this business cycle.

Most opinion surveys list "insecurity of financial transactions" and "loss of privacy" among the major impediments to electronic commerce, but in fact most users have only ague ideas about the threats and risks, and a very limited understanding of the technical and legal options for minimizing their risk. As a result all kinds of misperceptions exist.

Due to the lack of trust, most of the clients and cautious business operators may decide to skip use of the Internet and go back to traditional methods of doing business. So to counter this trend, the issues of privacy and security at the both ends must be constantly reviewed and appropriate countermeasures devised.

This paper will discuss architecture of e-commerce and its security and safety issues and will present some of the threats to e-commerce and customer privacy. These threats originate from both hackers as well as the ecommerce site itself.

Denial of Service, fishing, Trojan Horses, viruses and Worms are the major attacks on e-commerce. A brief description of these attacks will be given in this paper.

This paper will also discuss some safer point that should be followed in e-commerce like use of Secure Socket Layer and Firewall.

Keywords*: Privacy and Security Issues, Denial of Services, Trojan Horses, Viruses and Worms, Security Threats, Secure online shopping guidelines.*

1. Introduction

The main purpose of design of the World Wide Web (WWW) in 1989 was to share the information worldwide. Now area of the use of Internet has extended and various ideas prefixed with the letter **e** (electronic) like e-banking, e-booking, e-ticketing , e-governance etc. have been implemented which is accumulatively known as e-commerce. Mass of the people browse through catalogues, searching for best offers, order goods, and pay them electronically.

Moving commercial activity into distributed electronic environments creates a fundamental trust problem: how does a client know what happens at remote sites? The current secure Web infrastructure addresses some issues of server authentication and channel protection, but does not address this core trust problem.

Consider at the Credit Card Transaction Security Problem. The current Web

infrastructure provides secure transmission of a client's information to the server, but what happens there is anyone's guess. For example, consider the credit-card information and transaction amount a client sends when he wishes to purchase something. An adversary who compromises the server (or a malicious server operator) can use this data to carry out lots of mischief. He can increase the amount of the transaction. He can retain the amount but repeat the transaction many times. He can use the credit card information to forge additional transactions. This situation may significantly reduce the potential market for new e-merchants without a pre-established reputation.

Privacy - the control over one's personal data and security, the attempted access to data by unauthorized others are two critical problems for both e-commerce consumers and organization. Without either, consumers will not visit or shop at a site, nor can sites function effectively without considering both.

We examine some technical threats nature and its safety & security one by one.

2. The Threats to E-Commerce

2.1 Security vulnerabilities in e-commerce

There are many points of failure, or vulnerabilities in an e-commerce environment. Even in a simplified e-commerce scenario – a single user contacts a single web site, and then gives his credit card and address information for shipping a purchase – many potential security vulnerabilities exist. Indeed, even in this simple scenario, there are a number of systems and networks involved. Each has security issues.

A user must use a web site and at some point identify, or authenticate himself to the site. Typically, authentication begins on the user's home computer and its browser.

Unfortunately, security problems in home computers offer hackers other ways to steal ecommerce data and identification data from users.

The user's web browser connects to the merchant front-end. When a consumer makes an online purchase, the merchant's web-server usually caches the order's personal information in an archive of recent orders. This archive contains everything necessary for credit-card fraud. Further, such archives often hold 90 days' worth of customers' orders. Naturally, hackers break into insecure web servers to harvest these archives of credit card numbers. Accordingly, an e-commerce merchant's first security priority should be to keep the web servers' archives of recent orders behind the firewall, not on the front-end web servers. Furthermore, sensitive servers should be kept highly specialized, by turning off and removing all inessential services and

applications (e.g., ftp, email).

2.2 Viruses, Worms & Trojan Horses

Viruses, worms and Trojans are all part of a class of software called malware. Malware or malicious code (malcode) is short for malicious software. It is code or software that is specifically designed to damage, disrupt, steal, or in general inflict some other "bad" or illegitimate action on data, hosts, or networks.

There are many different classes of malware that have varying ways of infecting systems and propagating themselves. Malware can infect systems by being bundled with other programs or attached as macros to files. Others are installed by exploiting a known vulnerability in an operating system (OS),

network device, or other software, such as a hole in a browser that only requires users to visit a website to infect their computers. The vast majority, however, are installed by some action from a user, such as clicking an e-mail attachment or downloading a file from the Internet.

Malware cannot damage the physical hardware of systems and network equipment, but it can damage the data and software residing on the equipment.

Comparison:

	Virus	**Worm**
How does it infect?	It inserts itself into a file or executable program.	It exploits a weakness in an application or operating system by replicating itself.
How can it spread?	It has to rely on users transferring infected files to other computer systems.	It can use a network to replicate itself to other computer systems without user intervention.
Does it infect files?	Yes, it deletes or modifies files. Sometimes a virus also changes the location of files.	Usually not. Worms usually only monopolize the CPU and memory.
whose speed is more?	virus is slower than worm.	worm is faster than virus.
Definition	The virus is the program code that attaches itself to application program and when application program run it runs along with it.	The worm is code that replicate itself in order to consume resources to bring it down.

Trojans

A Trojan is another type of malware named after the wooden horse the Greeks used to infiltrate Troy. It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems. After it is activated, it can achieve any number of attacks on the host, from irritating the user (popping up windows or changing desktops) to damaging the host (deleting files, stealing data, or activating and spreading other malware, such as viruses). Trojans are also known to create back doors to give malicious users access to the system.

Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate. Trojans must spread through user interaction such as opening an e-mail attachment or downloading and running a file from the Internet.

Examples and damage:

On the whole, worms are considered more dangerous because of their ability to spread rapidly through the network. A virus harms an individual PC and so its damage is more localized.

Code Red: This worm replicated itself more than 250,000 times within nine hours. Code Red worm, slowed down Internet traffic when it began to replicate itself. Each copy of the worm scanned the Internet for Windows NT or Windows 2000 servers that did not have the Microsoft security patch installed. Each time it found an unsecured server, the worm copied itself to that server. The new copy then scanned for other servers to infect. Depending on the number of unsecured servers, a worm can create hundreds of thousands of copies.

ILOVEYOU: This bug is a virus, which is also known as VBS/Loveletter and Love

Bug, and written in VBScript. It started in the Philippines on May 4, 2000, and spread across the whole world in one day, as most computers are connected with the Internet and email systems. It infected 10% of all computers connected to the Internet causing about 5.5 billion dollars in damage. The damage was mainly done due to getting rid of the virus and explaining the receiver that the sender didn't mean to say "I LOVE YOU".

If you receive email with a subject line with the phrase ILOVEYOU (all one word, no spaces) in it… DON'T OPEN the attachment named Love-Letter-For-You.txt.vbs.

A scan of the Visual Basic code included in the attachment reveals that the virus may be corrupting MP3 and JPEG files on users' hard drives, as well as mIRC, a version of Internet Relay Chat. It also appears to reset the default start page for Internet Explorer.

Safety & Security

To protect you from the ILOVEYOU virus, and it's variants, first and foremost, never open any email attachment that you are uncertain of. That said, I strongly recommended that if you do not use Visual Basic scripting, (Most Don't) you should turn this option off.

The system can best be protected against by keeping up-to-date and installing security patches provided by operating systems and application vendors.

Also while downloading a file from the internet; many other pop-ups appear which might have spyware. So it is advisable not to click or install such a toolbar, unless the user is sure about the working of the toolbar.

2.3 Denial of Service (DOS) Attacks

When a denial of service (DoS) attack occurs, a computer or a network user is unable to access resources like e-mail and the Internet. An attack can be directed at an operating system or at the network.

How does an attack work?

One way to attack a company's network or website is to flood its systems with information. Web and e-mail servers can only handle a finite amount of traffic and an attacker overloads the targeted system with packets of data.

Impact

Denial-of service attacks can essentially disable the computer or the network. Depending on the nature of the enterprise, this can disable your organization.

Security

Separate Client and Server Addresses

- The IP address space can be divided into a set of client addresses and a set of server addresses.
- allow clients to initiate connections to servers, but not vice versa nor servers to initiate connections to servers.

RPF Checking of Server Addresses

- Using path-based client addresses severely restricts source-address spoofing by a client, but it does not restrict spoofing by servers.
- **R**everse **P**ath **F**orwarding largely prevents a server from spoofing the address of a server in a different domain.

Middlewalls

- simple special-purpose high-speed firewalls being deployed in the core of the Internet at inter-domain boundaries to serve as a filter of sorts
- Gives Upstream access control to a server under stress

DoS Shortfalls

- DoS attacks are unable to attack large

bandwidth websites – one upstream client cannot generate enough bandwidth to cripple major megabit websites.

- New distributed server architecture makes it harder for one DoS to take down an entire site.
- New software protections neutralize existing DoS attacks quickly
- Service Providers know how to prevent these attacks from effecting their networks.
- "Old" Internet Technology something new needs to take it's place (Hackers want the challenge of a new technology).

2.4 Fishing

Phishing is a form of data theft via submission of personal information to a fraudulent entity that poses as a legitimate one. This typically happens by sending data to a form that looks genuine but actually feeds into an underground database. Think of it as fraudsters fishing for your sensitive info – you're the fish and the worm is the fake entry field.

The most popular example relates to your bank account. A phisher will obtain your email address and send a message instructing you to update account details. You're then prompted to click a link that takes you to a website similar to your bank's. You willingly enter your information, never knowing that it's going directly to an identity thief.

As are most things online, phishing is evolving. The RSA Online Fraud Report for January 2010 indicates that phishing attacks increased by 17% in 2009. Additionally, consumer awareness of phishing schemes has increased to 76%. Awareness truly is the key to prevention – phishing is a basic tactic that is easily avoided by seeing the signs.

The only downside of this awareness is that fraudsters are now finding new ways to obtain the information important to the success of your online business. Take a look at these developing methods:

Security

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Don't send sensitive information over the Internet before checking a website's security .
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available

online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).

- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic.
- Take advantage of any anti-phishing features offered by your email client and web browser.

What do you do if you think you are a victim?

- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.
- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.

2.5 SQL Injection

A common hacking technique in which malicious code is used to access the databases of websites that don't have proper input validation. The malicious code returns unintended values or error messages to the hacker, who can then use the information to access the database, retrieve and modify data, insert malware or exploit other weaknesses.

Security

Such type of attack is due to the mistake of the developers of e-commerce site, here is some suggestion for them:

- Validating all user input values by testing type, length, format and range.
- Limiting or eliminating error code responses to external system users.
- Strengthening database security by disabling default or unnecessary stored procedures, disabling direct SQL queries, installing the latest security patches and protecting database and local administrative accounts.
- **Cross-Site Scripting**:

  A hacking technique in which malware is used to hijack user sessions, redirect users or take over the user's browser. Like SQL injection, cross-site scripting targets websites that don't have proper input validation.

Security

Such an attack can be mitigated by:

- Encoding the Web page output based on input parameters.
- Filtering input parameters for special characters.
- Filtering output based on input parameters for special characters.

Authentication and Session Management Flaws:

These weaknesses range from unprotected usernames or passwords in databases and application timeouts that are not properly set, to exposed session IDs in the website URL. Other vulnerabilities include weak password creation rules, poor password change or recovery features, and weak session IDs.

Security

Implementing strong authentication and session management controls, which can be found on the Application Security Verification Standard page at the Open Web Application Security Project (OWASP) website.

3. Prevention from Threats

There are many established policies and standards for avoiding security issues. However, they are not required by law. Some basic rules include:

- Never store a user's password in plain text or encrypted text on the system. Instead, use a one-way hashing algorithm to prevent password extraction.
- Employ external security consultants (ethical hackers) to analyze your system.
- Standards, such as the Federal Information Processing Standard (FIPS), describe guidelines for implementing features. For example, FIPS makes recommendations on password policies.
- Ensure that a sufficiently robust encryption algorithm, such as triple DES or AES, is used to encrypt all confidential information stored on the system.
- When developing third-party software for e-Commerce applications, use external auditors to verify that appropriate processes and techniques are being followed.
- Recently, there has been an effort to consolidate these best practices as the Common Criteria for IT Security Evaluation (CC). CC seems to be gaining attraction. It is directly applicable to the development of specific e-Commerce sites and to the development of third party software used as an infrastructure in e-Commerce sites.

Security best practices remain largely an art rather than a science, but there are some good guidelines and standards that all developers of e-Commerce software should follow.

Use this security checklist to protect yourself as a shopper:

- Whenever you logon, register, or enter private information, such as credit card data, ensure your browser is communicating with the server using SSL.
- Do not shop at a site when the browser does not recognize the server's SSL certificate. This check is done by your browser the first time your URL becomes HTTPS for the site. If the certificate is not recognized, then your browser presents a pop-up message to inform you.
- Use a password of at least 6 characters, and ensure that it contains some numeric and special characters (for example, c0113g3).
- Avoid reusing the same user ID and password at multiple Web sites.
- If you are authenticated (logged on) to a site, always logoff after you finish.
- Use a credit card for online purchases. Most credit card companies will help you with non-existent or damaged products.
- A bricks and mortar store with an online brand is most likely a legitimate site. However, the site may still have vulnerabilities.

Education

Education is the best way to ensure that your customers take appropriate precautions:

- Install personal firewalls for the client machines.
- Store confidential information in encrypted form.
- Encrypt the stream using the Secure Socket Layer (SSL) protocol to protect information flowing between the client and the e-Commerce Web site.
- Use appropriate password policies, firewalls, and routine external security audits.
- Use threat model analysis, strict development policies, and external security audits to protect ISV software running the Web site.

What additional steps can you take to protect your privacy?

- Do business with credible companies - Before supplying any information online, consider the answers to the following questions: do you trust the business? is it an established organization with a credible reputation? does the information on the site suggest that there is a concern for the privacy of user information? is there legitimate contact information provided?
- Do not use your primary email address in online submissions - Submitting your email address could result in spam. If you do not want your primary email account flooded with unwanted messages, consider opening an additional email account for use online (see Reducing Spam for more information). Make sure to log in to the account on a regular basis in case the vendor sends information about changes to policies.
- Avoid submitting credit card information online - Some companies offer a phone number you can use to provide your credit card information. Although this does not guarantee that the information will not be compromised, it eliminates the possibility that attackers will be able to hijack it during the submission process.
- Devote one credit card to online purchases - To minimize the potential damage of an attacker gaining access to your credit card information, consider opening a credit card account for use only online. Keep a minimum credit line on the account to limit the amount of charges an attacker can accumulate.
- Avoid using debit cards for online purchases - Credit cards usually offer some protection against identity theft and may limit the monetary amount you will be responsible for paying. Debit cards, however, do not offer that protection. Because the charges are immediately deducted from your account, an attacker who obtains your account information may empty your bank account before you even realize it.
- Take advantage of options to limit exposure of private information - Default options on certain websites be chosen for convenience, not for security. For example, avoid allowing a website to remember your password. If your password is stored, your profile and any account information you have provided on that site is readily available if an attacker gains access to your computer. Also, evaluate your settings on websites used for social networking. The nature of those sites is to share information, but you can restrict access to certain information so that you limit who can see what (see Staying Safe on Social

Network Sites for more information).

4. Conclusion

This article outlined the key players and security attacks and defenses in an e-Commerce system. Current technology allows for secure site design. It is up to the development team to be both proactive and reactive in handling security threats, and up to the shopper to be vigilant when shopping online.

References

1. Computerworld, 5/29/00, Vol 34.no 22.
2. Peter Keen. Ensuring E-Trust. ComputerWorld,
3. York Times Service, article appeared in 6/4/00 issue
4. Conference, SANS Institute 3/13/00 issue
5. Commerce: A Manager's Guide, Addison-Wesley, ISBN: 0-201-88067-9
6. The SANS Institute, www.sans.org/topten.htm
7. https://www.us-cert.gov/ncas/tips/ST04-013
8. http://www.securityfocus.com templates/forum_mes
9. www.sans.org/ddos_roadmap.html
10. http://en.wikipedia.org/wiki /Sasser_worm
11. http://virusall.com/computer %20 worms/worms.php
12. http://www.microsoft.com/protect/computer/basics/virus.mspx
13. http://en.wikipedia.org/wiki/Computer_virus
14. http://www.computereconom-ics.com/article.cfm?id=932
15. http://www.cert.org/tech_tips/denial_of_service.html