Journal of Information and Operations Management
ISSN: 0976–7754 & E-ISSN: 0976–7762 , Volume 3, Issue 1, 2012, pp-217-221
Available online at http://www.bioinfo.in/contents.php?id=55

NETWORK MANAGEMENT, SECURITY & PRIVACY ISSUES IN E-COMMERCE

RAIWANI Y.P.

Dept. of Computer Science, H N B Garhwal University Srinagar, Srinagar Garhwal (Uttarakhand) -246 174 India
*Corresponding Author: Email: yp_raiwani@yahoo.com

Received: December 12, 2011; Accepted: January 15, 2012

Abstract - In addition to buying and selling products online E-com also includes the entire online process of developing, marketing, selling, delivering, servicing and paying for products and services. Any disruption in network service, even for a short period, can lead to serious problems, and affect thousands and millions of people. The tremendous increase in online processing has been accompanied by an equal rise in the number and type of attacks against the control over one's personal data and the attempted access to data by unauthorized users. Without either, i.e. Privacy and Security, consumers will not visit or shop at a site, nor can sites function effectively without considering both. "The absence of consumer privacy protection may in fact be the number one obstacle to the growth of e-commerce." Some attacks have used vulnerabilities that are common in any web application, such as SQL injection or cross-site scripting. With proper understanding of business needs, management of enterprise information security resources, focus on consumer privacy, awareness about latest vulnerabilities, security threats and their solution, e-commerce will mature profusely and will immensely benefit every individual. This Paper reviews the current state of the art and the relevance for privacy and security respectively from technical to economic perspectives.
Keywords- E-Commerce; elements, phases, network management, privacy, security, and vulnerabilities.

Citation: Raiwani Y.P. (2012) Network Management, Security & Privacy Issues in E-Commerce. Journal of Information and Operations Management ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, pp-217-221.

Introduction

Contemporary electronic commerce involves everything from ordering "digital" content for immediate online consumption, to ordering conventional goods and services, to "meta" services to facilitate other types of electronic commerce. On the institutional level, big corporations and financial institutions use the internet to exchange financial data to facilitate domestic and international business. Network management, privacy and security are very hot and pressing issues for electronic commerce. Elements of typical e-commerce transactions are as follows [1]:

i) A product or service
ii) An area of operation i.e. A Website, that displays the product/ service offered and where business transaction can take place.
iii) A mean for the people to visit the place or Website.
iv) A mean for accepting payments, e.g. through net-banking, credit/debit cards, or through traditional billing methods either online or through mail.
v) A system to accept rejected/returned goods and services.
vi) A system to handle warranty claims, if required.
vii) A system to provide regular customer service through E- mail, Voice-mail, online forms, and online knowledge bases and through frequently asked questions (FAQs).

Steps to Follow in E-Commerse

Awareness, Presence, Pilot, Adoption, Process Investment and Cross Process Integration, may be six distinct phases of ideal E-Commerce.

Awareness step for most companies is building of workflow based mailing application tools for streamlining communication, cross the organization. This helps in instituting the basic understanding of the technology across the company. Internet based mailing tools can also helps drive a culture of openness. Presence phase translates into opening a gateway to the external world by establishing a web presence. A regularly updated web page opens a window to the outside users. Pilot phase is the first step in developing specific levels of interactivity with the web user. The idea is to provide a "read only" access to a basic business data. For the organization it

translates into developing secure and reliable links to the outside world, with an ability to publish real time information. In adoption phase companies can provide greater value to their customers by allowing them to transact with the core system of the organization. It significantly reduces the cost per transaction for the company and allow the customer greater flexibility of interacting with the company. An essential requirement here is to integrate the new web applications with the legacy transaction systems. Today's sophisticated customers want to be able to interact with organizations any time, anyhow. So, companies are looking for applications to manage and integrate all of these methods of communications into their Customer Relationship Management (CRM) Process. Process investment phase is to invest in the organization's process -transforming them and integrating multiple backend systems to create common user experience. In Cross Process Integration phase, the organization can decide to integrate all the customer touch points across all operational systems from supply to demand fulfilment. This phase requires business process redefinition and integration across multiple process and legacy systems. The customer can now at their convenience interact with any part of the company. The customer can book an order on the web, get a confirmation note with indicative delivery date, track the order through the manufacturing process and finally locate the order during the delivery phase till the order is fulfilled at the doorstep.

Privacy- Few Internet-related issues have generated as much controversy, conflict, and concern as privacy. The debate encompasses freedom of expression, security of intellectual property, marketers' abilities to gather information about consumers on the Web, workplace productivity, and rights of Internet users. Governments, industry, and citizen-advocacy groups are struggling to define workable privacy guidelines and enforcement procedures that will satisfy all parties in the rapidly changing universe of the commercial Internet. The tremendous increase in online processing has been accompanied by an equal rise in, the rate of personal data collection, commercial transactions, and surveillance of Web users.

Surveillance- Commercial Web sites' early collection of user data generally consisted only of how many hits a particular site received. But as Internet software and technology became more sophisticated, online information-gathering techniques grew more powerful and precise. Web sites can identify visitors via cookies **(**small text files that the Web site writes to a user's hard drive). Cookies contain the name of their proprietary Web site and a unique identifier they assign to a user's computer, which is written to the cookie file the first time a person, visits the site. On subsequent visits, the Web site reads the cookie and recognizes the user's computer. Only the originating site can read the cookie, which may also store user passwords. Most browsers contain a feature that permits users to disable cookies.

Banner ads- are another online information-gathering device. They are controlled by network advertisers, third-party companies that function as intermediaries between advertisers and Web-site companies. Banner ads place and read cookies, just like Web sites. Network advertisers can track users' surfing habits across the Web by placing banner ads on thousands of different Web pages. Cookies and banner ads can only generate aggregate user profiles, based on the computers used for browsing rather than individual human users. To collect more user-specific data, some companies permit users to customize their sites. Often they give users an incentive for registering, such as offering access to restricted content, in the hopes of gathering more detailed information about visitors. This helps online merchants fine-tune their profiles of individual users. When users enter personal data required for site registration or online purchases, the company gains access to that information. Many groups have motives for collecting and storing users' personal information online. Governmental and law-enforcement officials contend that access to such information spurs rapid identification of criminals, helping to combat credit fraud, terrorism, and illegal immigration. Businesses have a seemingly insatiable appetite for minute details about the identities and personal habits of online consumers. This information enables them to tailor promotions and advertising in hopes of generating sales and increased profits. Individual Web users appreciate the ease and efficiency provided by personalized Web sites, which store credit card information for future purchases, remember passwords, and modify Web pages automatically to cater to their interests. But commercial and governmental organizations can compromise the privacy of online users. For example, Toysmart.com, an online toy retailer, contained a privacy statement guaranteeing that it would not make its customer list available to outside organizations. But when its operation failed amid the dotcom shakeout, Toysmart.com attempted to sell its customer database to a third party [2].

Privacy Specific to E-commerce- Privacy remains an important issue for electronic commerce. Various study showed that nearly two thirds of the consumers surveyed "would shop more online if they knew retail sites would not do anything with their personal information". Most e-commerce Web sites monitor the movements of online visitors and consumers. Often companies sell or release customer information to third parties to promote additional products or to support direct-marketing campaigns. Online marketing generates spam, or "junk" e-mail, in the form of unsolicited advertisements and promotions. Studies indicate that many customers consider these practices an un-warranted invasion of their privacy. Internet users can block monitoring of their online behaviour in various ways. Two simple examples are giving false information when personal data is requested and encrypting their own e-mail. Software are also available to prevent online tracking and block spam. But despite users' nervousness about online surveillance, only few percent of Internet users set their browsers to reject cookies.

Workplace Privacy: Employees constitute another group whose Internet use has come under increasing scrutiny. Work-place surveillance pits employers' financial interests, the protection of corporate intellectual property, workplace productivity, and security against the privacy rights of employees. Frequently the supervision of employee behaviour falls to the information technology (IT) department. Many companies use monitoring software that scans not only Web-site URLs, but the actual content of Web pages, to determine whether employees' online activity is linked to their workplace duties. Global Privacy Standards: Some countries possess stringent privacy rules that restrict all unauthorized transmission of personal data of their citizens to any countries lacking legal standards that guarantee a similar level of online privacy protection. Some countries also created governmental privacy directors or agencies

to oversee Internet privacy.

Privacy for Children- There's a common understanding that children need special legal protections from harm and exploitation. Children are particularly vulnerable to manipulation by online marketers and more likely than adults to surrender personal or family information on the Web. To remedy such situations Children's Online Privacy Protection Act must be implemented, which prohibits organizations from gathering personal information online from children under age 13, unless their parents give "verifiable" consent before the information is collected or shared with third parties. Web -site operators must also post their privacy policies online and notify parents of the type of information that they collect.

Global Privacy Standards: Some countries possess stringent privacy rules that restrict all unauthorized transmission of personal data of their citizens to any countries lacking legal standards that guarantee a similar level of online privacy protection. Some countries also created governmental privacy directors or agencies to oversee Internet privacy

Self-regulation- Many countries relied primarily on industry self-regulation to ensure that Internet users receive an adequate level of privacy protection. Their businesses argue that self-regulation encourages industry to safeguard user privacy in order to boost consumers' confidence in the security of e-commerce transactions. In essence, business leaders believe that market forces will punish companies that breach privacy, causing them to lose business, while rewarding with increased sales those that protect privacy. In the spirit of self-regulation, many e-businesses post privacy policies on their Web sites and permit opt-out avenues for users who don't wish to submit personal information online. When companies violate their own privacy policies, breach of contract suits and actions for deceptive business practices or false advertising can be brought against them. But this arrangement provides no penalties for failure to have a privacy policy, and such policies rarely cover the actions of third parties, such as network advertisers, who might acquire personal data online

Network Management- Network management can be defined as monitoring, testing, configuring and trouble-shooting network components to fulfil the smooth and efficient operation of the network that provides the pre-defined quality of service for users. Issues related to the network management can be classified into five phases [3].

Configuration Management- Entities physically or logically related have an initial configuration when the network is setup, but can change with time, so the reconfiguration and subsequently the documentation of hardware, software and user account can be a daily occurrence in a large network; must be managed.

Fault Management- Fault is defined as abnormal condition in the system i.e. when fault occurs, either the system stop working properly or the system creates excessive errors. The Reactive fault management is responsible for detecting, isolating, correcting and recording fault. The record should show the exact location of the fault, the possible cause, the action taken to correct the fault, the cost and time it took for each step. Whereas the Proactive fault management tries to prevent faults from occurring. Although this is not always possible, some types of failures can be predicted and prevented. For example if a manufacturer specifies a lifetime for a component, it is good strategy to replace it before that time.

Performance Management- Tries to monitor and control the network to ensure that it is running as efficiently as possible. It also tries to quantify performance using some measurable quantity such as capacity, traffic, and throughput or response time. Capacity means if a LAN is designed for 100 stations, it will not operate properly if 200 stations are connected to it. During peak hours when the system is heavily used, blocking may occur, if there is excessive traffic. Throughput is monitored to make sure that it is not reduced to unacceptable levels. Any increase in response time is very serious condition as it is an indication that the networking is working above its capacity.

Accounting Management- Is the control of user access to network resources through charges i.e. it prevents user from monopolizing limited network resources and using the system inefficiently.For this Network managers can do short and long term planning based on the demand for network use.

Security Management- Is based on cryptography, which can provide confidentiality, integrity, authentication and non-repudiation of messages to make them secure and immune to attack. Privacy is handled by encryption. In PKI (public key infrastructure) a message is encrypted by a public key, and decrypted by a private key. The public key is widely distributed, but only the recipient has the private key. For authentication (proving the identity of the sender, since only the sender has the particular key) the encrypted message is encrypted again, but this time with a private key. Such procedures form the basis of RSA (used by banks and governments) and PGP (Pretty Good Privacy, used to encrypt emails).Unfortunately, PKI is not an efficient way of sending large amounts of information, and is often used only as a first step — to allow two parties to agree upon a key for symmetric secret key encryption. Here sender and recipient use keys that are generated for the particular message by a third body: a key distribution center. The keys are not identical, but each is shared with the key distribution center, which allows the message to be read. Then the symmetric keys are encrypted in the RSA manner, and rules set under various protocols. Naturally, the private keys have to be kept secret, and most security lapses indeed arise here.

Digital Signatures and Certificates- Digital signatures meet the need for authentication and integrity. To vastly simplify matters, a plain text message is run through a hash function and so given a value: the message digest. This digest, the hash function and the plain text encrypted with the recipient's public key is sent to the recipient. The recipient decodes the message with their private key, and runs the message through the supplied hash function to that the message digest value remains unchanged (message has not been tampered with). Very often, the message is also time stamped by a third party agency, which provides non-repudiation. What about authentication? How does a customer know that the website receiving sensitive information is not set up by some other party posing as the e-merchant? They check the digital certificate. This is a digital document issued by the CA (certification authority Verisign, Thawte, etc.) that uniquely identifies the merchant. Digital certificates are sold for emails, e-merchants and web-servers

Secure Socket Layers- Information sent over the Internet commonly uses the set of rules called TCP/IP (Transmission Control Protocol / Internet Protocol). The information is broken into packets, numbered sequentially, and an error control attached. Individual packets are sent by different routes. TCP/IP reassembles them

in order and resubmits any packet showing errors. SSL uses PKI and digital certificates to ensure privacy and authentication. The procedure is something like this: the client sends a message to the server, which replies with a digital certificate. Using PKI, server and client negotiate to create session keys, which are symmetrical secret keys specially created for that particular transmission. Once the session keys are agreed, communication continues with these session keys and the digital certificates.

PCI, SET, Firewalls and Kerberos- Credit card details can be safely sent with SSL, but once stored on the server they are vulnerable to outsiders hacking into the server and accompanying network. A PCI (peripheral component interconnect: hardware) card is often added for protection, therefore, or another approach altogether is adopted: SET (Secure Electronic Transaction), developed by Visa and MasterCard, uses PKI for privacy, and digital certificates to authenticate the three parties: merchant, customer and bank. More importantly, sensitive information is not seen by the merchant, and is not kept on the merchant's server. Firewalls (software or hardware) protect a server, a network and an individual PC from attack by viruses and hackers. Equally important is protection from malice or carelessness within the system, and many companies use the Kerberos protocol, which uses symmetric secret key cryptography to restrict access to authorized employees.

Security Vulnerability

There are a number of reasons why security vulnerabilities arise in shopping cart and online payment systems. One of the main reasons for such vulnerabilities is the fact that web application developers are often not very well versed with secure programming techniques. As a result, security of the application is not necessarily one of the design goals. This is exacerbated by the rush to meet deadlines in the fast-moving e-commerce world. Even one day's delay in publishing a brand new feature on your website could allow a competitor to steal a march over you. We've typically found this in cases where e-commerce sites need to add functionality rapidly to deal with a sudden change in the business environment or simply to stay ahead of the competition. In such a scenario, the attitude is to get the functionality online; security can always be taken care of later [4]. Another reason why security vulnerabilities appear is because of the inherent complexity in most online systems. Nowadays, users are placing very demanding requirements on their e-commerce providers, and this requires complex designs and programming logic. In a number of cases, we've found that e-commerce sites tout their 128-bit SSL certificates as proof that their sites are well secured. The gullibility of customers to believe in this has reduced over the past few years, but even now there are thousands of web sites displaying Verisign or Thawte certificate icons as proof of their security. The following sections look at common security vulnerabilities that have been discovered in shopping cart and online payment systems.

SQL Injection- SQL injection refers to the insertion of SQL metacharacters in user input, such that the attacker's queries are executed by the back-end database. Typically, attackers will first determine if a site is vulnerable to such an attack by sending in the single-quote (') character. The results from an SQL injection attack on a vulnerable site may range from a detailed error message, which discloses the back-end technology being used, or allowing the attacker to access restricted areas of the site because he manipulated the query to an always-true Boolean value, or it may even allow the execution of operating system commands. SQL injection techniques differ depending on the type of database being used. For instance, SQL injection on an Oracle database is done primarily using the UNION keyword [5] and is much more difficult than on the MS SQL Server, where multiple queries can be executed by separating them with the semi-colon.

Bill Manipulation- This is a vulnerability that is almost completely unique to online shopping carts and payment gateways. In the most common occurrence of this vulnerability, the total payable price of the purchased goods is stored in a hidden HTML field of a dynamically generated web page. An attacker can use a web application proxy such as Achilles to simply modify the amount that is payable, when this information flows from the user's browser to the web server. The final payable price can be manipulated by the attacker to a value of his choice. This information is eventually sent to the payment gateway with whom the online merchant has partnered. If the volume of transactions is very high, the price manipulation may go completely unnoticed, or may be discovered too late. Repeated attacks of this nature could potentially cripple the viability of the online merchant.

XSS scripting- The Cross-site Scripting (XSS) [8] attack is primarily targeted against the end user and leverages two factors: (i) The lack of input and output validation being done by the web application (ii) The trust placed by the end-user in a URL that carries the vulnerable web site's name. The XSS attack requires a web form that takes in user input, processes it, and prints out the results on a web page, which also contains the user's original input. In this case, if the user input is printed out without being parsed, then an attacker can embed JavaScript by supplying it as part of the input. By crafting a URL, which contains this JavaScript, a victim can be social engineered into clicking on it, and the script executes on the victim's system. In this case, when the victim clicks on this link, a message box with the text "OK" will open up on his system. In most cases, the attacker would craft the URL in order to try and steal the user's cookie, which would probably contain the session ID and other sensitive information. The JavaScript could also be coded to redirect the user to the attacker's website where malicious code could be launched using ActiveX controls or by utilizing browser vulnerabilities such as those in Internet Explorer or Netscape Navigator. However, the JavaScript can also be used to redirect the user to a site that looks similar to the original web site and requests the user to enter sensitive information such as his authentication details for that web site, or his credit card number or social security number.

Remote command execution- The most devastating web application vulnerabilities occur when the CGI script allows an attacker to execute operating system commands due to inadequate input validation. This is most common with the use of the system call in Perl and PHP scripts. Using a command separator and other shell metacharacters, it is possible for the attacker to execute commands with the privileges of the web server.

Authentication and Authorization- Authentication mechanisms that do not prohibit multiple failed logins can be attacked using tools such as Brutus [9]. Similarly, if the web site uses HTTP Basic

Authentication or does not pass session IDs over SSL (Secure Sockets Layer), an attacker can sniff the traffic to discover user's authentication and/or authorization credentials. Since HTTP is a stateless protocol, web applications commonly maintain state using session IDs or transaction IDs stored in a cookie on the user's system. Thus this session ID becomes the only way that the web application can determine the online identity of the user. If the session ID is stolen (say through XSS), or it can be predicted, then an attacker can take over a genuine user's online identity vis-à-vis the vulnerable web site. Here the algorithm used to generate the session ID is weak, it is trivial to write a Perl script to enumerate through the possible session ID space and break the application's authentication and authorization schemes [10].

Cyber Law

In India, The IT Act, 2000 as amended by The IT (Amendment) Act, 2008 is known as the Cyber law. It has a separate chapter XI entitled "Offences", in which various cyber crimes have been, declared as penal offences punishable with imprisonment and fine. As per IT (Amendment) Act, 2008, "Cyber Security" is defined under Section (2) (b) means protecting information, equipment, computer devices, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction. If crime is proved under IT Act, accused shall be punished for imprisonment, which may extend to three years or with fine, which may extend to five lakh rupees or both [11].

Conclusion

The e-commerce industry is growingly addressing security issues on their internal networks. There are guidelines for securing systems and networks available for the e-commerce systems personnel to read and implement. Educating the consumer on security issues is still in the infancy stage but will prove to be the most critical element of the e-commerce security architecture. Training programs, orientation programs will become more critical in order to increase the general populace's awareness of security on the Internet. IT and financial control/audit groups within the e-commerce site should form an alliance to overcome the general resistance to implementing security practices at the business level. In e-commerce systems, the vulnerabilities acquire a graver dimension due to the financial nature of transactions. What is at stake is not only a direct loss of revenues, but companies may face a serious loss to their reputations as well. In some cases, they may be faced with legal penalties for violating customer privacy or trust. One of the key activities during the design phase should be a detailed risk assessment exercise, the developers along with security experts must analyse issues related to Network management, Security vulnerabilities and privacy probabilities for the system.

References

[1] http://money.howstuffworks.com/ecommerce2.htm
[2] *http://ecommerce.hostip.info/pages/*867-874.
[3] Forouzan Behrouz A, *Data communication and Networking, fourth edition*.
[4] *http://www.securityfocus.com/bid*.
[5] Finnigan Pete, *SQL injection and Oracle.*
[6] *http://www.securityfocus.com/infocus/*1644.
[7] *Anley Chris,Advanced SQL injection*.
[8] *http://www.nextgenss.com*.
[9] *http://achilles.mavensecurity.com*.
[10] *http://www.cert.org/advisories*.
[11] *http://www.hoobie.net*.
[12] *Endler David, Brute-Force Exploitation of Web Application Session IDs*.
[13] *http://www.idefense.com*.
[14] Mali Prashant (2011) *Types of Cyber Crimes & Cyber Law in India, CSIC*.