Sādhanā Vol. 30, Parts 2 & 3, April/June 2005, pp. 119–140. © Printed in India

e-Commerce security – A life cycle approach

A SENGUPTA[1], C MAZUMDAR[1] and M S BARIK[2]

[1]Centre for Distributed Computing, Department of Computer Science and Engineering, Jadavpur University, Kolkata 700 032, Inida
[2]Department of Information Technology, Bengal Engineering and Science University, Shibpur 711 103, India
e-mail: sg_anirban@yahoo.co.in; chandanm@vsnl.com; mridul@it.becs.ac.in

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. This article examines the issues related to the security of the assets and transactions in the e-commerce components and activities. Since large public money is involved in the transactions, the role of information security and privacy is not exaggerated in this kind of business. After examining the technologies used in e-commerce, the article goes on to identify the security requirement of e-commerce systems from perceived threats and vulnerabilities. Then e-commerce security is viewed as an engineering management problem and a life cycle approach is put forward. How the e-commerce systems can be made secure using the life cycle approach is outlined. The relevant standards and laws are also discussed in the perspective of e-commerce. The article closes with some future research directions and conclusions.

Keywords. e-Commerce security; threats and vulnerabilities; security engineering life cycle; security standards; IT act.

1. Introduction to e-commerce

To many people, the term *electronic commerce* (sometimes shortened to *e-commerce*) (Kalakota & Whinston 1999) means shopping in the part of the internet called the World Wide Web. However, e-commerce has a much broader scope and encompasses many more business activities other than just web shopping. Some people and businesses use the term electronic business (or e-business) when they are talking about e-commerce in this broader sense. In this paper, we will use the term e-commerce in its broadest definition.

Although the web has made online shopping possible for many businesses and individuals, in a broader sense, e-commerce has existed for many years. For decades, banks have been

A glossary of technical terms in e-commerce is given at the end of the paper

using electronic funds transfers (EFTs) (Schneider & Perry 2001), which are electronic transmissions of account exchange information over private communications networks.

Businesses also have been engaging in a form of e-commerce, known as electronic data interchange (EDI), for many years. EDI occurs when one business transmits computer-readable data in standard format to another business. In the 1960s, businesses realized that many of the documents they exchanged related to the shipping of goods – such as invoices, purchase orders, and bills of lading – and included the same set of information for almost every transaction. They also realized that they were spending a good deal of time and money entering these data into their computers, printing paper forms, and then re-entering the data on the other side of the transaction. Although the purchase order, invoice, and bill of lading for each transaction contained much of the same information, each paper form had its own unique format for presenting that information. By creating a set of standard formats for transmitting that information electronically, businesses were able to reduce errors, avoid printing and mailing costs, and eliminate the need to re-enter data. Businesses that engage in EDI with each other are called *trading partners*. The standard formats used in EDI contain the same information that businesses have always included in their standard paper invoices, purchase orders, and shipping documents.

A good definition of e-commerce would mention the use of electronic data transmission to implement or enhance any business process. Some people use the term "internet commerce" to mean e-commerce that specifically uses the internet or the web as its data transmission medium. IBM has defined electronic business to be "the transformation of key business processes through the use of Internet technologies".

1.1 *Advantages of e-commerce*

The advantages of e-commerce for business entities can be summarized thus: *e-commerce can increase sales and decrease costs*. A firm can use e-commerce to reach narrow market segments that are widely scattered geographically. The internet and the web are particularly useful in creating virtual communities that become ideal target markets. A virtual community is a gathering of people who share a common interest, but, instead of this gathering occurring in the physical world, it takes place on the internet.

Just as e-commerce increases sales opportunities for the seller, it increases purchasing opportunities for the buyer. Businesses can use e-commerce in their purchasing processes to identify new suppliers and business partners. Negotiating price and delivery terms is easier in e-commerce, because the web can provide competitive bid information very efficiently. e-Commerce increases the speed and accuracy with which businesses can exchange information, which reduces costs on both sides of transactions.

e-Commerce provides buyers with a wider range of choices than traditional commerce, because they can consider many different products and services from a wider variety of sellers. The benefits of e-commerce also extend to the general welfare of society. Electronic payments of tax refunds, public retirement, and welfare support cost less to issue and arrive securely and quickly when transmitted via the Internet. Furthermore, electronic payments can be easier to audit and monitor than payments made by check, which can help protect against fraud and theft losses. e-Commerce can make products and services available in remote areas. For example, distance education is making it possible for people to learn skills and earn degrees no matter where they live or what hours of the day they have available for study.

1.2 *Disadvantages of e-commerce*

e-Commerce also has its disadvantages. It is difficult to conduct a few businesses electronically. For example, perishable foods and high-cost items such as jewellery or antiques may be impossible to adequately inspect from a remote location, regardless of the technologies that are devised in the future. However, most of the disadvantages of e-commerce today are due to the newness and rapidly developing pace of the underlying technologies.

Return on investment numbers is difficult to compute for investments in e-commerce, because the costs and benefits are hard to quantify. Costs, which are a function of technology, can change dramatically during even short-lived e-commerce implementation projects, because the underlying technologies change rapidly.

In addition to technology issues, many businesses face cultural and legal impediments to e-commerce. Some consumers are still somewhat fearful of sending their credit card numbers over the Internet. The legal environment in which e-commerce is conducted is full of unclear and conflicting laws. In many cases, government regulators have not kept up with technologies. As more businesses and individuals find the benefits of e-commerce compelling, many of these technology- and culture-related disadvantages will disappear.

Another important issue is security. Transactions between buyers and sellers in e-commerce include requests for information, quotation of prices, placement of orders and payment, and after sales services. The high degree of confidence needed in the authenticity, confidentiality, and timely delivery of such transactions can be difficult to maintain where they are exchanged over the Internet. The interception of transactions, and in particular credit card details, during transmission over the Internet is often a major obstacle to public confidence in e-commerce.

2. e-Commerce technologies

Several technologies are needed for e-commerce to exist. The most obvious one is the internet. Beyond that system of interconnected networks, many other sophisticated software and hardware components are needed to provide the required support structure: database software, network switches and hubs, encryption hardware and software, multimedia support, and the world wide web. Methods of connecting all the software and hardware elements in just the right way to support electronic commerce are changing and evolving everyday. The rate of change is rapid for all elements that support electronic commerce. Any business that engages in e-commerce and hopes to compete in the future must adapt to new internet technologies as they become available. The anticipated e-commerce overload requires companies to find faster and more efficient ways to deal with the ever-increasing rush of online shoppers and the increasing traffic between businesses.

2.1 *Characteristics of e-commerce technologies*

The following are the characteristics of e-commerce technologies (Burns 2002):

2.1a *Ease of automated processing:* A payer can now easily automate the generation and processing of multiple payments with minimal effort and cost. Previously, the dependency upon banks to handle most payments and the lack of a cheap, ubiquitous communications technology made automation of payment processes expensive and difficult to establish.

2.1b *Immediacy of result:* Payment immediacy occurs because of automation and the ability of the intermediate systems and providers to process payments in real-time. In manual, paper-based systems there exists a time delay due to the requirement of human intervention in the process.

2.1c *Openness and accessibility:* The availability of cheap computing and communications technology, and appropriate software enables small enterprises and individuals to access or provide a range of payment services that were previously only available to large organizations via dedicated networks or the transactional processing units of banks.

2.1d *Loss of collateral information:* The new technology dispenses with, or alters, collateral information accompanying transactions. This information has traditionally been part of the transaction, and has been relied upon by the transacting parties to validate individual payments. Collateral information can be defined as information:

- which is not essential to the meaning and intent of a transaction
- which is typically incidental to the nature of the communications channel over which the transaction is conducted; but nevertheless
- provides useful contextual information for one or more of the parties to the transaction.

Collateral information can include many things ranging from tone of voice in a telephone call to the business cards and letterheads and apparent authority of the person with whom the firm is dealing. Since information is received only via a single channel (such as an electronic message) in electronic systems, new processes are needed to support and reinforce payments in the same way as manual systems.

2.1e *Globalization:* Globalization, or the minimization of geographical factors in making payments, is an obvious aspect of the new payments systems. Its effect is upon areas such as size of the payments marketplace, uncertainty as to legal jurisdiction in the event of disputes, location and availability of transaction trails, and the ability of a payment scheme to rapidly adapt to regulatory regimes imposed by one country by moving to another.

2.1f *New business models:* New business models are being developed to exploit the new payment technologies, in particular to address or take advantage of the disintermediation of customers from traditional payment providers such as banks. Disintermediation is where the technology enables a third party to intervene between the customer and the banking system, effectively transferring the customer's trusted relationship with the bank to the new party.

3. Security threats to e-commerce – Requirements definition

e-Commerce security requirements can be studied by examining the overall process, beginning with the consumer and ending with the commerce server. Considering each logical link in the "commerce chain", the assets that must be protected to ensure secure e-commerce include client computers, the messages travelling on the communication channel, and the web and commerce servers – including any hardware attached to the servers. 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.

3.1 *Client threats*

Until the introduction of executable web content, Web pages were mainly static. Coded in HTML, static pages could do little more than display content and provide links to related pages with additional information. However, the widespread use of active content has changed this perception.

3.1a *Active content:* Active content refers to programs that are embedded transparently in web pages and that cause action to occur. Active content can display moving graphics, download and play audio, or implement web-based spreadsheet programs. 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. The best known active content forms are Java applets, ActiveX controls, JavaScript, and VBScript.

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. Because the internet is stateless and cannot remember a response from one web page view to another, cookies help solve the problem of 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.

3.1b *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.

3.1c *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).

3.2 *Communication channel threats*

The internet serves as the electronic chain linking a consumer (client) to an e-commerce resource (commerce server). Messages on the internet travel a random path from a source node to a destination node. The message passes through a number of intermediate computers on the network before reaching the final destination. It is impossible to guarantee that every computer on the internet through which messages pass is safe, secure, and non-hostile.

3.2a *Confidentiality threats:* Confidentiality is the prevention of unauthorized information disclosure. Breaching confidentiality on the internet is not difficult. Suppose one logs onto a website – say www.anybiz.com – that contains a form with text boxes for name, address, and e-mail address. When one fills out those text boxes and clicks the submit button, the

information is sent to the web-server for processing. One popular method of transmitting data to a web-server is to collect the text box responses and place them at the end of the target server's URL. The captured data and the HTTP request to send the data to the server is then sent. Now, suppose the user changes his mind, decides not to wait for a response from the anybiz.com server, and jumps to another website instead – say www.somecompany.com. The server somecompany.com may choose to collect web demographics and log the URL from which the user just came (www.anybiz.com). By doing this, somecompany.com has breached confidentiality by recording the secret information the user has just entered.

3.2b *Integrity threats:* An integrity threat exists when an unauthorized party can alter a message stream of information. Unprotected banking transactions are subject to integrity violations. Cyber vandalism is an example of an integrity violation. Cyber vandalism is the electronic defacing of an existing website page. Masquerading or spoofing – pretending to be someone you are not or representing a website as an original when it really is a fake – is one means of creating havoc on websites. Using a security hole in a domain name server (DNS), perpetrators can substitute the address of their website in place of the real one to spoof website visitors. Integrity threats can alter vital financial, medical, or military information. It can have very serious consequences for businesses and people.

3.2c *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. For example, if the processing speed of a single ATM machine transaction slows from one or two seconds to 30 seconds, users will abandon ATM machines entirely. Similarly, slowing any internet service will drive customers to competitors' web or commerce sites.

3.3 *Server threats*

The server is the third link in the client-internet-server trio embodying the e-commerce path between the user and a commerce server. Servers have vulnerabilities that can be exploited by anyone determined to cause destruction or to illegally acquire information.

3.3a *Web-server threats:* Web-server software is designed to deliver web pages by responding to HTTP requests. While web-server software is not inherently high-risk, it has been designed with web service and convenience as the main design goal. The more complex the software is, the higher the probability that it contains coding errors (bugs) and security holes – security weaknesses that provide openings through which evildoers can enter.

3.3b *Commerce server threats:* The commerce server, along with the web-server, responds to requests from web browsers through the HTTP protocol and CGI scripts. Several pieces of software comprise the commerce server software suite, including an FTP server, a mail server, a remote login server, and operating systems on host machines. Each of this software can have security holes and bugs.

3.3c *Database threats:* E-commerce systems store user data and retrieve product information from databases connected to the web-server. Besides product information, databases connected to the web contain valuable and private information that could irreparably damage a company if it were disclosed or altered. 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.

3.3d *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. Because CGIs are programs, they present a security threat if misused. Just like web-servers, CGI scripts can be set up to run with their privileges set to high – unconstrained. Defective or malicious CGIs with free access to system resources are capable of disabling the system, calling privileged (and dangerous) base system programs that delete files, or viewing confidential customer information, including usernames and passwords.

3.3e *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.

4. Implementing security for e-commerce (lifecycle approach)

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.

There is a subtle difference in the design of a software system and that of a security system. While designing softwares, the functional correctness of applications is the prime concern. In fact, in software systems, the designer aims at ensuring that for reasonable input, the user gets reasonable output. This can be traced from the system specification. But in the case of security systems, the designer has to ensure that the system properties are preserved in the face of attack. Thus the system outputs should not be completely disastrous for unreasonable inputs. In security systems, there definitely can be active interference from the adversary and the system should be hardened to withstand that. Moreover, in security systems, more functionality implies more complex system and more security holes in the system.

The steps to design security of a system is to model the system, identify the security properties to be preserved, model the adversary, and then ensure that the security properties are preserved under attacks. Detail modelling of the system and identification of the required security properties are possible. But it almost impossible to accurately model the adversaries and vulnerabilities of the system exploited by those advera\saries. The result is that there nothing called “absolute security”. Thus to the designer, system security means: *under given assumptions about the system, no attack of a given form will destroy specified properties*.

Thus system security in general and e-commerce security in particular is conceived of a *process* rather than a one-time developed *product*.

4.1 *Security engineering life cycle*

It is important to note that the e-commerce security need of an enterprise is dynamic rather than static and depends on the operational dynamics, shift or addition to business goals, technological advancement etc. Thereby, the process of designing and deploying an information security infrastructure is a continuous process of analysis, design, monitoring, and adaptation to changing needs. Often, the change in needs is frequent in the organizations. In order to

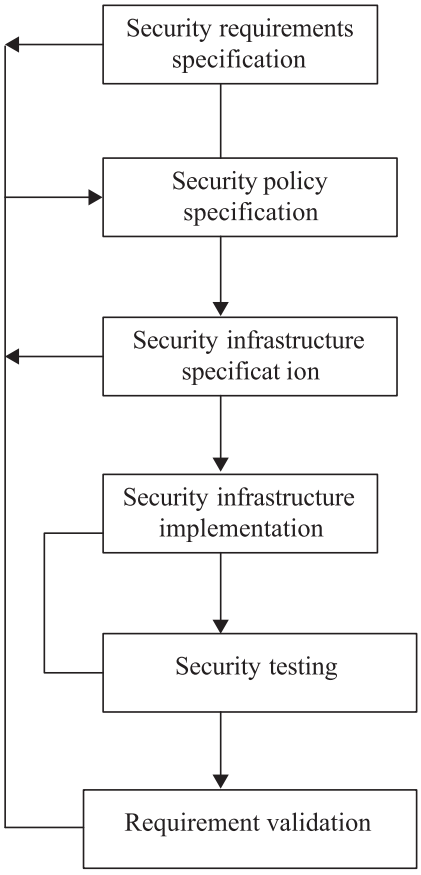

Figure 1. Security engineering life cycle.

be survivable under such frequent changes, the process has to be developed from a life-cycle approach. This observation leads to the concept of "security engineering life-cycle" (Mazumdar *et al* 2003). The security engineering life cycle consists of the following phases (figure 1):

4.1a *Security requirement specification and risk analysis:* This is the first phase in the security engineering life cycle. It collects information regarding assets of the organization that need to be protected, threat perception on those assets, associated access control policies, existing operational infrastructure, connectivity aspects, services required to access the asset and the access control mechanism for the services.

4.1b *Security policy specification:* This phase uses "security requirement specification" and "risk analysis report" as input and generates a set of e-commerce security policies. The policy statements are high-level rule-based and generic in nature, and, thereby, does not provide any insight to system implementation or equipment configuration.

4.1c *Security infrastructure specification:* This phase analyses the "security requirement specification" and the "security policy specification" to generate a list of security tools that are needed to protect the assets. It also provides views on the location and purpose of the security tools.

4.1d *Security infrastructure implementation:* The organization, in this phase, procures, deploys, and configures the selected security infrastructure at the system level.

4.1e *Security testing:* In this phase, several tests are carried out to test the effectiveness of the security infrastructure, functionality of the access control mechanism, specified operational context, existence of known vulnerabilities in the infrastructure etc.

4.1f *Requirement validation:* This phase analyses the extent of fulfillment of the security requirements of the e-commerce organization by the corresponding security policy and the implemented security infrastructure. Change in the business goal, operational environment, and technological advancement may lead to a fresh set of security requirements and thereby, triggering a new cycle of the "security engineering life cycle".

Now, let us see the Security Requirements, Security Policy, Security Infrastructure, and Security Testing phases in greater detail.

4.2 *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:

4.2a *Authentication:* This is the ability to say that an electronic communication (whether via email or web) does genuinely come from who it purports to. Without face-to-face contact, passing oneself off as someone else is not difficult on the internet. Forging the "From:" field in an email header is a trivial matter, and far more sophisticated attacks are standard fare for hackers.

In online commerce the best defence against being misled by an imposter is provided by unforgeable digital certificates from a trusted authority (such as VeriSign). Although anyone can generate digital certificates for themselves, 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.

Authentication can be provided in some situations by physical tokens (such as a drivers license), by a piece of information known only to the person involved (eg. a PIN), or by a physical property of a person (fingerprints or retina scans). Strong authentication requires at least two or more of these. A digital certificate provides strong authentication as it is a unique token (the certificate itself) and requires a password (something known only to the owner) for its usage.

4.2b *Privacy:* In online commerce, privacy is the ability to ensure that information is accessed and changed only by authorized parties. Typically this is achieved via encryption. Sensitive data (such as credit card details, health records, sales figures etc.) are encrypted before being transmitted across the open internet – via email or the web. Data which has been protected with strong 128-bit encryption may be intercepted by hackers, but cannot be decrypted by them within a short time. Again, digital certificates are used here to encrypt email or establish a secure HTTPS connection with a web-server. For extra security, data can also be stored long-term in an encrypted format.

4.2c *Authorization:* Authorization allows a person or computer system to determine if someone has the authority to request or approve an action or information. In the physical

world, authentication is usually achieved by forms requiring signatures, or locks where only authorized individuals hold the keys.

Authorization is tied with *authentication*. If a system can securely verify that a request for information (such as a web page) or a service (such as a purchase requisition) has come from a known individual, the system can then check against its internal rules to see if that person has sufficient authority for the request to proceed.

In the online world, authorization can be achieved by a manager sending a digitally signed email (an email stamped by their personal digital certificate). Such an email, once checked and verified by the recipient, is a legally binding request for a service. Similarly, if a web-server has a restricted access area, the server can request a digital certificate from the user's browser to identify the user and then determine if they should be given access to the information according to the server's permission rules.

4.2d *Integrity:* Integrity of information means ensuring that a communication received has not been altered or tampered with. Traditionally, this problem has been dealt with by having tight control over access to paper documents and requiring authorized officers to initial all changes made – a system with obvious drawbacks and limitations. If someone is receiving sensitive information online, he not only wants to ensure that it is coming from who he expects it to (authentication), but also that it hasn't been intercepted by a hacker while in transit and its contents altered. The speed and distances involved in online communications requires a very different approach to this problem from traditional methods.

One solution is afforded by using digital certificates to digitally "sign" messages. A travelling employee can send production orders with integrity to the central office by using their digital certificate to sign their email. The signature includes a hash of the original message – a brief numerical representation of the message content. When the recipient opens the message, his email software will automatically create a new hash of the message and compare it against the one included in the digital signature. If even a single character has been altered in the message, the two hashes will differ and the software will alert the recipient that the email has been tampered with during transit.

4.2e *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!". Non-repudiation allows one to legally prove that a person has sent a specific email or made a purchase approval from a website. Traditionally non-repudiation has been achieved by having parties sign contracts and then have the contracts notarized by trusted third parties. Sending documents involved the use of registered mail, and postmarks and signatures to date-stamp and record the process of transmission and acceptance. In the realm of e-commerce, non-repudiation is achieved by using digital signatures. Digital signatures which have been issued by a trusted authority (such as VeriSign) cannot be forged and their validity can be checked with any major email or web browser software. A digital signature is only installed in the personal computer of its owner, who is usually required to provide a password to make use of the digital signature to encrypt or digitally sign their communications. If a company receives a purchase order via email which has been digitally signed, it has the same legal assurances as on receipt of a physical signed contract.

4.3 *Security policy*

The first step in securing an e-commerce venture is to formulate written security policies (website 1) which clearly define the requirements for each component of the system (human,

technological, legal) and how they interact. An organization's security policy defines its position on the protection of its physical and IT assets. It identifies the physical and intellectual property assets that are most valuable for the continued success of the company, and specifies how they should be protected.

The security policy may cover issues like:

- What service types (e.g., web, FTP, SMTP) users may have access to
- What classes of information exist within the organization and which should be encrypted before being transmitted
- What client data does the organization hold. How sensitive is it? How is it to be protected?
- What class of employees may have remote access to the corporate network
- Roles and responsibilities of managers and employees in implementing the security policy
- How security breaches are to be responded to

The security policy should also consider physical aspects of network security. For example,

- Who has access to the corporate server?
- Is it in a locked environment or kept in an open office?
- What is the procedure for determining who should be given access?

The security policy regulates the activities of employees just as much as it defines how IT infrastructure will be configured. The policy should include details on how it is to be enforced and how individual responsibilities are determined.

For it to be effective, the policy needs regular testing and review to judge the security measures. The review process needs to take into account any changes in technology or business practices which may have an influence upon security. Lastly, the policy itself needs to be regarded as a living document which will be updated at set intervals to reflect the evolving ways in which the business, customers and technology interact.

4.4 *Security infrastructure*

The security infrastructure (website 1) is the implementation of the security policy. The security infrastructure is the technology which is chosen to secure the e-business and the rules by which it operates. Some examples of this include:

- enforcing password aging and expiration
- enforcing the complexity of passwords
- blocking prohibited outbound connections from the firewall
- requiring digital certificates to authenticate remote access connections to an organization's network
- requiring badges for physical access to building
- requiring all physical access to servers to be recorded in a written log

Again, the security infrastructure entails managing the behavior of both IT and human resources. It should be regularly policed:

- Who checks written logs?
- How often are firewall reports checked?

Finally, it must be enforced. The penalties for breaches of the security policy must be made clear to all employees and partners and must be enforced if policy requirements are broken or ignored.

4.5 *Testing e-commerce security*

The need for security testing of an organization arises due to two main factors. The primary factor is the importance of measuring the extent to which the security infrastructure implements the security policy and the security requirements of an organization. As the implementation of the security infrastructure needs human interventions, a proper security testing is needed to check out the existence of any "human error". The other factor is the vulnerability of the existing security infrastructure to the new threats and exploits. In recent years, the rate of arrival of new types of threat and new exploits has been alarming with respect to the information security context. This leads to the need for periodical security testing by which the vulnerability of the existing security infrastructure to the growing number of threats and exploits can be measured.

The main objective of security testing, therefore, includes

- Verification of the security requirement specification such as location of the asset(s), access control mechanism for the assets, operational context of the organization, existing system services and their access control mechanisms, and the connectivity within the organization and connectivity of the organization to the outside world
- Verification of the configuration of the security tools specified in the security infrastructure i.e. whether the security tools are properly installed and configured to maintain the security of the asset
- Verification of any gap between the proposed security infrastructure and the implemented security infrastructure
- Verification of the limitation of the proposed security infrastructure with respect to the known vulnerabilities

Thus, there are two aspects of testing – compliance checking and penetration testing.

4.5a *Compliance checking:* In compliance checking, it is seen whether the security infrastructure, that has been implemented, matches the security policy of the organization. A semi-automated tool can be used to match the policies with the existing infrastructure.

4.5b *Penetration testing:* In penetration testing, it is seen whether the existing security infrastructure of the organization is sufficient to ward off all possible security threats. Various automated and semi-automated security tools like Retina, Nessus etc. are available for penetration testing. They try and penetrate the organization's network and generate a report on the vulnerabilities and threats that are present in the network.

The feedback from the testing phase is used to upgrade the security infrastructure and security policy of the organization. After that, the testing is carried out again. Thus, security engineering is an iterative and dynamic process where all the phases need to be carried out at regular intervals to ensure the security of an organization.

5. Compliance and legal aspects

Now let us consider certain aspects dealing with adherence to standards and legal obligations.

5.1 *The standards*

There are various standards pertaining to the security aspects of enterprises. Some of them are ISO 17799 (Information technology – Code of practice for information security management)

(ISO/IEC 2000), SSE-CMM (Systems security engineering – Capability maturity model) (SSE-CMM 2003) and COBIT (Control objectives for information and related technology) (COBIT 2000). ISO 17799 provides detailed guidelines on how a management framework for enterprise security should be implemented. It conceives ten security domains. Under each domain there are certain security objectives to be fulfilled. Each objective can be attained by a number of controls. The controls may prescribe management measures like guidelines and procedures, or some security infrastructure in the form of tools and techniques. It details various methods that can be followed by enterprises to meet security needs for e-commerce. It talks about the need for security policies, security infrastructure, and continuous testing in the same manner as has been detailed above.

The main objective of the COBIT is the development of clear policies and good practices for security and control in IT for worldwide endorsement by commercial, governmental and professional organizations. The SSE-CMM is a process reference model. It is focused upon the requirements for implementing security in a system or series of related systems that are in the Information Technology Security domain.

5.2 *Legal and contractual aspects – international scenario*

The legal and regulatory framework (websites 2, 3) for international e-commerce is an area of wide debate and covers wide areas such as taxation, consumer protection and jurisdiction. However, many legal and regulatory issues are directly related to the security aspects of e-commerce and are illustrated in table 1 below:

Table 1. Legal issues and their impact on business.

Issues	Business impact
The European Union Directive on Data Protection of 1995 requires member states to enact new measures to ensure that personal information held on information systems is adequately protected. One of the key measures introduced is a restriction on the export of personal data to countries that do not have comparable legislation in place (see information privacy) This has a bearing on e-commerce applications that involve cross-border transfer of personal information	Additional costs involved in complying with data protection legislation Possible restrictions in scope of e-commerce applications Legal action following breaches of the EU Directive
The legal recognition of electronic documents as substitutes for paper equivalents varies from country to country. In some cases certain types of document have to exist in paper form to have legal validity. Similarly, electronic (or digital) signatures used to prove the authenticity of electronic transactions have varying legal acceptability in different jurisdictions	Lack of legal recourse in the event of a dispute
Some security solutions for e-commerce rest heavily on cryptographic products. These products are subject to restrictions on export, import or use in some countries because of their potential military or criminal application. However, the situation with cryptography is changing and moves are being made in some countries to relax controls	Restrictions on an organization's freedom to employ the desired level of protection leading to unacceptable business exposures

The legislative and regulatory regime is undergoing rapid change in response to the development of e-commerce. However, some countries react more quickly and thus incompatibilities arise, particularly affecting cross-border e-commerce. Organizations should monitor this area carefully to enable them to adapt their e-commerce strategies appropriately.

5.3 *Indian IT Act 2000*

The Indian (Duggal 2000; website 4) was enacted on 7th June 2000 and was notified in the official gazette on 17th October 2000. It aims to provide a legal and regulatory framework for promotion of e-commerce and e-governance. It is applicable to the whole of India. Some of the major provisions contained in the IT Act 2000 are as follows:

- Electronic contracts will be legally valid
- Legal recognition of digital signatures
- Security procedure for electronic records and digital signature
- Appointment of certifying authorities and controller of certifying authorities, including recognition of foreign certifying authorities
- Various types of computer crimes defined and stringent penalties provided under the Act
- Establishment of Cyber Appellate Tribunal under the Act
- Act to apply for offences or contraventions committed outside India
- Power of police officers and other officers to enter into any public place and search and arrest without warrant
- Constitution of Cyber Regulations Advisory Committee who will advise the Central Government and Controller

However, there are a few more areas which should be taken care of in the subsequent amendments to the IT Act. These are as follows:

- Electronic fund transfer – Electronic payment system
- Digital copyright
- Taxation – Income tax, sales tax
- Consumer protection
- Sale or the conveyance of immovable property

6. 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.

SSL's foremost drawback is its reliance on certificate authentication at the user end, which requires users to have at least a basic understanding of the technology and processes involved in ensuring security. The same weakness is responsible for the demise of PKI (public key infrastructure) security; browser vulnerabilities and user ignorance often result in unsecured

Table 2. Classes of mobile commerce applications.

Class of wireless applications	Examples
Mobile inventory management	Tracking the location of goods and services, such as boxes, packets, troops, or cattle
Product location	Locating certain items, such as TVs, VCRs, or cars
Proactive service management	Transmitting information about aging components, such as automobile parts, to vendors
Wireless re-engineering	Improving business services, such as claim adjustments or insurance
Mobile auction and reverse auction	Offering, selling, and bidding
Mobile entertainment services	Providing services such as video on demand
Mobile office	Providing services for business people, such as traffic jam reports, airport and flight information, and procurement of products and services
Mobile distance education	Offering classes using streaming audio and video
Wireless data centre	Providing downloadable information from data warehouses
Mobile music and music on demand	Allowing downloading and storing of music from the Internet

transactions. The latest version of SSL, known as TLS (Transaction Level Security) (website 5), has not taken hold as widely as its predecessor. Instead, analysts predict that XML will serve as the basis for the next phase of secure e-commerce transactions.

XML security, although it will retain the issue of trusting signers, will deal with transactions as if they were documents, allowing companies to send purchase orders and checks via e-mail. The need for complex XML security technology will arise in the future.

The next phase of electronic business growth will be in wireless and mobile commerce (Varshney *et al* 2000). Some of the emerging classes of mobile commerce applications are listed in table 2 below.

Non-repudiation of service is an essential feature of e-commerce security service to establish the legal basis of an electronic transaction. The dynamic aspects of e-commerce, such as cancelling and refunding payment, or changing payment methods, can give rise to disputes among participants. Today, only a few frameworks address non-repudiation of service; also, these frameworks address partial non-repudiation of service. Research is underway to define new frameworks for non-repudiation.

IT security is in its awkward adolescence. Some parts are mature, some are in their infancy. Everything else is somewhere in-between.

7. 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. Proper management of enterprise information security resources is the need of the hour. We have, in this paper, put forth a "security engineering life cycle" approach to manage the information resources of an enterprise so that e-business can be carried out securely. 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.

Glossary of security terms

Access control: Access control refers to the rules and deployment mechanisms which control access to information systems, and physical access to premises.

Access control list: An access control list (ACL) is a file which a computer's operating system uses to determine users' individual access rights and privileges to folders/directories and files on a given system.

Anti-virus program: Software designed to detect, and potentially eliminate, viruses before they have had a chance to wreak havoc within the system, as well as repairing or quarantining files which have already been infected by virus activity.

Application service provider (ASP): An ASP rents software to users and provides access over the Internet, instead of selling it outright.

Active server pages: Active server pages are web pages (HTML pages), embedded within which, are (small) programs or scripts that run just before the page is delivered to the user.

Audit log: Computer files containing details of amendments to records, which may be used in the event of system recovery being required.

Authentication: This refers to the verification of the authenticity of either a person or of data.

Authorization: The process whereby a person approves a specific event or action.

Availability: Ensuring that information systems and necessary data are available for use when they are needed.

Back door: This is the name given to a 'secret' access route into the system. Such routes are usually undocumented and are not originally specified.

Biometric access controls: Security access control systems which authenticate (verify the identity of) users by means of physical characteristics, e.g. face, fingerprints, voice or retinal pattern.

BS 7799: British Standard for Information Security which was re-issued in 1999 in two parts. Part 1 is the code of practice for Information Security Management and Part 2 specifies the requirements for implementing information security in compliance with the code of practice. In October 2000, BS 7799 was elevated to being a standard of the international standards organization (ISO) standard – ISO 17799.

Buffer overflow attacks: This is type of DoS attack whereby data are sent to the server at a rate and volume that exceeds the capacity of the system, causing errors.

Bug: A fault in a computer system, usually associated with software.

Business continuity plan (BCP): This is a plan to ensure that the essential business functions of the organization are able to continue (or re-start) in the event of unforeseen circumstances; normally a disaster of some sort.

Certification authority: A trusted third party clearing house that issues digital certificates and digital signatures. Such certificates include an organization's name, a serial number, an expiry date. In addition, to allow for the encryption and decryption of data, the public key of the organization is also included. Finally, the digital signature of the certificate-issuing authority is included so that a recipient can verify that the certificate is valid. The following companies provide various levels of certification services for organizations and individuals, like VeriSign, Entrust, Baltimore Technologies and Thawte.

Cipher: A cipher is the generic term used to describe a means of encrypting data. In addition, the term *cipher* can refer to the encrypted text itself.

Common gateway interface (CGI): CGI is a programming method of passing information between a website and an applications program and vice versa. There are significant security risks in implementing CGI scripts using scripting languages such as Perl.

Computer viruses: These are pieces of programming code which have been purposely written to inflict an unexpected result upon some other program. There are now approximately 50,000 viruses and their variants for which known cures of 'vaccines' are available. Viruses are transmitted within other (seemingly) legitimate files or programs, the opening or execution of which causes the virus to run and to replicate itself within a computer system, as well as performing some sort of detrimental action.

Confidentiality: Assurance that information is shared only among authorized persons or organizations. Breaches of confidentiality can occur when data are not handled in a manner adequate to safeguard the confidentiality of the information concerned.

Controls: Procedures that can reduce, or eliminate, the risk of a threat becoming an incident.

Cookie: A small identifier file placed on a user's computer by a website, which logs information about the user and their previous/current visits for the use of the site next time the user makes contact. The website owners claim that this is beneficial to the user, allowing faster access, and 'personalization' of the site for that user.

Cracker: This is either a piece of software (program) whose purpose is to 'crack' the code to, say a password, or refers to a person who attempts to gain unauthorised access to a computer system.

Cryptography: The subject of cryptography is primarily concerned with maintaining the privacy of communications.

Cyber crime: Cyber crime is any criminal activity which uses network access to commit a criminal act.

Data/information: In the area of information security, data (and the individual elements that comprise the data) when processed, formatted and re-presented, gains meaning and thereby become information.

Decryption: The process by which encrypted data is restored to its original form in order to be understood/usable by another computer or person.

Denial of service: Denial of service (DoS) is an action against a service provider over the internet whereby a client is denied the level of service expected. DoS attacks do not usually have theft or corruption of data as their primary motive.

DES/AES: DES – Data Encryption Standard, and AES – Advanced Encryption Standard are both data encryption standards for the scrambling of data to protect confidentiality.

Digital certificate: A digital certificate is the electronic version of an ID card that establishes a person's credentials and authenticates a connection when performing e-commerce transactions over the internet, using the web.

Digital signature: A digital signature is an electronic equivalent of an individual's signature. It authenticates the message to which it is attached and validates the authenticity of the sender. In addition, it also provides confirmation that the contents of the message to which it is attached, have not been tampered with, en route from the sender to the receiver.

Digital watermark: A unique identifier that becomes part of a digital document and cannot be removed. The watermark is invisible to the human eye but a computer can analyze the document and extract the hidden data.

DMZ: A DMZ or de-militarized zone, is a separate network added between a protected network and an external network, in order to provide an additional layer of security.

DNS: Domain name system (or server). The DNS is the means by which user-friendly web addresses are translated into arcane IP addresses. The DNS ensures that messages are routed to the correct site.

Eavesdropping: Listening to someone else's conversation.

e-Business: Another term for e-commerce.

e-Commerce: e-commerce, e-business or e-tailing are electronic transactions, performed over the internet – and usually via the web - in which the parties to the transaction agree, confirm and initiate both payment and goods transfer.

Encryption: The process by which data are temporarily re-arranged into an unreadable or unintelligible form for confidentiality, transmission, or other security purposes.

e-Trading: e-Trading is that part of e-commerce which specializes in financial services. It deals in corporate paper (e.g. stocks and shares), purchase of commodities, currencies etc. It can be business-to-consumer or business-to-business.

Extranet: An extranet is a private network which uses the internet protocols and extends beyond an organization's premises, typically to allow access by clients, suppliers, or selected third parties.

Firewalls: Firewalls are security devices used to restrict access between two communication networks.

Guideline: Guidelines are more general statements designed to achieve the policy's objectives by providing a framework within which to implement procedures. Where standards are mandatory, guidelines are recommendations.

Hacker: An individual whose primary aim is to penetrate the security defenses of large, sophisticated, computer systems.

HTTP: This protocol, the Hyper Text Transfer Protocol, is used for the transmission of information, graphics, sounds and animation between a client web browser and the web-server.

HTTPS and SSL: The Secure Hyper Text Transfer Protocol uses HTTP but additionally activates web-server security, in the form of Secure Sockets Layer (SSL). This means that the communications between the client and the (host) web-server are encrypted and, additionally, that the host web-server may be validated by the client using a digital certificate on the server.

Information asset: An information asset is a definable piece of information, stored in any manner which is recognized as 'valuable' to the organization.

Integrity: Assurance that the information is authentic and complete. Ensuring that information can be relied upon to be sufficiently accurate for its purpose.

International organization for standardization (ISO): This is a group of bodies from approximately 130 countries whose aim is to establish, promote and manage standards to facilitate the international exchange of goods and services.

Internet: A publicly accessible wide area network that can be employed for communication between computers.

Internet service provider (ISP): An internet service provider – commonly referred to as an 'ISP' – is a company which provides individuals and organizations with access to the internet, plus a range of standard services such as e-mail and the hosting (running) of personal and corporate websites.

Intranet: A local area network within an organization, which is designed to look like, and work in the same way as, the internet. Intranets are essentially private networks, and are not accessible to the public.

Intrusion: An uninvited entry into a system by an unauthorized source.

Intrusion detection system (IDS): Intrusion detection systems are complex software applications, which monitor network activity.

Logic bomb: A logic bomb is a piece of program code buried within another program, designed to perform some malicious act.

Malicious code: Malicious code includes all and any programs (including macros and scripts) which are deliberately coded in order to cause an unexpected (and usually, unwanted) event on a computer system.

Masquerading: Identifying yourself as someone else, i.e. purporting to be another (probably genuine) user for example, sending an e-mail to a client under someone else's name.

Non disclosure agreement (NDA): A non disclosure agreement (NDA) is a legally binding document which protects the confidentiality of ideas, designs, plans, concepts or other commercial material.

Non-repudiation: It ensures that neither the sender nor the receiver of a message are able to deny the transmission.

Patch: A patch is a temporary arrangement used to overcome software problems or glitches. A patch will normally be released as a 'quick fix' prior to the next formal release of the software.

Penetration: Intrusion, trespassing, unauthorized entry into a system. Merely contacting a system or using a key board to enter a password is not penetration, but gaining access to the contents of the data files by these or other means does constitute penetration.

PKI: Public key infrastructure (PKI) is the use and management of cryptographic keys – a public key and a private key – for the secure transmission and authentication of data across public networks.

Policy: A policy may be defined as 'An agreed approach in theoretical form, which has been agreed to/ratified by a governing body, and which defines direction and degrees of freedom for action.' In other words, a policy is the stated views of the senior management (or Board of Directors) on a given subject.

Procedure: A procedure spells out the specific steps of how the policy and the supporting standards and guidelines will actually be implemented. They are a description of tasks that must be completed in a specific order.

Protocol: A set of formal rules describing how to transmit data, especially across a network.

RSA: Stands for Rivest, Shamir and Adleman, who are the developers of the public key encryption and authentication algorithm.

Security breach: A breach of security is where a stated organizational policy or legal requirement regarding Information Security, has been contravened. However every incident which suggests that the Confidentiality, Integrity and Availability of the information has been inappropriately changed, can be considered a Security Incident.

Security for electronic transactions (SET): SET was originally supported by companies such as MasterCard, VISA, Microsoft and Netscape and provides a means for enabling secure transactions between purchaser, merchant (vendor) and bank.

Smart card: Smart cards look, and feel like, credit cards, but have one important difference, they have a 'programmable' micro-chip embedded. Their uses are extremely varied but, for information security, they are often used not only to authenticate the holder but also to present the range of functions associated with that user's profile.

Smurf attack or ping attack: This is where an illegitimate 'attention request' or *Ping* is sent to a system, with the return address being that of the target host (to be attacked). The intermediate system responds to the ping request but responds to the unsuspecting victim system. If the receipt of such responses becomes excessive, the target system will be unable to distinguish between legitimate and illegitimate traffic.

Sniffers: A sniffer is a program which captures and analyses packets of data as it passes across a network. Such programs are used by network administrators who wish to analyse loading across network segments, especially where they suspect that spurious packets are 'bleeding' from one network to another.

Social engineering: Social engineering is a means by which information is extracted, usually verbally, by someone impersonating a legitimate holder or user of the information in question.

Spam: Electronic equivalent of junk mail.

Spoofing: Alternative term for identity hacking and masquerading.

Steganography: Steganography is the technique whereby a message, possibly encrypted, is concealed within another medium. In the world of computing, this means that a seemingly innocuous graphic or sound file (say) can conceal a message which could be used to disguise corporate espionage.

SYN attack: This DoS attack takes places when connection requests to the server are not properly responded to, causing a delay in connection. Although these failed connections will eventually time out, should they occur in volume, they can deny access to other legitimate requests for access.

Teardrop attack: The exploitation of features of the TCP/IP protocol whereby large packets of data are split into 'bite-sized chunks' with each fragment being identified to the next by an 'offset' marker. Later the fragments are supposed to be re-assembled by the receiving system. In the teardrop attack, the attacker enters a confusing offset value in the second (or later) fragment which can crash the recipient's system.

Threat: A threat is anything that can disrupt the operation, functioning, integrity, or availability of a network or system.

Time-bomb: As the name suggests, a piece of hidden program code designed to run at some time in the future, causing damage to, or loss of, the computer system.

Trojan horse: A trojan horse is a malicious, security-breaking program that is disguised as something benign, such as a directory lister, archiver, game. A trojan is a type of virus that normally requires a user to perform some action before the payload can be activated.

Van Eck monitoring: Monitoring of the activity of a computer or other electronic equipment by detecting low levels of electromagnetic emissions from the device. It is named after Dr. Wim van Eck who discussed the topic in 1985.

Virtual private network (VPN): A virtual private network emulates a private network over a public network infrastructure, using specialist hardware and software.

Virus: A virus is a form of malicious code and as such is potentially disruptive. It may also be transferred unknowingly from one computer to another.

Vulnerability: A vulnerability is an inherent weakness in the design, configuration, or implementation of a network or system that renders it susceptible to a threat.

White hat/black hat hackers: White hat hackers are hackers who perform hacking for legitimate reasons, e.g. IT security technicians testing their systems and researchers testing the limits of systems. On the other hand, black hat hackers are those who perform clandestine hacking for malicious reasons; such persons can also be referred to as 'crackers'. Grey hat hackers are those who seem to fall between both camps.

Worm: A worm is a malicious program that propagates itself over a network, reproducing itself as it goes.

References

Burns S 2002 Unique characteristics of e-commerce technologies and their effects upon payment systems. GSEC (GIAC Security Essentials Certification) – Version 1.3

COBIT 2000 Control objectives for information and related technology: COBIT, 3rd edn, July 2000, Released by the COBIT Steering Committee and the IT Governance Institute

Duggal P 2000 *Cyberlaw in India – An analysis* (New Delhi: Saaksharth)

ISO/IEC 2000 Information technology – Code of practice for information security management. ISO/IEC 17799: 2000(E)

Kalakota R, Whinston A B 1999 *Frontiers of e-commerce* (Reading, MA: Addison-Wesley/Longman)

Mazumdar C, Barik M S, Das S, Roy J, Barkat M A 2003 Final technical report for project development of validated security processes and methodologies for web-based enterprises

Schneider G P, Perry J T 2001 *Electronic commerce*. Course Technology, Cambridge, MA

SSE-CMM 2003 Systems security engineering capability maturity model. SSE-CMM, Model Description Document Version 3.0, June 15, 2003

Varshney U, Vetter R J, Kalakota R 2000 Mobile commerce: a new frontier. *Computer* Oct. : 32–38

Websites

The house of secure e-commerce. http://www.istart.co.nz/index/HM20/PC0/PV21902/EX24014/AR25056

e-Commerce security. www.upu.int/security/en/e-commerce_security_en.pdf

Legal aspects of e-commerce. http://www.crime-research.org/library/Belousov_sep.html

FAQ on Information Technology Act. http://www.tamilnadunri.com/india/itpolicy/faq.html

The state of e-commerce security. http://www.newsfactor.com/perl/story/19462.html