Quantum cryptography integration

B.Giridhar
Associated Professor, Sri Venkateswara College of Engineering &Tecnology, Srikakulam

Abstract
Today, e-commerce services became more popular on the Internet and the web. Network security is extremely essential for e-commerce services, and it is always the key to the success of e-commerce (e-commerce). In this article, we address various security problems concerning both the conventional and the new generation e-commerce model, such as P2P authentication, authorization, non-repudiation, and integrity. By examining the key characteristics of P2P e-commerce, we summaries several trust model design concepts in e-commerce. We provide a comprehensive overview of network security problems relating to e-commerce and e-commerce applications, and offer a related e-commerce security research framework. In contrast with other security approaches, we think that as long as security concerns are properly handled, P2P e-commerce will achieve tremendous success on future e-commerce marketplaces.

Keywords - Network Security, P2P Model, E-Commerce Security.

1. Introduction

Security has become one of the most significant problems that must be addressed before electronic trade is successful (e-commerce). The cheap cost and large internet accessibility of companies and consumers has triggered a revolution in e-commerce, and an e-commerce application may handle one or many stages of a normal commercial transaction. For example, five stages of a commercial transaction may be distinguished [1]. Firstly, the seller offers particular products or services (information). Secondly, the client may submit the request online according to this offer. Third, the consumer makes a payment and the merchant provides the customer with the products or services. Payment management may include many methods such as internet banking, the post office, delivery cash (C.O.D) etc[2]. Many businesses take use of e-commerce possibilities and many more are anticipated to follow. Examples include online shopping, online banking and distant learning, online games, virtual casinos, Pay TV and video-on-demand services.

Many companies and consumers are still hesitant about e-commerce, and security concerns are frequently mentioned as the only major obstacle. This erosion of confidence in online exchanges is driven by ongoing reports of hacker assaults on e-commerce sites and misuse of customer privacy[3].

In this report, we address several security concerns with e-commerce, particularly the trust model employed in the new e-commerce generation (P2P e-commerce). First of all, we cover more current technologies and some fundamental terminology in the remainder of this article. Next, we sum up several trust model design concepts in the conventional e-commerce and P2P e-commerce models. We are hoping that these principles will assist to build a rich and thriving e-commerce platform based on conventional or innovative P2P technology.

2. Security and Web Service

2.1 Web services Web services

The Web Service is a fresh new distributed SOA (Service Oriented Architect) computing model composed of three members and three fundamental activities. The 3 players are the service provider, the service applicant and the service broker. Publishing, searching and binding are the three fundamental activities. All of them operate on and describe the component and software module of the web service[4]. The web service SOA framework is illustrated in Figure 1.

2.2. Web service security specification

The (web services security) WS-Safety, issued jointly by Microsoft, IBM and Verisign[5], is currently the most approved and comprehensive Web service security standard. It is the basis of the security of the Web service and includes generally recognized security concepts, mechanisms and technological support. The aim of WS-Security is to guarantee that data processing with application programmed via web service is complete and private, and to prescribe the extension and message header for SOAP. The WS-Security brings together many security models, settings and techniques. It is one of the basic service-oriented requirements. Any system may guarantee that it is mutually compatible with others through its platform and language-independent approach.

2.3. Security Client Issues

From the perspective of view of the user, customer security is usually the most important issue. Customer safety generally involves the use of conventional computer security technologies such as appropriate identification and permission of the user, access control and anti-virus protection. The customer may also demand server authentication and rejection of reception with respect to communications services. Furthermore, some applications may need anonymity (e.g., anonymous browsing on the Web).

The data study of popular online banks [6] indicates that online banking customer-side security protection has to be improved. Most banks are susceptible to virus and cyber assaults using a single cypher security configuration method. One of the key aspects of internet banking is that it can always, everywhere and anyhow provide secure and customized client service. The online banking transaction will fail without adequate security protection. The weakest component of internet banking service providers' customer side safety protection [7]. The use of encryption to offer online transaction authentication and privacy, strong cryptography, and access control, integrity and accountability for transaction authorization, is the foundation.

2.4. Security issues on the server side

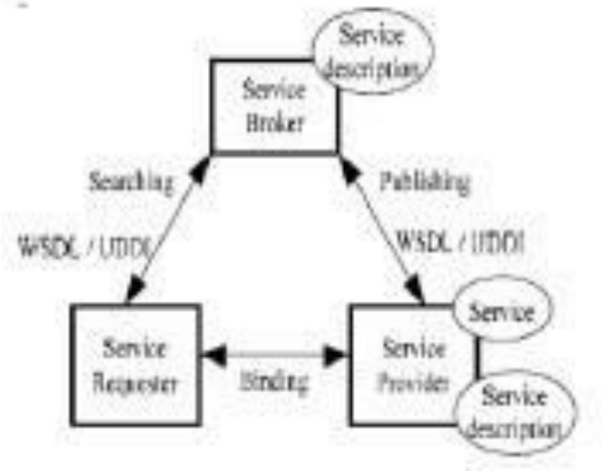
In contrast, server security is usually the main issue from the point of view of the service provider. Security on the Server side needs appropriate customer identification and authorization, origin non-repudiation, sender anonymity (e.g. Web anonymity), audit trail and accountability along with dependability and availability. Figure 2 shows the basic server-side security mechanism.

2.5. Security Transaction Issues

For both the client and the server, transaction security is equally essential. Security of transactions needs different security services, such as authentication of data, access control, confidentiality of data, integrity of data, and non-repudiation services[4]. In addition, transaction anonymity assurances may also be required for some applications. Figure 3 illustrates the basic online banking system data procedure.

3. Existing security technologies for e-commerce

There are a lot of helpful solutions available for e-commerce security but are not well-known or widely dispersed in major software projects. This project will finish, transfer and disseminate a number of current security technology to improve its impact on e-commerce security. Several network security technologies have been developed and used in the past. Network security technologies often include access control and communication safety in addition to physical security measures, such as dedicated communication connections and mechanical locking



.

Fig. 1. Web service framework

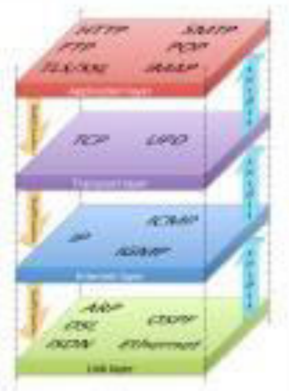


Fig. 2. General security mechanism on the server side.

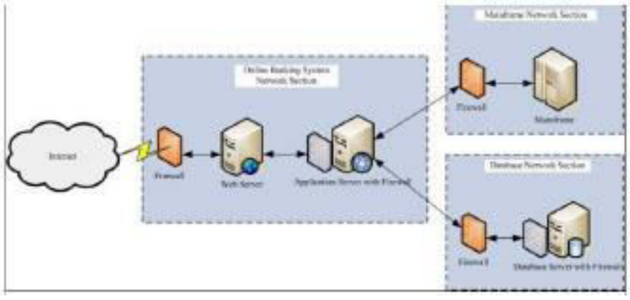

Mainframe Network Section
Online Banking System Network Section
Internet
Firewall
Web Server
Application Server with Firewall
Firewall
Mainframe
Database Network Section
Firewall
Database Server with Firewall

Fig. 3. General online banking system schematic

3.1. Control of access

The first and most apparent issue for network security concerns access control. In the area of physical safety, the word access control refers to the practise in which authorised people limit entry into the property, building or room. A person (guard, bouncer or receptionist) may accomplish physical access control, either by mechanical means such as locks and key, or by technologic methods such as a card access system.

Several technologies are available to restrict access to intranet and internet resources. Authentication, authorisation and audit are included in the access control. It also incorporates such safeguards as biometric scans and metal locks, secret routes, digital signatures, encryption, social obstacles, and human- and automated surveillance. The entities who may execute actions on the system are termed subjects in every access control model, while the entities which represent resources to which access can be regulated are named objects. Sujets and objects should both be regarded as software and not as human users. A human user may affect the system only via the software entities he or she controls. While some systems associate topics with user IDs such that every process launched by a user is authorised by default, this level of control is not sufficiently fine-grained to fulfil the principle of least privilege. Access control systems offer critical identification and authentication (I&A), permission and accountability services where:

1) Identification and authentication: identify who may log in to a system and associate people with software topics which may be controlled by login;

2) Authorisation: what a subject can do;

3) Accountability: indicates what the subject (or all user-related topics) performed.

In summary, access control techniques and related safety measures for many access control systems are well known and extensively used [3].

3.2. Security Communication

Communications security (COMSEC) means that steps and monitoring are made to deny unauthorised people information deriving from telecommunications, ensuring the safety and physical safety of such telecommunications equipment.

1) Crypto security: the communications security component resulting from the supply and appropriate usage of technically competent cryptosystems. This involves the secrecy and validity of the communication.

2) Emissions Security (EMSEC): protection arising out of all actions taken to deny information of value to unauthorised people that may arise from intercepting, analysis of the compromise emanations from cryptoequipment, computers and telecommunication networks.

(3) Physical safety: a communications security component which arises from all physical precautions required for the safeguarding of sensitive equipment, material and records by unauthorised people.

4) Transmission safety (TRANSEC): a communication security component resulting from the use of procedures to safeguard transmissions against interception and use by methods other than cryptanalysis (e.g. frequency hopping and spread spectrum).

4. Classical techniques of cryptography

Cryptography is the act of converting plain text or original information into an incomprehensible form (cookie) so that they may be sent through unsafe channels or communications. The procedure is controlled by a data string (key). Anyone who holds the encrypted text while on the unsafe channel should have the proper key to retrieve the original information. This key is believed to be the authorised receiver. [4] Cryptography is a study of message transmission techniques in a disguised form in order to delete the disguised message only to destinations. It is the skill of transforming the message into various forms, such that no one can read them without the "key." You may transform the message using 'code' or 'cypher.' Two major classes originate from Cryptosystems:

4.1 Asymmetric encryption

The issue of key distribution is addressed in asymmetrical cryptography. It utilises a pair of encryption keys as illustrated in figure 1: a public key, which encrypts data, and a private or secret key matching to the decryption process. You broadcast your world's public key and keep your private key hidden. Anyone who has a public key
copy may then encrypt information that is readable only.

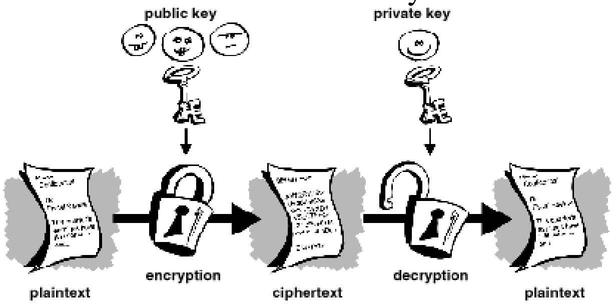


Figure 4: Asymmetrical encryption

4.1 Symmetric encryption

In symmetric encryption, also known as a secret key or a symmetrical key, a single key is utilised in encryption as well as decryption. [5] Figure 2 illustrates symmetrical encryption by encrypting and decrypting plain text with the same password (private key). This encryption has the drawback of the sender and receiver's private key dissemination.

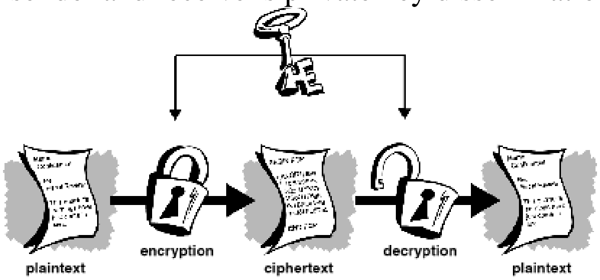


Figure 5: Cryptography of symmetry

There are a number of drawbacks to classic cryptographic methods. Quantum cryptography is done:

5. Quantum encryption

Quantum encryption consists of two words: Quantum and Cryptography. Quantum is a tiny discreet amount of physical property a system may contain and cryptography allows sensitive information to be stored or sent across insecure networks such that none other than the intended receiver can read it. Quantum cryptography thus uses the quantity for cryptographic purposes. Quantum Cryptography is built on and enhances traditional techniques via the use of quantum phenomena. [6] In quantum cryptography, a quantum key distribution (QKD) is used to generate a secret key between two parties utilising the quantum channel and an authenticated classical channel, as shown in figure: 3. The private key is then used to encrypt communications transmitted via an uncertain classic channel (such as a conventional internet connection). Modern cryptosystems utilise quantum cryptography which ensures the key is safe in quantum mechanics without condition.

Heisenberg's principles of uncertainty, Wave/Part duality, Qubits, no cloning theorem, for instance. The Uncertainty principle of Heisenberg says that the more exact one attribute is measured, the less accurately the other can be measured. Quantum cryptography offers unconditional security using this concept effectively. In photon polarisation, the notion of Wave/Particle Duality is utilised. A qubit or a quantum bit is a quantity of information. Like a bit of a qubit, a qubit may maintain these two bits in superimposition status. The no-cloning theorem indicates that a potential eavesdropper can not intercept the measurement and remit a photon without adding a substantial and noticeable signal mistake. This means that two people - the sender and recipient, often referred to as "Alice" and "Bob" - may exchange information and detect the temperature in the communication channel. The key acquired by employing quantic encryption then may be used with any selected encryption method, which can be sent over a normal communication channel to encrypt and decode a message. When the secret key using Quantum encryption is created, it may be used in conjunction with conventional methods such as the former pad to transmit meaningful information in total confidentiality. In QKD, two parties, Alice and Bob, acquire and measure certain quantum states. A QKD system is composed of a quantum channel and a traditional channel. The quantum channel is used for just transmitting Qubits (single photons) and must be a transparent visual route. A typical IP channel may be the classical channel. The key generation in QKD is done via communicationquantum canals[3]. quantum channels. Through conventional channels, they communicate to identify which of their findings might lead to secret key bits. QKD[9] systems produce fresh private keys continuously and randomly that both sides automatically share.

A affected key can only decode tiny quantities of encoded information in a QKD system, since the private key may be changed every second or even constantly. Each photon is encrypted with a little value of 0 or 1 to create a secret key from a stream of single photons, usually by a photon in some overlay, such polarisation.

The photons are produced as light pulses by a standard laser so weak that most pulses do not emit photons. This means of communication may generate genuine random and secret keys that can subsequently be utilised for the creation of appropriate keys using traditional cryptographic techniques.

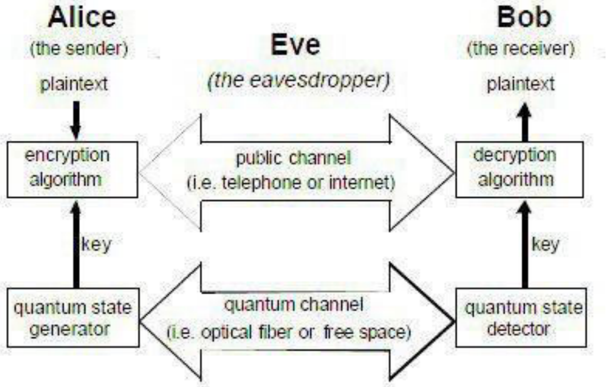


Figure 3: Cryptography of quantities

6. Quantum Cryptography Protocols

A quantum (cryptographic) protocol is a process of data transfer that uses quantum phenomena to guarantee safe transmissions. Initially, quantum protocols such as BB84 were designed for cryptographic keys exchange alone. If perfect cryptography, such as a one-time pad, is used to exchange cryptographic keys, the keys are safe. A traditional cryptography using these keys may then be used to secretly transmit data. Indeed, after the keys are swapped, a classic utilised. This implies that cryptography is probably impenetrable. To date, the three major quantum cryptography methods suggested are:

6.1 Protocol BB84

BB84 was created by Charles Bennett and Gilles Brassard in 1984 for a quantum distribution system. It is the first protocol of quantum cryptography. The protocol is provably safe, depending on the quantum feature that data gain is feasible only at the cost of disrupting the signal if the two states we attempt to differentiate are not orthogonal. It is typically described as a technique of securely transmitting a private key for one-time pad encryption from one party to another.

6.2 Protocol E91

The Ekert method utilises intertwined photon pairs. These may be made by Alice, Bob and some source, like Eve eavesdropper, which is independent from both. The photons are distributed such that Alice and Bob each get one photon per pair.

The system depends on two interlocking characteristics. Firstly, the entangled states correspond precisely in that when Alice and Bob measure both whether their particles are polarised vertically or horizontally, they will always have a 100 percent chance of the identical response. The same applies if both measure any additional (orthogonal) complimentary polarizations. The specific outcomes are entirely random, though; Alice cannot anticipate whether vertical polarisation or horizontal polarisation will occur. Secondly, any effort to eavesdrop these correlations would undermine Alice's and Bob's detection of them.

6.3 Protocol BB92

Shortly after the BB84 protocol was released, Charles Bennett recognised that two orthogonal bases for encoding and decoding should not be used. Instead, a single non-orthogonal basis may be utilised without compromising the protocol's security against eavesdropping. This concept is utilised in the BB92, which is the same as the BB84 protocol. The main change in B92 is that just two states are needed instead of the potential four polarisation states in BB84.

As in Figure 3, 0 may be stored in the rectilinear base as 0 degrees and 1 can be encoded in a diagonal basis as 45 degrees. Like the BB84, Alice sends Bob a string of photons packed with random bits, but this time Alice choose which bases she needs to utilise. Bob still selects a measuring basis randomly, but he won't measure anything if he chooses the incorrect foundation; a condition in quantum physics known as the erasure. After each bit, Bob may only inform Alice whether or not he has measured it properly.

7. Conclusion

A lot of research is taking on on e-commerce security and numerous security products and e-commerce systems are being created and commercialised. It is essential to highlight in this scenario that security is a system feature of e-commerce. The greatest thing we can do is demonstrate that a certain system is resistant to a number of well-known assaults. This article has further addressed security problems connected to P2P e-commerce authentication, licencing, secrecy, non-repudiation and trust model. The future P2P e-commerce is summarised as follows:

I The conventional technique of authentication is based on the identity to offer security or access control methods; in addition, classic encryption and authentication algorithms need a high degree of computer power. Therefore, P2P e-commerce may concentrate on how to enhance the authentication mechanism and optimise the conventional encryption and authentication method.

ii) Effective models of trust may improve user confidence in P2P e-commerce in comparison with the conventional approach specified in this article.

iii) P2P e-commerce problems linked to security should be studied thoroughly in contrast to conventional methods.

Security engineering thus includes making sure things do not fail in the face of a clever and malevolent opponent who induces defects exactly at the wrong moment and in exactly the wrong manner. Note also that safety is orthogonal to usefulness. This is represented in some standards for assessment and certification like the ITSEC or the Common Criteria[4]. Just because a thing works correctly doesn't imply it's safe. Likewise, it doesn't imply it is useful just because a product is secure. Contrary to functionality, security is not apparent to the user and is especially difficult to sell (the automobile industry has the same problem). Bad cryptography, for example, looks like excellent encryption, and the difference is hard to detect (even for an experienced expert). Instead of the present state of mathematical or computational methods, quantum cryptography promises to revolutionise secure communication via security based on basic principles of physics. There are devices to implement such techniques and the performance of demonstration systems is constantly increased. In the next several years or months such systems may start encrypting some of the government and industry's most important secrets.

References

[1] Yuan sen. E-Bunsiness Security Technology Introduction. Software Publishing, BeiJing. 2009. 2009.

[2] Peng Xinying. Peng Xinying. Research on security of e-bunsiness. Science and technology of Gansu, 2009, 25(2): 43-45.

[3] PENG Feilong. A trust model for XKMS-based e-commerce. Computer Software Applications, 2008, 25(1):140-142.

[4] Qi XIE, ZHAO, Lihong. Security of web services research and implementation. Engineering for Computer Science, 2007, 28(1): 4366-4368.
[5] Zhu Lingxi. Security E-Bunsiness. AtJing. Jiaotong University in Beijing. 2006.
[6] W3C Working Party Note, Web architecture of Web services, http://www.w3c.org/TR/ws-arch, 2004.
[7] IBM,Microsoft,Developerworks/l ibrary/wssecure, 2002. [1.0],http://www.ibm.com /l ibrary/wssecure.
[8] International Journal Network Security & Its pplications (IJNSA), Vol 1, No 2 July 2009, "Quantum key distribution (QKD) and Commodity Security Protocols: Introduction and Integration."
[9] C. Elliott, D. Pearson, and G. Troxel, "Quantum cryptography for practical use," Karlsruhe, Germany: 2003 Applications, technology, architecture and computer communications protocols Conference Proceedings 2003.
[10] ALAN MINK, DBART and S WIESNER, "Subway Advances for Quantum Cryptography"
Crypto.August 1982 Proceedings
[11]
Nelson, B., Phillips, A., Enfinger, F. and Steuart, C. Forensics and Research Guide.
Boston:Thomson Training Technology, 2004.
articles/cryptography/introduction-to-modern.
[12] Charles H. Bennett, Q.I.M. Rearch Division, T.J. Watson Research Center, Yorktown Heights, New York, 10598, QNC.
[13]
"Basic Quantum Cryptography" Gerald Scharitzer Technology University of Vienna, Automation Institute.
[14]
Bennett C H G Brassard S. [1] "Performance of 2 Quantum Core Distribution Protocols" by C.-H. F. Fung, K. Tamaki, and H.-K. Lo; Phys.