A Review on Ecommerce Security

Mrs. Sunita S. Padmannavar

ABSTRACT

The rapid evolution of computing and communication technologies and their standardizations have made the boom in e-commerce possible. Lowering of the cost of operation, increase in the speed of transactions, and easy global reach to customers and vendors have been the reasons for the overwhelming popularity of this new way of commerce. Due to the impersonal nature of communication over the internet, there are many security concerns involved. These concerns range from the verification for the identities of the people concerned, to the protection and validity of data in transfer. This paper will discuss fundamental security threats associated with the increasing reliance of e-commerce for business transactions and various ways to minimize these threats.

Keywords - E-commerce, E-markets, E-tailing, B2B, B2C, B2G, C2C, m-commerce, electronic payment system, E-banking

I. INTRODUCTION

E-commerce is usually associated with buying and selling over the Internet, or conducting any transaction involving the transfer of ownership or rights to use goods or services through a computer-mediated network. Thus ***E-commerce*** is the use of electronic communications and digital information processing technology in business transactions to create, transform, and redefine relationships for value creation

between or among organizations, and between organizations and individuals.

Benefits of Electronic Commerce:

• Global Distribution of Information

• Expands the Market Reach- beyond Geographic boundaries (Small Business can also access global marketplace)

• Saves on Cost of Printing Information brochure and Catalogs

• Everyone accesses the latest version of product, catalog, and information

• Efficient and quick delivery of information needs of users

II. TYPES OF E-COMMERCE

The major different types of e-commerce are: business-to-business (B2B), business-to-consumer (B2C), business-to-government (B2G), consumer-to-consumer (C2C), and mobile commerce (m-commerce).

B2B e-commerce is simply defined as e-commerce between companies. E-markets are simply defined as Web sites where buyers and sellers interact with each other and conduct transactions

Business-to-consumer e-commerce, or commerce between companies and consumers, involves customers gathering information, purchasing physical goods (i.e., tangibles such as books or consumer products) or information goods (or goods of electronic material or digitized content, such as software, or e-books) and, for information goods, receiving products over an electronic network. E-tailing (or electronic retailing) is the selling of retail goods on the Internet. It is the most common form of business-to-consumer (B2C) transaction.

Business-to-government e-commerce or B2G is generally defined as commerce between companies and the public sector. It refers to the use of the Internet for public procurement, licensing procedures, and other government-related operations.

Consumer-to-consumer e-commerce or C2C is simply commerce between private individuals or consumers. For example eBay, allows online real-time bidding on items being sold in the Web

Consumer-to-business (C2B) transactions involve reverse auctions, which empower the consumer to drive transactions.

M-commerce (mobile commerce) is the buying and selling of goods and services through wireless technology.

The existing practices in buying and paying online

In most developing countries, the payment schemes available for online transactions are the following:

A. Traditional Payment Methods

- **Cash-on-delivery.** Many online transactions only involve submitting purchase orders online. Payment is by cash upon the delivery of the physical goods.
- **Bank payments.** After ordering goods online, payment is made by depositing cash into the bank account of the company from which the goods were ordered.

Delivery is likewise done the conventional way.

B. Electronic Payment Methods

- **Innovations affecting consumers**, include credit and debit cards, automated teller machines (ATMs), stored value cards, and e-banking.
- **Innovations enabling online commerce** are e-cash, e-checks, smart cards, and encrypted credit cards. They

are employed by a few large companies in specific secured channels on a transaction basis.

- **Innovations affecting companies** pertain to payment mechanisms that banks provide their clients, including inter-bank transfers through automated clearing houses allowing payment by direct deposit.

An electronic payment system

An electronic payment system (EPS) is a system of financial exchange between buyers and sellers in the online environment that is facilitated by a digital financial instrument (such as encrypted credit card numbers, electronic checks, or digital cash) backed by a bank, an intermediary, or by legal tender.

Many developing countries are still cash-based economies. Cash is the preferred mode of payment not only on account of security but also because of anonymity, which is useful for tax evasion purposes or keeping secret what one's money is being spent on. For other countries, security concerns have a lot to do with a lack of a legal framework for adjudicating fraud and the uncertainty of the legal limit on the liability associated with a lost or stolen credit card. In some, among the relevant issues that need to be resolved with respect to EPS are: consumer protection from fraud through efficiency in record-keeping; transaction privacy and safety, competitive payment services to ensure equal access to all consumers, and the right to choice of institutions and payment methods.

E-banking includes familiar and relatively mature electronically-based products in developing markets, such as telephone banking, credit cards, ATMs, and direct deposit. It also includes electronic bill payments and products mostly in the developing stage, including stored-value cards (e.g., smart cards/smart money) and Internet based stored value products.

Due to the impersonal nature of communication over the internet, there are many security concerns involved. These concerns range from the verification for the identities of the people concerned, to the protection and validity of data in transfer. Despite the increasing use of the internet in business transactions, a major security issue with e-commerce activities is associated with confidentiality of electronic payment details. A wide range of security concerns exist: Disruption or denial of service attacks , Unauthorized use of credit cards ,Invasion of privacy—especially related to minors , Unauthorized changes to database records , Fraud , Misuse of data about vulnerable populations , Spreading viruses , Employee misuse of the Net , Employee privacy ,Email harassment etc. The security vulnerabilities affect both individuals and groups, public and private entities, and large and small organizations.

III. SECURE TRANSACTIONS

Secure email and web transactions are important not only for ecommerce but also for Internet enabled healthcare, education, government services, and even entertainment. Secure ecommerce transactions require web servers and browsers that can handle:

- Digital certificates that are confirmed by a third-party Certification Authority and attest to a web site's real identity
- Secure Socket Layer (SSL) protocol that enables encryption (Look for **https** instead of **http** in the URL)
- Digital payments that are likely to be credit card transactions but may take another form

Digital certificates are handled quickly and quietly by server and browser unless there is some sort of problem, in which case the user is notified. When the SSL protocol is invoked, the user is notified and the image of a closed lock may appear on the browser screen. Since consumers are the weakest link, organizations offering ecommerce must take special care to alert them about possible security problems.

Key customer-related elements include:

- Uses a search engine to find product and vendor's web site.
- Looks for signs that web site is legitimate.
- Browses the product catalog.
- Selects purchases and clicks shopping cart icon.
- Transfers to secure **https** page and enters credit card info which is encrypted and sent to processor. Receives email confirmation.
- Receives email notification that item was shipped.
- Product arrives and buyer is satisfied with safe, secure online purchase.

It's important to make your customers feel comfortable about ordering online. Keeping your site and customer data safe has to meet four requirements:

- Privacy: information must be kept from unauthorized parties.
- Integrity: message must not be altered or tampered with.
- Authentication: sender and recipient must prove their identities to each other.
- Non-repudiation: proof is needed that the message was indeed received.

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. 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, SET 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. Sensitive information has to be protected through at least three transactions:

- Credit card details supplied by the customer, either to the merchant or payment gateway. Handled by the server's SSL and the merchant/server's digital certificates.
- Credit card details passed to the bank for processing. Handled by the complex security measures of the payment gateway.
- Order and customer details supplied to the merchant, either directly or from the payment gateway/credit card processing company. Handled by SSL, server security, digital certificates (and payment gateway sometimes).

IV. PRACTICAL CONSEQUENCES

1. The merchant is always responsible for security of the Internet-connected PC where customer details are handled. Virus protection and a firewall are the minimum requirement. To be absolutely safe, store sensitive information and customer details on zip-disks, a physically separate PC or with a commercial file storage service. Always keep multiple back-ups of essential information, and ensure they are stored safely off-site.

2. Where customers order by email, information should be encrypted with PGP or similar software. Or payment should be made by specially **encrypted checks and ordering software**.

3. Where credit cards are taken online and processed later, it's the merchant's responsibility to check the security of the **hosting company**'s web server. Use a reputable company and demand detailed replies to your queries.

V. SECURITY THREATS TO E-COMMERCE

E-Commerce security requirements can be studied by examining the overall process, beginning with the consumer and ending with the commerce server. While telecommunications are certainly one of the major assets to be protected, the telecommunications links are not the only concern in computer and e-commerce security. For instance, if the telecommunications links were made secure but no security measures were implemented for either client computers or commerce and web-servers, then no communications security would exist at all.

Client threats: Until the introduction of executable web content, Web pages were mainly static.

Active content: Active content refers to programs that are embedded transparently in web pages and that cause action to occur. Active content is used in e-commerce to place items one wishes to purchase into a shopping cart and to compute the total invoice amount, including sales tax, handling, and shipping costs. Since active content modules are embedded in web pages, they can be completely transparent to anyone browsing a page containing them. Anyone can embed malicious active content in web pages. This delivery technique, called a *Trojan horse*, immediately begins executing and taking actions that cause harm. Embedding active content to web pages involved in e-commerce introduces several security risks. Malicious programs delivered quietly via web pages could reveal credit card numbers, usernames, and passwords that are frequently stored in special files called cookies. Cookies help to remembering customer order information or usernames or passwords. Malicious active content delivered by means of cookies can reveal the contents of client-side files or even destroy files stored on client computers.

Malicious codes: Computer viruses, worms and Trojan horses are examples of malicious code. A Trojan horse is a program which performs a useful function, but performs an unexpected action as well. Virus is a code segment which replicates by attaching copies to existing executables. A worm is a program which replicates itself and causes execution of the new copy. These can create havoc on the client side.

Server-side masquerading*:* Masquerading lures a victim into believing that the entity with which it is communicating is a different entity. For example, if a user tries to log into a computer across the internet but instead reaches another computer that claims to be the desired one, the user has been spoofed. This may be a passive attack (in which the user does not attempt to authenticate the recipient, but merely accesses it), but it is usually an active attack (in which the masquerader issues responses to mislead the user about its identity).

Communication channel threats: Messages on the internet travel a random path from a source node to a destination node through a number of intermediate computers on the network. It is impossible to guarantee that every computer on the internet through which messages pass is safe, secure, and non-hostile.

Confidentiality threats*:* Confidentiality is the prevention of unauthorized information disclosure.

Integrity threats: An integrity threat exists when an unauthorized party can alter a message stream of information.

Availability threats: The purpose of availability threats, also known as delay or denial threats, is to disrupt normal computer processing or to deny processing entirely.

Server threats: Servers have vulnerabilities that can be exploited by anyone determined to cause destruction or to illegally acquire information.

Database threats: E-commerce systems store user data and retrieve product information from databases connected to the web-server. Some databases store username/password pairs in a non-secure way. If someone obtains user authentication information, then he or she can masquerade as a legitimate database user and reveal private and costly information.

Common gateway interface threats: A common gateway interface (CGI) implements the transfer of information from a web-server to another program, such as a database program. CGI and the programs to which they transfer data provide active content to web pages.

Password hacking*:* The simplest attack against a password-based system is to guess passwords. Guessing of passwords requires that access to the complement, the complementation functions, and the authentication functions be obtained. If none of these have changed by the time the password is guessed, then the attacker can use the password to access the system.

VI. IMPLEMENTING SECURITY FOR E-COMMERCE

Let us now look at the fundamental strategic requirements an organization needs to consider if it wants to ensure that an e-commerce or online security project will be a success. Technology components of good online security, such as encrypted email, secure SSL websites, and intranets/extranets all have a role to play in protecting valuable data, but for security to be effective it must be designed as a whole and applied consistently across an organization and its IT infrastructure. To the designer, system security means: *under given assumptions about the system, no attack of a given form will destroy specified properties*.

Security requirements

During this phase, the security needs of an enterprise are identified. These needs are governed by the necessity to protect the following security attributes:

Authentication: This is the ability to say that an electronic communication (whether via email or web) does genuinely come from who it purports to. A trusted authority demands real-world proof of identity and checks its validity before issuing a digital certificate. Only certificates from trusted authorities will be automatically recognized and trusted by the major web browser and email client software.

Privacy: In online commerce, privacy is the ability to ensure that information is accessed and changed only by authorized parties.

Authorization: Authorization allows a person or computer system to determine if someone has the authority to request or approve an action or information.

Integrity: Integrity of information means ensuring that a communication received has not been altered or tampered with.

Non-repudiation: Non-repudiation is the ability to guarantee that once someone has requested a service or approved an action, they cannot turn around and say "I didn't do that!"

Security policy: An organization's security policy defines its position on the protection of its physical and IT assets.

VII. FUTURE RESEARCH

Most e-commerce transactions currently are secured by the SSL (secure sockets layer) protocol, which is designed to encrypt data exchanges over the internet. While SSL is generally viewed as effective, an increasing number of vulnerabilities and other issues have spurred some e-commerce players to think about more secure standards. E-Commerce is evolving toward using XML (Extensible Markup Language) technology, which not only will serve as the foundation of many web services, but also will secure transactions between machines, relying on complex trust hierarchies to do so.

VIII. CONCLUSION

Electronic commerce is growing rapidly. A number of technologies have converged to facilitate the proliferation of e-commerce. The rapid advances in computer technology coupled with rapid acceleration in communication networks and the development of sophisticated software have revolutionized the way business is done. However, this is not sufficient to proliferate e-commerce applications. With proper understanding of business needs and management of enterprise information security resources, e-commerce will mature profusely and will immensely benefit every individual. This work was partially supported by grants from the R&D in e-Commerce & Information Security Group, Department of Information Technology, Ministry of Communication and IT, Govt. of India.

REFERENCES:

1. A sengupta, C mazumdar,M s barik, e-Commerce security – A life cycle approach, Vol. 30, April/June 2005.
2. Robert Chesnut, The e-Commerce Safety Guide, www.paypal.com/security
3. http://www.sans.org/reading_room/whitepapers/ecommerce/information-security-issues-e-commerce_37
4. http://www.ecommerce-digest.com/ecommerce-security-issues.html
5. http://en.wikibooks.org/wiki/E-Commerce_and_E-Business/E-Commerce_in_Developing_Countries