E-Commerce security

Dr. Nada M. A. Al-Slamy

Alzaytoonah University MIS Dept. Amman, Jordan 962

Summary

Internet has made the idea of an idealized marketplace seem plausible. However, there are still concerns regarding the exchange of money securely and conveniently over the internet. PRETTY GOOD PRIVACY (PGP) provides a confidentiality and authentication service that can be used for E-commerce This research is undertaken firstly to study the benefit of using PGP approaches as a method of E-commerce security , and secondly to specify the benefits of encryption methods and techniques to secure internet E-commerce. PGP is used behind SSL method to provide high security with E-commerce.

Key words:

Input here the part of 4-5 keywords.

1. Introduction

Electronic commerce is buying and selling of goods and services across the internet. Commercial activities over the internet have been growing in an exponential manner over the last few years. When it comes to payment, one needs to establish a sense of security. Customers must be able to select a mode of payment and the software must verify their ability to pay. This can involve credit cards, electronic cash, encryption, and/or purchase orders. The more of these techniques are supported by an E-commerce package, the more secure the system can be, and therefore the more customers are benefits from E-commerce abilities [1][2].

E- Commerce business has 4 different consists of components to build business to consumer, All of these elements combined give the store a personality & the end uses a true shopping experience [2].

1- Product Catalog.
2- Sopping Cart.
3- Transaction Security.
4- Order Processing.

This research is undertaken firstly to propose method of E-commerce security policies, and secondly to specify the benefits of encryption methods and techniques to secure internet E-commerce[3][4].

2. Security and E-Commerce

It is clear that electronic commerce will revolutionize businesses, and customers will be offered new and exciting services. As E-commerce businesses are growing, more secure technologies are being developed and improved every day. The current internet security polices and technologies fail to meet the needs of end users. The success or failure of an E-commerce operations hinges on myriad factors, including but not limited to the business model, the team, the customers, the investors, the product, and the security of data transmissions and storage. Any business that wants to have a competitive edge in today’s global marketplace should adopt a comprehensive security policy in consultation with partners, suppliers, and distributors that will provide safe environment for the coming proliferation of E-commerce [2][5].

Public Key Infrastructure (PKI) refers to the notion that the best way to establish a system of secure communications over networks is to establish an infrastructure that will support public key encryption. The PKI would create an environment where any Internet user could "carry" certificates around that identify them in a variety of ways. Authentication of parties could become very cheap and easy. Some e-commerce proponents suggest that creation of a seamless and robust PKI would have enormous implications for speeding the growth of e-commerce, see figure 1.

Manuscript received May 5, 2008.
Manuscript revised May 20, 2008.

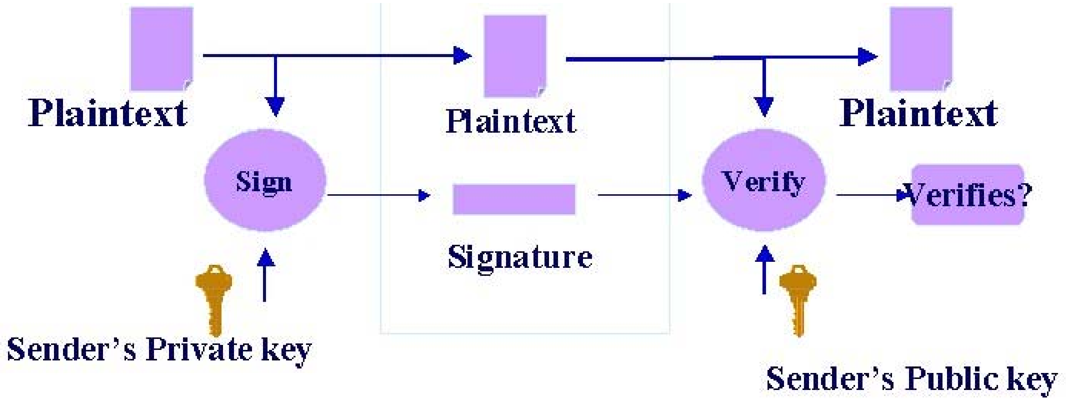

Figure 1: public key Infrastructure (PKI)

E-commerce software packages should also work with secure electronic transfer (SET) or secure socket layer (SSL) technologies for encryption of data transmissions. (SSL) protocols, which allow for the transmission of encrypted data across the Internet by running above the traditional TCP/IP protocols.

In cyberspace, both the customer and the vendor have difficulty in proving their identity to each other with certainty, particularly during a first transaction. How does the buyer securely transmit sensitive information to the seller? How does the seller know that this is a legitimate purchase order? How do both parties know that a nefarious third party has not copied and/or altered the transaction information? These questions and others, describe the problem effecting commercial transactions over the internet, or any public network.

Customer (clients) need to be sure that:-

1- They are communicating with the correct server.
2- What they send is delivered unmodified.
3- They can prove that they sent the message.
4- Only the intended receiver can read the message.
5- Delivering is guaranteed.

On the other side, vendors (severer) need to be sure that:

1- They are communicating with the right client
2- The content of the received message is correct.
3- The identity of the author is unmistakable.
4- Only the author could have written the message.
5- They acknowledge receipt of the message.

All of the concerns listed above can be resolved using some combination of cryptographic method, and certificates methods[3].The type of risk involved resulting from inadequate security is:

1- Bugs or miss-configuration problems in the web sever that can cause the theft of confidential documents.

2- Risks on the Browsers' side i.e. breach of user's privacy, damage of user's system, crash the browser etc

3- Interception of data sent from browser to sever or vice versa. This is possible at any point on the pathway between browser and the server i.e. network on browser's side, network on server's side, end user's ISP (Internet Service Provider), the server ISP or either ISP's regional access.

3. Polices of E-commerce security measure

There are different policies used to ensure and measure security in E-commerce environment, we shall explain some of them in the following sections, which are: Privacy, Cryptography, and certificates.

3.1 Privacy policy

According to a study released by commerce Net & Nielsen Media Research," More than 2 out of every five people in North America are now Internet users, & the web is becoming as integral part of daily life", see table 1 . Without a through privacy security policy, it's not possible to spend money in a responsible and cost – effective manner. Develop a privacy security policy that includes defining the sensitivity of information, the exposure of the organization if that information was likelihood of those risks becoming reality. A policy may contain many elements including purchasing guidelines, statements of availability and Privacy.

Privacy polices architecture the manner in which a company collects, uses, protects data, and the choices they offer consumers to exercise rights when their personal information is used. On the basis of this policy, consumers can determine whether and to what extent they wish to make information available to companies [1][5].

What People Shop for Online (But don't Necessarily Buy)	
Category	Shopers (millions)
Cars and parts	18.2
Books	12.6
Computers	12.4
Clothing	11.6
CDs/Videos	11.4
Source Nielsen/Commerce Net	

3.2 Cryptography

Cipher systems are classified into 2 classes which are:-

1- Secrete key cipher system.
2- Public-key cipher system

In the following we shall describe each class briefly

Secrete Key: Secret key cryptography is the oldest type of method in which to write things in secret. There are tow main type of secrete key cryptography, transposition and substitution. Transposition cipher , encrypt the original message by changing characters order in which they occurred. Where as in substitution cipher, the original message was encrypted by replacing there characters with other characters. In both types, both the sender and receiver share the same secret keys. The most widely used secret key scheme today is called Data Encryption Standard (DES). DES cipher work with 56-bit secret key and 16 rounds to transform a block of plaintext into ciphertext.

Public Key: Public-key cryptography was developed to solve the secret-key distribution problem associated with secrete key method. It was first publicly described in 1976 by Stanford University Professor Martin Hellman and graduate student Whitfield Diffie. Public key method use tows different (as shown in figure 1), but mathematically related, keys. One of the keys is used to encrypt the data, i.e. plaintext and the second key is used to decrypt the cipher text The second problem that Diffie pondered, and one that was apparently unrelated to the first was that of "digital signatures". Rivest Shamir-Adleman (RSA) scheme is the most widely accepted and implemented general-purpose approach to public-key encryption.

The RSA scheme is a block cipher in which the plaintext and cipher text are integers between 0 and n-1 for some n. A typical size of n is 1024 bits, or 309 decimal digits. The block size must be less than or equal to log2(n). Encryption and decryption are of the following form, for some plaintext M, and cipher text C:

$$C= M ^{\wedge} e \mod n$$

$$M= C^{\wedge}d \mod n = (M^{\wedge}e)^{\wedge}d \mod n = M ^{\wedge} ed \mod n$$

Both sender and receiver must know the value of n [3][4][6]. The sender knows the value of e, and only the receiver knows the values of d. Thus, this is a public-key encryption algorithm with

a public key of KU= {e,n},

and a private key of KR={d,n}

3.3 Certificate

Certificates bind identity, authority, public key, and the other information to a user. For most internet E-commerce application, certificates using a format defined in international telecommunication union telecommunication standardization sector (ITU-T). Recommendation X.509 is employed. An X.509 certificate contains such information as the:

1- Certificate holder's name and identifier.
2- Certificate holder's public key information.
3- Key usage limitation definition.
4- Certificate policy information.
5- Certificate issuer's name and identifier.
6- Certificate Validity period.

In today's E-commerce environment, buyers may get personal certificates to prove their identity to a web site but it is the vendor sites that really need to have certificates to prove their identity to buyers.

4. Pretty Good Privacy(PGP)

PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications. PGP has grown explosively and is now widely used, three main reasons can be cited for this growth:

.First: It is based on algorithm that has survived extensive public review and are considered extremely secure.

.Second: It has a wide range of applicability,

.Third: It was not developed by, nor is it controlled by, any governmental or standards organization

The actual operation of PGP consists of five services: authentication, confidentiality, compression, e-mail compatibility, and segmentation. In the following sections we examine the first two services since they are highly concern with this paper aim, that is E-commerce security [3][4].

4.1 Authentication

Authentication requires a digital signature. The process begins with a mathematical summary called a “hash”, which acts as a “Fingerprint” of the message. The message contents cannot be changed without altering the has code, see figure 1. This hash code is then encrypted with sender’s private key and attached to the message. When the message has been received, the hash code attached to the message is compared to another hash code or summary calculated by the recipient. IKeys for digital signatures are filed in a public-key directory, made up of “certificates” for every user. A trusted Certification Authority (CA) manages and distributes these certificates, in addition to distributing electronic keys. As shown in figure 2, the digital signature scheme done in the following sequence[3][7]:

- The sender creates a message.
- SHA-1 hashing code is used to generate a 160-bit hash code of the message.
- The hash code is encrypted with RSA using the sender’s private key, and the result is prep ended to the message.
- The receiver uses RSA with the sender’s public key to decrypt and recover the
- The receiver generates a new hash code for the message and compares it with the decrypted hash code. If the two match, the message is accepted as authentic.

The combination of SHA-1 and RSA provides an effective digital signature scheme. Because of the strength of RSA, the recipient is assured that only the possessor of the matching private key can generate the signature. Because of the strength of SHA-1, the recipient is assured that no one else could generate a new message that matches the hash code and, hence, the signature of the original message. Although signatures normally are found attached to the message or file that they sign, detached signatures are also supported. A detached signature may be stored and transmitted separately from the message it signs [3][4][8].

4.2 Confidentiality

Confidentiality is provided by encrypting message to be transmitted or to be stored locally as files as described in the following sequences, see figure 1:
- The sender generates a message and a random 128-bit number to be used as a session key for this message only.
- The message is encrypted, with session key.
- The session key is encrypted with RSA, using the recipient’s public key, and is prep ended to the message.
- The receiver uses RSA with its private key to decrypt and recover the session key.
- The session key is used to decrypt the message.

Te last three PGP services [3]:
Compression : A message may be compressed using ZIP.
E-mail compatibility: An encrypted message may be converted to an ASCII string by using some conversion algorithm, to provide transparency for E-commerce.
Segmantation:To ccommodate maximum message size limitations, PGP perform segmentation.

Based on the discussion above, we can conclude that the advantages of electronic commerce outweigh the negatives by a wide margin. Great success is possible for those businesses which implement E-commerce, if powerful security techniques are supported. In the future Global Village, all the financial transactions would be conducted virtually over the internet. With the rapid developments towards achieving security on the “net”, the time is not too far where paper money and physical banks would become extinct. The few development in this direction are some of the products developed and being used by Security First Technologies: Virtual Bank Manager, Virtual Credit Card Manager, Virtual Investment Manager, Virtual Loan Manager [7].

5. Summary

1.To be on the cutting edge of e-commerce, you need to understand how to best utilize cryptography to offer secure services for your customers over the Internet.
2. The success or failure of an e-commerce operation hinges on myriad factors, including but not limited to the business model, the team, the customers, the investors, the product, and the security of data transmissions and storage. Data security has taken on heightened importance since a series of high-profile "cracker" attacks have humbled popular Web sites, resulted in the impersonation of Microsoft employees for the purposes of digital certification, and the misuse of credit card numbers of customers at business-to-consumer e-commerce destinations.
3. Public Key Encryption ostensibly creates a world in which it does not matter if the physical network is insecure. Even if - as in the case of a distributed network like the Internet, where the data passes through many hands, in the form of routers and switches and hubs - information could be captured, the encryption scheme keeps the data in a meaningless form, unless the cracker has the private key.
4. Public key encryption is much slower than shared key encryption, so products like PGP use the public/private keys to share a secret key, which is then used to encrypt the rest of the dialog. PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications.

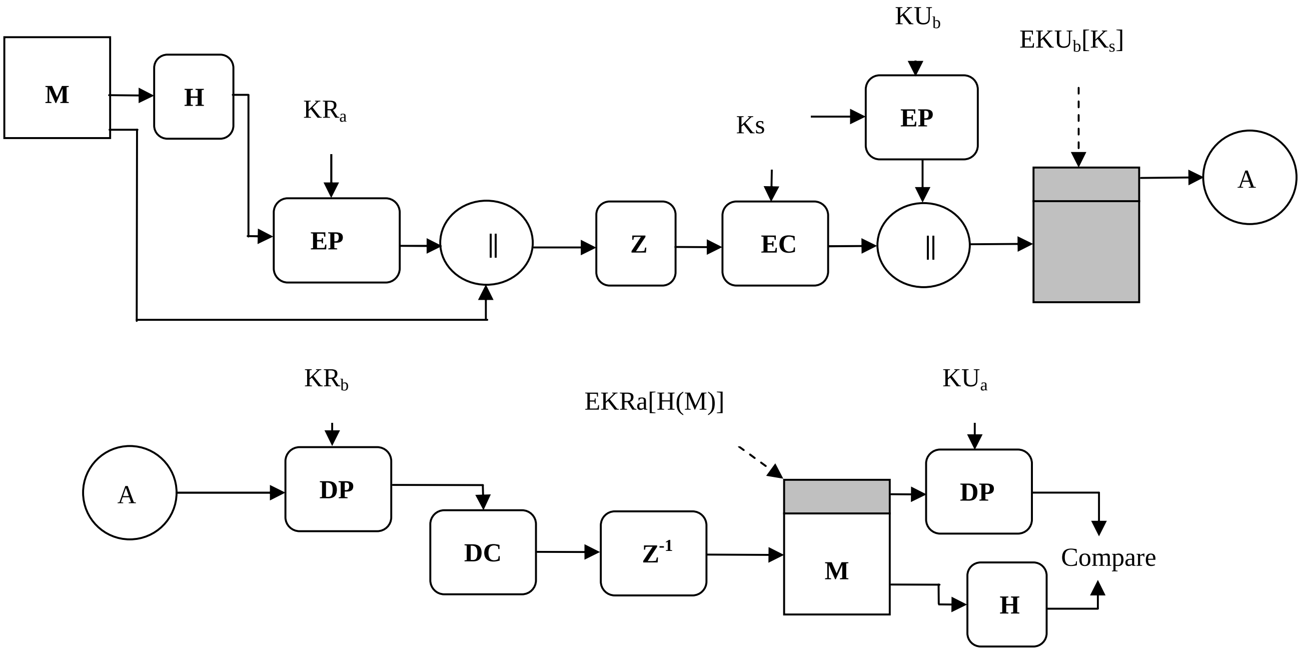

Fig2. PGP Cryptographic functions

References

[1] David J. Olkowski, Jr., "Information Security Issues in E-Commerce", SANS GIAC Security Essentials , March 26,2001.

[2] Paul A. Greenberg, "In E-Commerce We Trust … Not ", E-commerce Time, February 2, 2001, URL: http:// WWW.ecommercetimes.com/perl/story/?id=7194.

[3] William Stallings, "Cryptography and network Security", 3rd edition, Prentice Hall,2003.

[4] Michall E. Whitman and Herbert J. Maiiord, "Information Security", Thomson, Inc. , 2003.

[5] Dave Chaffey, "E-Business and E-Commerce", 2nd , Prentice Hall, 2005

[6] Mark Merkow . Jim Breithaupt, "Information Security Principles and Practices", Pearson Prentice Hall, 2006.

[7] A. Coulibaly & A. Inam ." Security Issues Facing E-Commerece", From Internet http://WWW.ACM.COM

[8] Brian McWilliams and Clint Boulton,"Another E-Commerce SiteSuffers Hack Attack", intermetnews.com, March 2, 2000.

Nada M. A. Al-Slamy (1971) , PhD in Computer Science / Theory of computer Science and Artificial Intelligence. She is Assistant Professor at Management of Information System Department in the Faculty of Economics and Administrative Sciences at Al-Zaytoonah University of Jordan. She Interests in. fields : Computational theory, Artificial Intelligence, Information Security, Data Mining and Data Retrieval.