IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4284

E-Commerce Security Issues

Ali Salehnia
Computer Science Department, South Dakota State University, Tel: (605) 688-5717, Ali_Salehnia@sdstate.edu

Hassan Pournaghshband
Dept of Computer Science, Southern Polytechnic State University, Georgia, Tel: (770) 528-4282, hpournag@spsu.edu

Copyright Idea Group Inc.

ABSTRACT

This paper explores the different types of EC security applications and technologies currently in use, and points out the possible weaknesses and drawbacks of the existing security measures in addition, it seeks to identify the privacy issues involved in EC and the range of possible solutions that may be adopted as ways to resolve those issues. A discussion of the privacy issues involved in EC, in addition to including how the personal information is being gathered and used by others and the privacy protection solutions, particularly ones that are technology-based.

INTRODUCTION

"Electronic commerce" (EC) is the term used to describe financial transactions in the electronic marketplace. This typically includes buying or selling products or services on the Internet via secure networks or extranets. Transactions may be business-to-business or business-to-consumer [10].

An EC site can be as simple as a catalog page with a phone number, or it can range all the way to a real-time credit card processing site where customers can purchase downloadable goods and receive them on the spot. EC merchants can range from a small business with a few items for sale all the way to a large online retailer.

Electronic commerce began in the 1970's when larger corporations started creating private networks to share information. This process is called "Electronic Data Interchange" (EDI). The drawback to EDI, however, has been that it requires expensive private networks and has left some suppliers out of the loop. That problem has been substantially curtailed by moving these EDI processes to the Internet. Other organizations wanting the benefits of EDI simply move to the Internet, and bypass EDI altogether. EDI laid the foundation for electronic commerce [10].

Electronic commerce is increasingly used to describe online retailing. Companies are created solely to take advantage of the Internet to do business and do not actually have physical stores [3].

Electronic commerce is changing how businesses market their products and how they serve their customers and business partners. While EC growth has opened doors to new opportunities and new tools, it has brought with itself new burdens and risks to corporate entities. Businesses must evaluate the parameters of establishing an online presence and conducting online operations with their customers and business associates. More than likely, the potential benefits will demand drastic changes within the company's borders. Before companies can offer such services to its external partners, they must first deal with internet issues. In essence, a company must efficiently conduct electronic business before it can conduct electronic commerce. In the near future, entering the EC marketplace may no longer be an option—it will become a necessity [9].

The most significant barrier to EC is consumer concerns about security and privacy.

In a Georgia Tech's Graphics, Visualization, and Usability Center's 1998 survey of online users, more than one half of respondents were very concerned about online security and privacy issues. Most (85 percent) responded that security and privacy features would be deciding factors in choosing whether to buy online [21].

Security and privacy issues are two separate but closely related issues. Consumers concerned about security question how data are protected from unintended uses as the data are transmitted and after they reach the merchant. Privacy issues generally focus on secondary use of information transmitted online. Consumers buying online want to know if the seller has asked only for the information needed to complete the transaction, if the seller will use that information only for the purpose intended, and if the seller will not give or sell that information to others without the consumer's consent. Discussion of online security has been focused on online payment options, specifically the security of credit card information sent online.

ELECTRONIC COMMERCE SECURITY

Since security is a major barrier to EC acceptance, businesses must earn the confidence of their customers. The goals of security are to provide secrecy, integrity, and availability, which mean that the data may only be accessed and modified by authorized persons [27]. Security plans should be included in the business strategy and should focus on data integrity, network integrity, and authorized access. Access controls, firewall systems, and encryption tools should be implemented to minimize security threats that may come from outside and from within the company's boundaries.

Threats to data integrity, privacy, fraud and theft can occur at many levels. As in any system, the system's security is only as strong as its weakest component. Many times the threats come from within. To address this thought, many companies, in addition to the security controls focused on external threats, employ electronic monitoring devices to monitor the activities of its employees. Similar to audit mechanisms, office automation devices and software enable methods of safeguarding the computer systems and tracking employee productivity. Many employees believe that they can discourage losses by monitoring. The most common methods and devices implemented are video cameras, telephone surveillance, and keystroke and file access monitoring [26].

Measures to Make EC Security Safe

Encryption

As offices and organizations have connected to the Internet to provide service for consumers, many have begun eyeing the Internet infrastructure as an inexpensive vehicle for wide area and remote connections. To use the Internet for these purposes, however, companies have to protect their information with encryption. Encryption is simply the process of using a formula, called an encryption algorithm, to translate plain text into an incomprehensible cipher text and then back to plain text again. Essential to encryption is a numeric value called the key that becomes part of the encryption algorithm, setting the encryption process in motion.

The most widely used encryption methods for EC security are public and private keys cryptography, Data Encryption Standard (DES) RSA (Rivest Shamir Adleman), and digital signature. Cryptography might be summed up as the study of techniques and applications that depend on the existence of difficult problems. Cryptography allows people to carry over the confidence found in the physical world to the electronic world, thus allowing them to do business electronically without worries of deceit and deception.

Every day hundreds of thousands of people interact electronically, whether it is through EC, e-mail, or cellular phones. Cryptogra-

This paper appears in *Issues and Trends of Information Technology Management in Contemporary Organizations,* the proceedings of the Information Resources Management Association International Conference. Copyright © 2002, Idea Group Inc.

phy makes secure websites and electronically safe transmissions possible. For a website to be secure, all of the data transmitted between the computers where the data is kept and where it is received must be encrypted. This allows people to do online banking, online trading, and to make online purchases with their credit cards, without worrying that any of their account information is being compromised. Cryptography is very important to the continued growth of the Internet and EC [22].

There are two types of cryptosystems:

1. Public key cryptography
2. Secret key cryptography

In traditional cryptography, the sender and receiver of a message know and use the same secret key: the sender uses the secret key to encrypt the message, and the receiver uses the same secret key to decrypt the message. This method is known as secret key or symmetric cryptography. The main challenge is getting the sender and receiver to a degree on the secret key without anyone else finding out. If they are in separate physical locations, they must trust a courier, a phone system, or some other transmission medium to prevent the disclosure of the secret key. Anyone who overhears or intercepts the key in transit can later read, modify, and forge all messages encrypted or authenticated using that key. The generation, transmission and storage of keys are called key management. All cryptosystems must deal with key management issues. Because all keys in a secret key cryptosystem must remain secret, secret key cryptography often has difficulty providing secure key management, especially on the Internet with a large number of users.

In order to solve the key management problem, Whitfield Diffie and Martin Hellman introduced the concept of public key cryptography in 1976. Public key cryptosystems have two primary uses, encryption and digital signatures. In their system, each person gets a pair of keys; one is called the public key and the other is called the private key. The public key is published, while the private key is kept secret. The need for the sender and receiver to share secret information is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared. In this system, it is no longer necessary to trust the security of some means of communications. The only requirement is that public keys be associated with their users in a trusted (authenticated) manner (for instance, in a trusted directory). Anyone can send a confidential message by just using public information, but the message can only be decrypted with a private key, which is in the sole possession of the intended recipient. Furthermore, public key cryptography can be used not only for privacy (encryption), but also for authentication (digital signatures) and other various techniques [2][8].

Digital signature is any type of text or message, encrypted with a private key, and thereby identifies the source. Digital certificate is an electronic document that verifies the owner of a public key and a Certificate Authority (CA) issues it. In a public key cryptosystem, the private key is always linked mathematically to the public key. Therefore, it is always possible to attack a public key system by deriving the private key from the public key. Typically, the defense against this is to make the problem of deriving the private key from the public key as difficult as possible. For instance, some public key cryptosystems are designed so that deriving the private key from the public key requires the attacker to factor a large number; in this case it is computationally infeasible to perform the derivation. This is the idea behind the RSA public key cryptosystem [8][2].

If many keys are used, encryption key management is not an easy task. Public Key Infrastructure (PKI) is a management system designed to provide public key encryption and digital signature support for applications and services. By managing keys and certificates through a PKI, an organization can establish and maintain a secure networking environment [2][11][13][20].

Following scenario is an example of uses of encryption: When A wishes to send a secret message to B, she looks up B's public key in a directory, uses it to encrypt the message and sends it off. B then uses his private key to decrypt the message and read it. No one listening in can decrypt the message. Anyone can send an encrypted message to B, but only B can read it (because only B knows his private key). The secret key cryptography when is sometimes referred to as symmetric cryptography is a 56-bit key. It is the more traditional form of cryptography, in which a single key can be used to encrypt and decrypt a message. Secret key cryptography not only deals with encryption, but it also deals with authentication. One such technique is called Message Authentication Codes (MACs). The main problem with secret key cryptosystems is getting the sender and receiver to agree on the secret key without anyone else finding out. This requires a method by which the two parties can communicate without fear of spying. However, the advantage of secret key cryptography is that it is generally faster than public key cryptography [23].

The most popular secret key cryptosystem in use today is DES (data encryption standard). IBM developed DES in the middle 1970´s and it has been a federal standard ever since 1976**.**

Data Encryption Standard (DES)

DES is the first standard cipher the business world had. It is still widely used, but it is aging and getting much less secure. A knowledgeable attacker who can afford plenty of expensive computer equipment can now break DES easily [23]. DES started in 1973, and the US National Bureau of Standards asked for proposals for a standard cipher. In 1975, IBM developed DES, and in 1981, the American National Standards Institute approved DES as a standard for business use. Banks made much use of it. DES was quietly built into all kinds of software applications. As software, it protects computer networks. Because it was a standard, any system using DES could talk to any system using it. The key length is 56 bits. In order to crack a key, one has to check 5 trillion keys per second [1].

Rivest Shamir Adleman (RSA)

RSA is a public key cryptosystem that offers both encryption and digital signatures (authentication). Ron Rivest, Adi Shamir, and Leonard Adleman developed RSA in 1977; RSA stands for the first letter in each of its inventors' last names. RSA is so useful as a secure electronic envelope for small messages and as a way of signing messages, that it is a part of a lot of hardware and software [29]. The encryption and authentication take place without any sharing of private keys: each person uses only another's public key or one's own private key. Anyone can send an encrypted message or verify a signed message, but only someone in possession of the correct private key can decrypt or sign a message [23].

Firewall

A firewall is simply a barrier between two networks—in most cases an internal network, often called the trusted network, and an external network, called the untrusted network (in this case, the Internet). Firewalls examine incoming and outgoing packets according to a set of policies defined by the administrator; they either let them through or block them. Firewalls aren't an Internet security cure-all, but they are essential to just about any Internet security strategy [29].

Many routers use a firewall technique called packet filtering. This examines the source and destination addresses and ports of incoming TCP and UDP packets and denies or allows packets to enter based on a set of predefined rules. Packet filters are inexpensive, are transparent to users, and have a negligible impact on network performance. Configuring packet filtering, however, is a relatively complex process. It usually requires precise knowledge of network, transport, and sometimes even application protocols [2].

Security Threats to EC

A number of security threats and risks make the unsecured Internet difficult as a medium for conducting EC. Security holes can be classified into the following groups: physical security holes, software security holes, and inconsistent usage holes [24]. Physical security holes

Copyright Idea Group Inc.

involve unauthorized parties gaining physical access to a computer or LAN. The unauthorized access may arise from an employee accessing internal systems to obtain credit card numbers, private keys and digital certificates, personal or sensitive corporate information for the purpose of financial gain, or for other illegal purposes. On the Internet, hackers may gain access to network resources by guessing passwords or cracking traded password lists for the same reasons an employee would, or to compromise authentication systems such as Certificate Authorities (CA) [12][13][15].

Software security holes result when badly written programs are compromised into doing things they shouldn't. Attacks of this type usually allow the attacker to gain super-user access, giving them free reign over the entire system. Inconsistent usage holes occur when a system administrator assembles a combination of hardware and software so that the system is seriously flawed from a security point of view [12][14][15].

1. Interception: This is an attack on confidentiality of one or more parties, whereby an unauthorized party intercepts TCP/IP packets for some illicit purpose [29][7]. The broadcasting nature of the Internet allows any party on the same physical wire to intercept any packets that are transmitted across it [30]. An unauthorized party may intercept packets to obtain passwords, credit card numbers, billing or personal information, account balances and the like. In addition, this type of attack has the ability to permit theft of information-based products and software that must be downloaded from commercial sites [7].
2. Data Modification: In this form of attack the unauthorized party intercepts and deliberately modifies the contents of packets, and the intended recipient receives the modified packet ([7][28]. The motives for data modification are numerous, including changing the address on an order, changing the account to transfer funds to, or changing the payee on an electronic check.
3. Spoofing: Spoofing attacks enable one party to pretend to be another party [7]. In a spoofing attack, the attacker creates a misleading context in order to trick the victim into making an inappropriate security-relevant decision [16]. The spoofing attack can be used by an attacker to pretend to be a legitimate vendor to collect thousands or millions of credit card numbers, account numbers, or other sensitive information from unsuspecting customers [7]. In addition, the attacker may use the spoofing attack to deliberately discredit a company's good reputation, or to pretend to be a bank or Certificate Authority to directly attack a merchant for financial gain.
4. Repudiation: Repudiation simply allows either the sender or receiver to deny that a message was transmitted because of the Internet's inability to verify parties in a transaction [28]. Repudiation of transactions can cause major problems with billing systems and transaction processing arrangements [7]. In the real world, the customer is authenticated by signatures, pin numbers, and so forth, which can be validated by inspection or by the banks' authentication systems. As the Internet does not provide the means to authenticate parties in transactions, the customer can simply deny that the transaction occurred.
5. Viruses: These are all programs that have the ability to cause unexpected and undesirable effects on network resources and software. All have the ability to delete software, consume bandwidth, transmit information to other hosts, and create other undesirable effects that can cause serious disruption and compromise to software and information stored on a system.
6. Denial of Service Attacks: Denial of service attacks prevent or inhibit the normal use or management of network resources [28]. An attacker may send repeated emails to fill up the mailbox (and possibly crash the system), continuous HTTP or other protocol requests that prohibit anyone else from using these resources. An attack of this form on a merchant will effectively stop business until the problem is discovered and corrected. This arises because client-server is the basic architecture of the Internet meaning that any server will respond to any request for its service from any client that requests it.

All of these security threats and risks make the Internet a very risky place to do business. Countermeasures for most of these security threats exist, including encryption, digital certificates, encrypted communication channels such as Secure Socket Layer (SSL), Firewalls, and so on. The implementation of the countermeasure often requires experienced persons to locate, recognize and implement the appropriate solutions. While most large organizations are aware of the threats and the methods to counter them, the average small business operator or individual wishing to sell its wares on the Internet will lack the relevant knowledge, understanding and experience to effectively counter most Internet security threats [11][13][15].

Even where appropriate security countermeasures are in place, they should never be considered foolproof. Digital certificates must be stored on hard drives and are therefore subject to theft [25]. Firewalls, despite their reported benefits, can still fall victim to misconfiguration and software security holes that allow them to be subverted. There have been numerous reports of successful attacks on both commercial and organizational sites that use firewall technology [4][17]. Encryption is vulnerable to brute force methods of attack [17][19]. Problems can be found with most security countermeasures, and the Internet payment systems in use today all use some combination of these countermeasures to provide a secure method of allowing electronic payment.

SUMMARY

In this paper E-Commerce security issues were discussed. The measures to be taken to enforce security and privacy in the E-commerce environment were also reviewed. The different types of EC security applications and technologies currently in use were explored. The possible weaknesses and drawbacks of the existing security measures as well identification of the privacy issues involved in EC and the range of possible solutions that may be adopted were pointed out.

REFERENCES

[1] Adams C. & Lloyd S. (1999). Understanding the Public-Key Infrastructure. New Riders Publishing.
[2] Austin T., Huaman D. & Austin T.W. (2000). Public Key Infrastructure Essentials, John Wiley & Sons.
[3] Bakos, Yannis. (1998). "The emerging role of electronic marketplaces on the Internet," Communications of the ACM, 41 35-42.
[4] Bank, D., (1996). "Mission Possible: Shoppers Find Out How Safe the Web Is —Improper Program Installation Lets Browsers Easily Access Credit-Card Information," Wall Street Journal, Nov 8.
[5] Bank96a, (1996). "Perception isn't security reality, Bank Systems and Technology, "Wall Street Journal , Dec. 1996.
[6] Bank96b, (1996). "RSA debuts SET developer's kit, Bank Systems & Technology," Wall Street Journal , Dec. 1996.
[7] Bhimani, A., (1996). "Securing The Commercial Internet," Communications Of The ACM, vol. 39, No 6, pp. 29-35, June 1996.
[8] Brands S.A. (2000) 'Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy" MIT Press.
[9] Choi, Soon-Yong; Stahal, Dale O.; and Whinston, Andrew B. (1998). "Commerce on the Internet: What's holding it up?". http://cism.bus.utexas.edu/works/articles/intergov.html
[10] "E-Commerce guide's ask the experts." (2000). http://e-comm.internet.com/solutions/questions/q7.ecommerce.html.
[11] Ellison C. (1999). "The nature of a usable PKi," Computer Networks. Vol. 31 pp.823- 830.
[12] Ellison C. (2000a). "Naming and Certificates," Proc. Computers, Freedom & Privacy . http://www.cfp2000.org/papers/ellison.pdf
[13] Ellison C. (2000b). "SPKI/SDSI and the Web of Trust," http://world.std.com/~cme/html/web.html
[14] Ellison C. & Schneier B. (2000a). "Risks of PKI: Electronic Commerce Inside Risks," Comm. Of ACM 43, 2. http://www.counterpane.com/insiderisks5.html
[15] Ellison C. & Schneier B. (2000b) "Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure," Computer Secu-

Copyright Idea Group Inc.

rity Journal, v 16, n 1, 2000, pp. 1-7, at http://www.counterpane.com/pki-risks.html.
[16] Felten, E, W., Balfanz, D., Dean, D., & Wallach, D, S., (1997). "Web Spoofing," An Internet Con Game. Princeton University.
[17] Ghosh, Anup K. (1997). "Securing E-Commerce: A Systematic Approach," Journal of Internet Banking and Commerce. http://www.ARRAYdev.com/commerce/JIBC/9704-04.htm.
[18] Ghosh, A. (998). E-commerce security: weak links, best defenses. John Wiley & Sons.
[19] Ghosh, Shikhar. (1998). "Making Business of the Internet," Harvard Business Review Abstract. http://www.hbsp.harvard.edu/products/hbr/marapr98/98205.html.
[20] Gibbs, Mark. (1999). "Breaking Global Barriers," Network World. http://www.nwfusion.com/ec/0222global.htm.
[21] Graphics, Visualization, and Utilization Center. (1998). "GVU's 10th WWW User Survey." Available: http://www.gvu.gatech.edu/gvu/user_surveys/survey-1998-10.
[22] Grossman W. (2000). "Circles of Trust'," Scientific American. http://www.sciam.com/2000/0800issue/0800cyber.html
[23] Gutmann P. (2000). "X.509 Style Guide," http://www.cs.auckland.ac.nz/~pgut001/pubs/x509guide.txt
[24] Kalakota, R., & Whinston, A, B. (1996). Frontiers of Electronic Commerce, Addison Wesley.
[25] McClure, S., (1998). "SSL makes headway as an encryption standard, Netscape Enterprise Developer," http://www.netscapeworld.com.
[26] McCullagh A. & Caelli W. (2000). "Non-Repudiation in the Digital Environment," http://firstmonday.org/issues/issue5_8/mccullagh/index.html
[27] Pfleeger, Charles P. (1989). Security in Computing. Englewood Cliffs NJ: Prentice-Hall Inc.
[28 Stallings,W. (1995). Network And Internetwork Security: Principles And Practice. Prentice-Hall.
[29] Stamper, David A. (1999). Business Data Communicatins (5th. ed.). New York: Addison Wesley.
[30] Tanenbaum, A., (1996). Computer Networks, Third Edition, Prentice Hall.

Copyright Idea Group Inc.
Copyright Idea Group Inc.
Copyright Idea Group Inc.
Copyright Idea Group Inc.

0 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/proceeding-paper/commerce-security-issues/31884

Related Content

Agriculture 4.0 and Bioeconomy: Strategies of the European Union and Germany to Promote the Agricultural Sector – Opportunities and Strains of Digitization and the Use of Bio-Based Innovations

Immo H. Wernicke (2021). *Encyclopedia of Information Science and Technology, Fifth Edition (pp. 1323-1335).*

www.irma-international.org/chapter/agriculture-40-and-bioeconomy/260269

Contemporary Leadership Development in Kazakhstan

Gainiya Tazhina, Judith Parker and Arslan Ivashov (2018). *Encyclopedia of Information Science and Technology, Fourth Edition (pp. 5626-5637).*

www.irma-international.org/chapter/contemporary-leadership-development-in-kazakhstan/184263

An Artificial Intelligent Centered Object Inspection System Using Crucial Images

Santosh Kumar Sahoo and B. B. Choudhury (2018). *International Journal of Rough Sets and Data Analysis (pp. 44-57).*

www.irma-international.org/article/an-artificial-intelligent-centered-object-inspection-system-using-crucial-images/190890

A Novel Approach to Enhance Image Security using Hyperchaos with Elliptic Curve Cryptography

Ganavi M and Prabhudeva S (2021). *International Journal of Rough Sets and Data Analysis (pp. 1-17).*

www.irma-international.org/article/a-novel-approach-to-enhance-image-security-using-hyperchaos-with-elliptic-curve-cryptography/288520

An Efficient Random Valued Impulse Noise Suppression Technique Using Artificial Neural Network and Non-Local Mean Filter

Bibekananda Jena, Punyaban Patel and G.R. Sinha (2018). *International Journal of Rough Sets and Data Analysis (pp. 148-163).*

www.irma-international.org/article/an-efficient-random-valued-impulse-noise-suppression-technique-using-artificial-neural-network-and-non-local-mean-filter/197385