

95-752 INTRODUCTION TO INFORMATION SECURITY MANAGEMENT (FALL 2009)

E-commerce Security

Encryption Methods for secure e-commerce websites

Diana Widjaja

H. John Heinz III College
Carnegie Mellon University

Table of Contents

1. Introduction	3
2. Background.....	4
3. Analysis	5
A. Public Key Infrastructure	5
B. Digital Signatures.....	6
C. Digital Certificates	8
D. Secure Socket Layer (SSL)	9
E. Secured e-commerce transaction flow	10
4. External factors affecting e-commerce security	11
5. Conclusion.....	11

1. Introduction

As the internet experiences progress and innovation, small and big companies alike are moving their goods and services online as a channel to increase revenues. Internet commerce, or e-commerce, is claimed to have generated \$30 billion in 2005¹. Increasing financial and commercial transactions online have led a rise in cybercrimes which take advantage of security flaws in online payment systems to steal sensitive data for financial thefts. Consumer confidence has been adversely affected, with 37% of e-shoppers stopped buying goods online because of identity theft concerns, resulting in a \$40 billion loss in online sales². Most consumers consider security features as critical factors influencing their decisions to conduct financial transactions online³.

As businesses turn electronic, digital credentials has become a requirement and information security an inevitable necessity to guard the online businesses. E-commerce relies on encryption to secure data transmission by controlling data access and protect information on the internet and ultimately boost consumer confidence. Encryption is the encoding of data using an algorithm such that it is incomprehensible to anyone in the event that the data transmission is intercepted, unless the key is known to enable file decryption. By implementing encryption, integrity is maintained while digital authentication is enforced, thus allowing both customers and merchants to verify the identity of the other party, a concept fundamental to secure online credit card transactions. The credibility of an e-commerce website may be negatively impacted if theft of customer information occurs, especially risky since 90% of all online payments are dealt by credit cards.

The paper will explore public key encryption methods and its impact on e-Commerce, discussing the application and implementation on this field along with its strengths and weaknesses, followed by an analysis of established trends such as Public Key Infrastructure in e-Commerce to enhance security.

¹ VeriSign, "Building an e-commerce trust infrastructure", 2000

² Forrester Research, "The checkout tools that boost eBusiness", 2007

³ Gartner, Inc., "Banks need to strengthen user authentication while appeasing consumers", 2008

2. Background

Online transactions come with associated risks in the form of spoofing, unauthorized disclosure and action, eavesdropping, and data alteration¹. Given the risks, e-commerce remains lucrative as it removes time and distance barriers for customers globally and attracts new ones, while increasing profitability as a cost-effective delivery channel by potentially eliminating overhead costs. The opportunities presented by this channel have therefore given rise to the need to address associated risks of online transactions with encryption.

Security is enforced through basic goals to achieve a trustable infrastructure for e-commerce. The first step to ensure customers' identities are safely guarded requires strong authentication, which assures users that the website they are dealing with are legitimate. When customers engage in payment or financial transactions, data transmission must be secured, and this process involves protecting the confidentiality and integrity of data. With the best interest of consumers addressed, it is critical to safeguard the transactions with regards to the e-commerce entities as well; the trust infrastructure should not render it possible for online consumers to repudiate their online transactions, a situation addressed by digital signatures.

Two types of encryption methods, symmetric and asymmetric, offer reliable protection to online businesses. Symmetric encryption (private key encryption) uses a common key between two or more parties for encryption and decryption. While symmetric key cryptography is computationally efficient with shorter keys and shorter lifespan, asymmetric key cryptography is computationally expensive and requires very long keys which has longer lifespan. However, for e-commerce purposes, asymmetric encryption has proven to be more important⁴ with the implementation of the second key which increases data integrity. Asymmetric encryption is also known as public key encryption, involving long prime numbers or keys—private and public—that act like a digital signature to prove one's identity online or certify documents for its authenticity. The public key encrypts messages while the private key decrypts them. It is more secure than symmetric encryption as knowing one key does not translate to the ability to infer the other key.

⁴ John Palfrey, "Security and the basics of encryption in e-commerce"

3. Analysis

A. Public Key Infrastructure

An effective tool for ensuring the safety of e-commerce transactions, public key infrastructures (PKI) combines a digital signature and certificate authority (CA), which can be public or private—a business acting as its own CA is private while a public one offers its services to businesses and provides secure key management. The role of a CA is built on the concept of trust, since web entities do not have sufficient trust established between them to perform business transactions. PKI is based on public key (asymmetric key) encryption, where a receiver generates an asymmetric key pair (private and public). The public key is shared with other participants who wish to encrypt data with the receiver while the private key is used to decrypt the data, addressing key management problems since no shared keys are required. Major US vendors in this field comprise VeriSign Inc and GlobalSign.

As the foundation of PKI, public key cryptography refers to the generation, distribution, organization, and the control of cryptographic keys. RSA, the commonly used algorithm in public key cryptography, implements keys based on the product of two large prime numbers. This method attributes to its cryptographic strength since factoring large composite numbers is highly challenging, given a sufficiently large key length. Using the public and private key mentioned previously, it enables encryption of cleartext data with the public key and decryption with the private one.

The RSA algorithm generates public and private key pair by the following method⁵. Two sufficiently large prime numbers are selected and multiplied together with its product stored, or $n = pq$, where n is also known as the modulus. Another number e less than n is chosen, with the characteristics of being relatively prime to $(p-1)(q-1)$; in other words, e and $(p-1)(q-1)$ only have 1 as the common factor. An additional number d is selected such that $(ed-1)$ is divisible by $(p-1)(q-1)$ where $ed = 1 \text{ mod } (p-1)(q-1)$. In this case, e and d correspond to the public and private exponents respectively while the public key is the pair (n, e) and the private key is (d) .

⁵ RSA, <http://en.wikipedia.org/wiki/RSA>, accessed December 2009

Additionally, public key cryptography (or asymmetric encryption) is implemented with a hashing algorithm⁶ such as Secure Hash Algorithm (SHA-1) or Message Digest 5 (MD-5) to provide an efficient integrity mechanism in e-commerce websites. SHA-1 has emerged as the preferred method when weaknesses were found on MD-5 algorithm⁷. Applied to e-commerce, PKI secures the integrity of posted prices, identification and authentication for a large customer base, confidentiality of customer and transaction information, and non-repudiation to minimize disputes.

Although PKI attempts to solve the man-in-the-middle problem and other cybercriminal acts, the system is not without its flaws. As public key cryptography requires expensive computation particularly for larger data transmissions, RSA is preferred only for exchange keys while a conventional algorithm such as DES is used for the bulk of the content. Additionally, critics argue⁸ that PKI is not essential or does not solve e-commerce security. It has been argued that although a CA handle key management well, consumers cannot necessarily trust a certificate from the particular CA for a particular purpose such as making a micropayment, questioning the essence of trust and authority of CA vendors.

B. Digital Signatures

Based on the public-key encryption method combined with data hashing functions such as MD-5 and SHA-1, digital signatures are implemented to verify the origin and contents of the online transaction, translating to consumers proving their identity to vendors in the transaction and providing non-repudiation features. They address the inherent problem in public key encryption in which all recipients have the public key. Setting the foundation for digital certificates, digital signatures enable the transaction source to be traced and reinforced data integrity during transmission, invalidating the signature if data is tampered before it reaches the destination.

⁶ Sun Microsystems, "Public key infrastructure overview", 2001

⁷ MD5 considered harmful today, <http://www.win.tue.nl/hashclash/rogue-ca/>, accessed December 2009

⁸ Computer Security Journal, Volume XVI, Number 1, "Ten risks of PKI: What you're not being told about public key infrastructure", 2000

Digital signatures are implemented based on the RSA algorithm⁹, and works inversely from encryption. They are generated by encrypting cleartext using the sender's own private key, and decrypted at the recipient side using the sender's public key. Figure 1. Signing data with a hash algorithm shows the signing process incorporating the digital signature into a certificate to produce a digitally-signed file. A one-way hash function, SHA-1 provides a mechanism that simplifies the hash computation from some data but difficult to determine any data from a computed hash value, eliminating the need for a secret key. Signing a hash instead of the whole document results in efficiency as the signature is much smaller in size speed up the hashing process. It also leads to compatibility of the hash function to be converted into the proper format, and integrity of the text since it does not have to be separated in blocks.

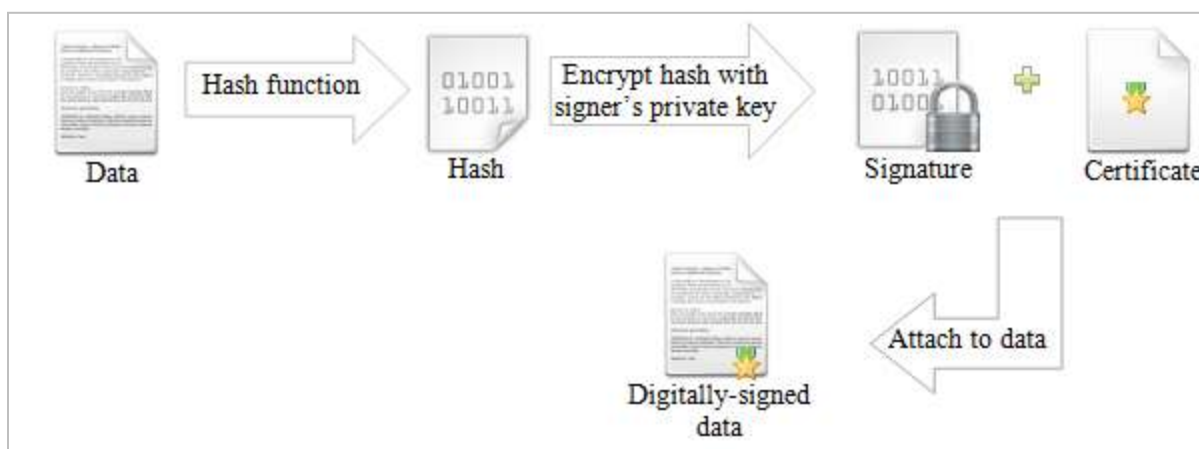


Figure 1. Signing data with a hash algorithm

Despite its hashing strength, digital signatures are still vulnerable against attacks. If the private key is compromised by a third party, the message can be intercepted and signed with another private key, enabling the third party to pose as the original sender. Other known attack models¹⁰ include known message attacks and adaptive chosen message attacks resulting in unreliability of digital signatures. The vulnerabilities can be prevented by using the key exchange method of the public key system. A sender can encrypt the message again with the receiver's

⁹ "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, 21(2): 120-126, 1978

¹⁰ Shafi Glodwasser et al, "A digital signature scheme secure against adaptive chosen-message attacks", 1988

public key before sending it, while the receiver decrypts the message with his or her own private key before encrypting it again with the sender's public key.

C. Digital Certificates

Similar to the concept of a digital passport, digital certificates are files that distinctively identify users and websites to enable confidential and secure communications using digital signatures to associate a public key with the website identity. Typically, the signature is issued and created by a CA. A public-key certificate issued by a CA such as that shown in Figure 2. Digital certificate issued by a CA verifying Amazon.com specifies a validity period and an expired certificate should not be trusted, and always includes the name of the e-commerce website, name of the issuing CA, a serial number, and most importantly, the digital signature of the CA. Before issuing the certificate, the CA would request contact information of the website from a public domain name registrar and verify that the published address matches the email address supplied in the certificate request. A common standard used for defining digital certificates is X.509, which regulates the contents of the certificate before it is signed by a CA¹¹.



Figure 2. Digital certificate issued by a CA verifying Amazon.com

¹¹ An X.509 Certificate, <http://www.planetlarg.net/linux-cluster/technologies/websec-certificate-x509.htm>, accessed December 2009

Field	Value
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	VeriSign Class 3 Secure Server...
Valid from	Wednesday, July 29, 2009 7:...
Valid to	Friday, July 30, 2010 6:59:59 ...
Subject	www.amazon.com, Amazon.c...
Public key	RSA (2048 Bits)

Figure 3. Digital certificate fields and corresponding values

Although digital certificates are widely adopted by major businesses, certificate practices may not be completely secure. Although digital certificates guarantees the uniqueness of the website that users are interacting with, the relationship between the certificate owner, the website operator, and the website content owner may be vague and therefore not guaranteed. Research has shown that authentication and authorization should also be separated as much as possible even though digital certificates accommodate authorization information within their fields¹².

D. Secure Socket Layer (SSL)

Secure Socket Layer protocol is the web standard for authenticating web sites and encrypting the communication channel between users and web servers. Based on the implementation of PKI and digital signatures via web server certificates that enable SSL encryption and authentication, SSL certificates establishes e-commerce trust by performing SSL server authentication and SSL encryption. It uses a private key to encrypt data transferred over the connection, encrypting via 40-bit or 128-bit encryption methods, which is reinforced by SSL certificates (128-bit) for unique website identification.

When a user enters a secured site, the URL changes to “https://” instead of the regular “http://”, which is simply http over an encrypted SSL connection. At SSL server authentication, server certificates verify a web server’s identity, while the web browser checks that the server certificate and public ID are valid and have been issued by a CA. This step is essential during credit card transactions when the user needs to verify the vendor server’s identity. At the SSL encryption stage, a secure channel is established and enables data transmission between the web

¹² Mark Norman et al, “Are personal digital certificates really usable and scalable?”, 2006

browser and server to be encrypted by sender and decrypted by receiver. The transmission is protected and maintains data integrity of private data such as credit card information.

E. Secured e-commerce transaction flow

Combining the various aspects of PKI technology and applying it to an e-commerce website like Amazon.com, consumers are first redirected to an SSL-based checkout page containing product information and any session-based information associated with the purchase. After entering payment information such as credit card information, SSL encrypts the web session to prevent data interception. The user's web browser requests the digital certificate from Amazon.com to verify its authenticity by examining the digital signature on the certificate against a list of CA. After the web server successfully authenticates, the user's web browser generates a unique session key to encrypt data transmission using asymmetric encryption, after which it encrypts the session key with the public key such that only Amazon.com can read the session key, and finally sends it to the server which then decrypts the session key using its own private key.

The web browser then sends a message to Amazon.com server informing that future transmissions will be encrypted with the session key. Responding to this step, the server informs the user's browser that future messages from the server will be encrypted with the session key, after which an SSL-secured session is established. Applying symmetric encryption to encrypt and decrypt transmissions within the secured channel, the transaction is rendered successful. The session key is then eliminated after the established session is ended.

When Amazon.com presented its digital certificate to a user's web browser, which is equipped with a list of certificate authorities and other information for validation purposes, the web browser examines the certificate and acknowledges that it claimed to be for Amazon.com. At this point, if the URL entered by the user does not match the name on the certificate, the browser returns an alert. Consequently, the web browser checks that the certificate was signed by a CA called VeriSign, and having found it on the list of pre-installed CA, will verify the signature from VeriSign, or otherwise issue an alert that the certificate or signature is invalid.

4. External factors affecting e-commerce security

A trust infrastructure sets the foundation of e-commerce transaction activities, but users of these websites have to remain vigilant for red flags. Digital certificate warnings have been shown to be ineffectual as a high majority of users surveyed ignore expiration notices¹³ prompted by the browser, with tech-savvy users more likely to ignore it. Expired certificates could indicate a man-in-the-middle attack and compromise users' information. Additionally, a domain mismatch warning may signal a phishing attack but could sometimes be ignored by users.

Web browsers, the only application known to connect users and e-commerce websites, may expose users to potential risks. Even secure websites are vulnerable to forged security certificates by sophisticated cybercriminals¹⁴ to bypass built-in verification methods found in web browsers without the user warned about the problem. Exploiting SSL technology, the vulnerability enables a forged authentication certificate to display the padlock icon common to a secure website, and is attributed to a weakness in the MD5 algorithm, which is a standard cryptographic function used to verify SSL certificates.

5. Conclusion

E-commerce has become heavily reliant on PKI technology to boost consumer's confidence and safeguard their most fundamental assets—business data and customer's personal information. Public key encryption emerged as superior over private key encryption for online transactions as it eliminates the need for secret key exchange. Combined with the strengths of digital signatures/certificates and the SSL protocol, a consumer's online experience becomes more secure through key establishment and server authentication, reducing the risks associated with online data theft.

Nevertheless, flaws present in these technologies should not make vendors and consumers complacent. Vendors can devise a data security plan to maintain the privacy, integrity, authentication, and non-repudiation of their e-commerce strategies, which may include the implementation of firewalls to protect servers and networks or setting up the Kerberos protocol

¹³ Joshua Sunshine et al, "Crying wolf: An empirical study of SSL warning effectiveness", 2009

¹⁴ Web browser flaw could put e-commerce security at risk, http://news.cnet.com/8301-1009_3-10129693-83.html, accessed December 2009

to minimize insider's threats, among other pertinent policies. Consequently, online consumers should remain aware of their online shopping habits and be alert of anything that may be amiss before completing a purchase.