Cryptography for Enabling E-Commerce

KEYWORDS

G.VENKATESHWARAN

ASSISTANT PROFESSOR, DEPT.OF CS&AF, FACULTY OF SCIENCE AND HUMANITIES SRM UNIVERSITY, KATTANKULATHUR, CHENNAI

INTRODUCTION:

Businesses have increasingly embraced electronic commerce to modernize their operations. E-commerce essentially consists of the provision of products and services over electronic systems, such as the Internet, computer networks, email or mobile phones, and may be applied to various business functions**:** Marketing, Sales, distribution, financial transactions, service and support. The digital world is getting crowded. The number of Web sites has skyrocketed into the millions as companies supplement their traditional merchandising avenues with electronic commerce. As this new medium has become pervasive, companies with an Internet presence have labored to distinguish their Web sites and marketing techniques from the offerings of others. Consumers who purchase goods and services over the Internet want things faster, cheaper, and better. Waiting for a slow Web site to download overly complicated graphics or navigating through clunky computer screens have prompted Internet consumers to switch to user-friendly Web sites. Unlike shoppers in a grocery store or a shopping mall, shoppers on the Internet can dump vendors at the click of a mouse. The rash of security problems on the Internet and the Web demonstrates that lack of trust is limiting the use of the Internet for business and commerce. For the Internet to realize its potential as a medium for information, trade, and entertainment, the public must have confidence that their transactions will be confidential and protected. Whether accessing personal data in on-line public databases or making a credit card purchase, the public must trust that the Internet is a secure place to do business.

With E-commerce service continuously increasing value also is an increasing demand for security enhancing techniques like the secure socket layer (ssc) are available and commonly used, the efforts to protect the privacy of individuals are scarely perpecptible. As e-commerce service also enable the service provider to easily acquire personal data, e.g., the consumption habits of the customers, countermeasures must be taken to protect the primary of customers, who are afraid that their personal data maybe misused or sold. Privacy is important for customers and even concerned about privacy issues. To make e-commerce successful, we need to bring privacy protecting techniques into the applications to guarantee that no misuse can occur.

ELECTRONIC E-COMMERCE:

E-Commerce Is a particular form of e-Business. Electronic business methods enable companies to link their internal and external data processing systems more efficiently and flexibly, to work more closely with suppliers and partners, and to better satisfy the needs and expectations of their customers. Compared to e-Commerce, e-Business is a more generic term because it refers not only to information exchanges related to buying and selling but also servicing customers and collaborating with business partners, distributors and suppliers. E-Business encompasses sophisticated business-to-business interactions and collaboration activities at a level of enterprise applications and business processes, enabling business partners to share in-depth business intelligence, which leads, in turn, to the management and optimization of inter-enterprise processes such as supply chain management. More specifically, e-Business enables companies to link their internal and external processes more efficiently and flexibly, work more closely with suppliers and better satisfy the needs and expectations of their customers.

E-Business encompasses sophisticated business-to-business interactions and collaboration activities at a level of enterprise applications and business processes, enabling business partners to share in-depth business intelligence, which leads, in turn, to the management and optimization of inter-enterprise processes such as supply chain management. More specifically, e-Business enables companies to link their internal and external processes more efficiently and flexibly, work more closely with suppliers and better satisfy the needs and expectations of their customers.

In practice, e-business is more than just e-commerce. While e-business refers to more strategic focus with an emphasis on the functions that occur when using electronic capabilities, e-commerce is a subset of an overall e-business strategy. E-commerce seeks to add revenue streams using the World Wide Web or the Internet to build and enhance relationships with clients and partners and to improve efficiency using the Empty Vessel strategy. Often, e-commerce involves the application of knowledge management systems.

E-business involves business processes spanning the entire value chain: electronic purchasing and supply chain management, processing orders electronically, handling customer service, and cooperating with business partners. Special technical standards for e-business facilitate the exchange of data between companies. E-business software solutions allow the integration of intra and inter firm business processes. E-business can be conducted using the Web, the Internet, intranets, extranets, or some combination of these.

Basically, electronic commerce (EC) is the process of buying, transferring, or exchanging products, services, and/or information via computer networks, including the internet. EC can also be benefited from many perspective including business process, service, learning, collaborative, community. EC is often confused with e-business.

In e-commerce, information and communications technology(ICT) is used in inter-business or inter-organizational transactions (transactions between and among firms/organizations) and in business-to-consumer transactions (transactions between firms/organizations and individuals).

In e-business, on the other hand, ICT is used to enhance one's business. It includes any process that a business organization (either a for-profit, governmental or non-profit entity) conducts over a computer-mediated network.

A more comprehensive definition of e-business is: "The transformation of an organization's processes to deliver additional customer value through the application of technologies, philosophies and computing paradigm of the new economy."

CRYPTOGRAPHY :

Cryptography is the study of information hiding and verification. It includes the protocols, algorithms and strategies to securely and consistently prevent or delay unauthorized access to sensitive information and enable verifiability of every component in a communication.

Cryptography is derived from the Greek words: kryptós, "hidden", and gráphein, "to write" - or "hidden writing". People who study and develop cryptography are called cryptographers. The study of how to *circumvent* the use of cryptography for unintended recipients is called cryptanalysis, or code breaking. Cryptography and cryptanalysis are sometimes grouped together under the umbrella term cryptology, encompassing the entire subject. In practice, «cryptography» is also often used to refer to the field as a whole, especially as an applied science.

Cryptography is an interdisciplinary subject, drawing from several fields. Before the time of computers, it was closely related to linguistics. Nowadays the emphasis has shifted, and cryptography makes extensive use of technical areas of mathematics, especially those areas collectively known as discrete mathematics. This includes topics from number theory, information theory, computational complexity, statistics and combinatory. It is also a branch of engineering, but an unusual one as it must deal with active, intelligent and malevolent opposition.

One basis for privacy are blind signatures, a cryptographic protocol invented by chaum. Blind signatures allow to receive a digital signatures from an authority on any message or document. So that the authority is neither able to recognize the signed document later nor can the authority determine the content of the document to be signed.

Blind signatures are a cryptographic tool that is well suited to enable privacy protecting e-commerce applications. In encryptographic frameworks however, only the major cryptographic tools like digital signatures and ciphers are provided as abstract tools.

Cryptographic protocols, especially blind signatures, are not available in those frameworks. We strongly believe that a modular framework is necessary for all cryptographic tools for enabling the immediate replacement of an algorithms in the case of its possible breakdown.

Base Cryptography Functions:

Base cryptographic functions provide the most flexible means of developing cryptography applications. All communication with a cryptographic service provider (CSP) occurs through these functions.

A CSP is an independent module that performs all cryptographic operations. At least one CSP is required with each application that uses cryptographic functions. A single application can occasionally use more than one CSP.

If more than one CSP is used, the one to use can be specified in the CryptoAPI cryptographic function calls. One CSP, the Microsoft Base Cryptographic Provider, is bundled with the CryptoAPI. This CSP is used as a default provider by many of the CryptoAPI functions if no other CSP is specified.

Each CSP provides a different implementation of the cryptographic support provided to CryptoAPI. Some provide stronger cryptographic algorithms; others contain hardware components, such as smart cards. In addition, some CSPs can occasionally communicate directly with users, such as when digital signatures are performed by using the user's signature private key.

Base cryptographic functions are in the following broad groups:

- Service Provider Functions
- Key Generation and Exchange Functions
- Object Encoding and Decoding Functions
- Data Encryption and Decryption Functions
- Hash and Digital Signature Functions.

CRYPTOGRAPHIC PROCESS BASIC PROCESS:

M is the original message. K enc is encryption key 'M' is the scrambled message 'K' dec is decryption key. It is difficult to get M just by knowing 'M'. E and P are related such that E(k enc, M) = 'M'

D(K dec,M)='M'

D(K dec,E (K enc,M)=M

Plain text – 'M' cipher text – 'M' original plain text – 'M'

Decryption function – D

Encryption Funtion – E.,

So how does cryptographic process work? The idea is rather simple, let's say you have plain text M. By providing the encryption key and the encryption function, you get cipher text M. The cipher text can be decrypted using decryption function and a decryption key and the result is the original text. In cryptographic process the mathematical property is such that it is practically impossible to derive M from M unless the key is known.

ENCRYPTION AND DECRYPTION:

Encryption is the conversion of data into a form, called a cipher text, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

The use of encryption/decryption is as old as the art of communication. In wartime, a cipher, often incorrectly called a code, can be employed to keep the enemy from obtaining the contents of transmissions. (Technically, a code is a means of representing a signal without the intent of keeping it secret; examples are Morse code and ASCII.) Simple ciphers include the substitution of letters for numbers, the rotation of letters in the alphabet, and the "scrambling" of voice signals by inverting the sideband frequencies. More complex ciphers work according to sophisticated computer algorithms that rearrange the data bits in digital signals.

In order to easily recover the contents of an encrypted signal, the correct decryption key is required. The key is an algorithm that undoes the work of the encryption algorithm. Alternatively, a computer can be used in an attempt to break the cipher. The more complex the encryption algorithm, the more difficult it becomes to eavesdrop on the communications without access to the key.

Encryption/decryption is especially important in wireless communications. This is because wireless circuits are easier to tap than their hard-wired counterparts. Nevertheless, encryption/decryption is a good idea when carrying out any kind of sensitive transaction, such as a credit-card purchase online, or the discussion of a company secret between different departments in the organization. The stronger the cipher -- that is, the harder it is for unauthorized people to break it -- the better, in general. However, as the strength of encryption/decryption increases, so does the cost.

In recent years, a controversy has arisen over so-called strong encryption. This refers to ciphers that are essentially unbreakable without the decryption keys. While most companies and their customers view it as a means of keeping secrets and minimizing fraud, some governments view strong encryption as a potential vehicle by which terrorists might evade authorities.

These governments, including that of the United States, want to set up a key-escrow arrangement. This means everyone who uses a cipher would be required to provide the government with a copy of the key. Decryption keys would be stored in a supposedly secure place, used only by authorities, and used only if backed up by a court order. Opponents of this scheme argue that criminals could hack into the key-escrow database and illegally obtain, steal, or alter the keys. Supporters claim that while this is a possibility, implementing the key escrow scheme would be better than doing nothing to prevent criminals from freely using encryption/decryption.

The following points are related to that when will you encrypt a data?

Encrypt data that moves

Data moving from one trust zone to another, whether within your organization or between you and an external network, is at high risk of interception. Encrypt it.

Data moving from trusted portions of the network to end-user devices over wireless LANs almost always at high risk. Encrypt it.

Encrypt for separation of duties when access controls are not granular enough

For flat file storage, encrypting a spreadsheet file in a department share provides an additional layer of separation. Only employees with the right authorization have access. Application access controls protecting databases often do not provide granular control to strictly enforce need-to-know or least privilege. Using database solutions with field- and row-level encryption capabilities can help strengthen weak application-level access controls.

Encrypt when someone tells you to

And then there are local, state, and federal regulations. Couple regulatory constraints with auditor insistence, and you often find yourself encrypting because you have to. This type of encryption is often based on generalizations instead of existing security context. For example, just because you encrypt protected health information does not mean it is secure enough… but it satisfies HIPAA requirements.

Encrypt when it is a reasonable and appropriate method of reducing risk in a given situation

This law is actually a summary of the previous three. After performing a risk assessment, if you believe risk is too high because existing controls do not adequately protect sensitive information, encrypt. This applies to risk from attacks or non-compliance.

How to Encrypt

Implementing secure and operationally efficient encryption solutions is not easy, and maintaining them adds to total cost of ownership (TCO). Further, data is often spread between internal and cloud-based storage. Any solution you select must support all current and future data storage and transport characteristics.

One approach is to purchase a system, install it in your data center, and assign in-house staff to manage it. While this might seem like a good idea, the opportunity costs are high. As with most commodity security controls, encryption solutions can be managed by anyone; they do not require the special knowledge of the business possessed by you or other members of the internal security and LAN teams. Your skills are better applied to projects, assessments, and other business critical activities. Consequently, consider outsourcing encryption and key management.

Encryption-as-a-Service vendors provide all the services and protection we discussed, including key management and encryption according to business policy. In addition to encrypting the data center, they can also serve as a third-party that ensures all data housed by your other cloud service providers is managed by encryption policies as if it were in your own data center. Figure 7-18 is an example of an EaaS solution.

The ES provider does not house your data, only your keys. Your in-house administrator, via a Web interface, performs configuration of encryption policies and subject access. Software as a service or storage as a service providers have no access to data while at rest. Finally, the "cloud" can also mean your own data center.

Whether in house or outsourced, make sure your centralized encryption solution meets the following requirements:

- Central storage, management, protection, and management of keys
- Enforcement of your data encryption policies across all relevant data, wherever it is in your network or in the cloud
- Granular access to policy and key management functions based on separation of duties and least privi-

lege

- Publicly known, tested, and unbroken ciphers used for all encryption

CODING AND DE-CODING:
In computers, encoding is the process of putting a sequence of characters (letters, numbers, punctuation, and certain symbols) into a specialized format for efficient transmission or storage. Decoding is the opposite process -- the conversion of an encoded format back into the original sequence of characters. Encoding and decoding are used in data communications, networking, and storage. The term is especially applicable to radio (wireless) communications systems.

The code used by most computers for text files is known as ASCII (American Standard Code for Information Interchange, pronounced ASK). ASCII can depict uppercase and lowercase alphabetic characters, numerals, punctuation marks, and common symbols. Other commonly-used codes include Unicode, Bin Hex, Uuencode, and MIME. In data communications, Manchester encoding is a special form of encoding in which the binary digits (bits) represent the transitions between high and low logic states. In radio communications, numerous encoding and decoding methods exist, some of which are used only by specialized groups of people (amateur radio operators, for example). The oldest code of all, originally employed in the landline telegraph during the 19th century, is the Morse.

The terms encoding and decoding are often used in reference to the processes of analog-to-digital conversion and digital-to-analog conversion. In this sense, these terms can apply to any form of data, including text, images, audio, video, multimedia, computer programs, or signals in sensors, telemetry, and control systems. Encoding should not be confused with encryption, a process in which data is deliberately altered so as to conceal its content. Encryption can be done without changing the particular code that the content is in, and encoding can be done without deliberately concealing the content.

Encryption and Its Application to E-commerce:
Realize the major concerns in e-commerce are **confidentiality, integrity, authenticity, and non-repudiation**.

Understand major difference the public key encryption from symmetric key encryption is that it used two keys - public key and private key. This provides great convenience in key deployment and other security service features.

Know how confidentiality, integrity and authenticity services are provided using a public key encryption scheme, such as RSA.

Know what digital signature (DS) is and how to create a DS.

Add knowledge from 3 and 4 together you will understand how a workable authentication and secure transmission system can be implemented

Understand that we need a trusted third party (TTP) to issue digital certificate. This TTP is a certificate authority (CA). CA uses its own private key to send the digital certificate to users for authentication purposes.

Know that e-commerce is mainly based on the web, so that we need secure socket layer (SSL) and S-HTTP to secure data transmissions. Also we need security electronic transaction (SET) for payment transactions.

Cryptographic Algorithms
Various types of cryptographic systems exist that have different strengths and weaknesses. Typically, they are divided into two classes; those that are strong, but slow to run and those that are quick, but less secure. Most often a combination of the two approaches is used (e.g.: SSL), whereby we establish the connection with a secure algorithm, and then if successful, encrypt the actual transmission with the weaker, but much faster algorithm.

Symmetric Cryptography
Symmetric Cryptography is the most traditional form of cryptography. In a symmetric cryptosystem, the involved parties share a common secret (password, pass phrase, or key). Data is encrypted and decrypted using the same key. These algorithms tend to be comparatively fast, but they cannot be used unless the involved parties have already exchanged keys. Any party possessing a specific key can create encrypted messages using that key as well as decrypt any messages encrypted with the key. In systems involving a number of users who each need to set up independent, secure communication channels symmetric cryptosystems can have practical limitations due to the requirement to securely distribute and manage large numbers of keys.

Common examples of symmetric algorithms are DES, 3DES and AES. The 56-bit keys used in DES are short enough to be easily brute-forced by modern hardware and DES should no longer be used. Triple DES (or 3DES) uses the same algorithm, applied three times with different keys giving it an effective key length of 128 bits. Due to the problems using the DES alrgorithm, the United States National Institute of Standards and Technology (NIST) hosted a selection process for a new algorithm. The winning algorithm was Rijndael and the associated cryptosystem is now known as the Advanced Encryption Standard or AES. For most applications 3DES is acceptably secure at the current time, but for most new applications it is advisable to use AES.

Asymmetric Cryptography (also called Public/Private Key Cryptography)
Asymmetric algorithms use two keys, one to encrypt the data, and either key to decrypt. These inter-dependent keys are generated together. One is labeled the Public key and is distributed freely. The other is labeled the Private Key and must be kept hidden.

Often referred to as Public/Private Key Cryptography, these cryptosystems can provide a number of different functions depending on how they are used.

The most common usage of asymmetric cryptography is to send messages with a guarantee of confidentiality. If User A wanted to send a message to User B, User A would get access to User B's publicly-available Public Key. The message is then encrypted with this key and sent to User B. Because of the cryptosystem's property that messages encoded with the Public Key of User B can only be decrypted with User B's Private Key, only User B can read the message.

Another usage scenario is one where User A wants to send User B a message and wants User B to have a guarantee that the message was sent by User A. In order to accomplish this, User A would encrypt the message with their Private Key. The message can then only be decrypted using User A's Public Key. This guarantees that User A created the message Because they are then only entity who had access to the Private Key required to create a message that can be decrcrypted by User A's Public Key. This is essentially a digital signature guaranteeing that the message was created by User A.

A Certificate Authority (CA), whose public certificates are installed with browsers or otherwise commonly available, may also digitally sign public keys or certificates. We can authenticate remote systems or users via a mutual trust of an issuing CA. We trust their 'root' certificates, which in turn authenticate the public certificate presented by the server.

PGP and SSL are prime examples of a systems implementing asymmetric cryptography, using RSA or other algorithms.

E-commerce Based on Pretty Good Privacy:
I Authentication: Validates the identity of machines and users.

II. Encryption: Encodes data to guarantee that information cannot be viewed by unauthorized users or machines.

III. Digital signing: Provides the electronic equivalent of a handwritten signature and also enables enterprises to verify the integrity of data and determine whether it has been tampered with in transit.

IV. Access control: Determines which information a user or application can access and which operations it can perform once it gains access to another application also called authorization.

CONCLUSION:

Privacy, Integrity, Confidentiality and non-repudiation are main security dimension to protect E-Commerce transactions against threats. These objectives are achieved by cryptography functions and techniques. When customers and merchants perform a transaction over internet. The protection of information against security threats is a major issue. During sending the sensitive information, the data must be protected from unauthorized access to maintain its privacy and integrity.

REFERENCE 1. M. Abe and T. Okamoto. Provably secure partially blind signatures. In Advances in Cryptology — CRYPTO 2000, volume 1880 of Lecture Notes in Computer Science, || 2. Fiego G.Milhil and V.Withelm. © Springer.Verlag Berlin Heidelberg 2001. || 3. Cryptography and E-commerce written by A.Wiley Tech Brief. || 4. Magazines and Internet sites.. |