IJCAT - International Journal of Computing and Technology, Volume 1, Issue 9, October 2014
ISSN : 2348 - 6090
www.IJCAT.org

Integration of Quantum Cryptography

[1] Santosh Kumar Das, [2] Hari Ram Swamy, [3] B.Giridhar, [4] Mr Chandan Kumar Giri

[1, 2] B.Tech Student

[3, 4] Asst.prof in CSE dept

Abstract - Nowadays electronic commerce services have risen to become more and more popular on Internet and Web environment. Exchange security on network is very important for e-commerce service and it is always the key factor that affects the success of electronic commerce (e-commerce). In this paper, we discuss some security related issues about traditional and new generation of e-commerce model, such as authentication, authorization, non-repudiation, and integrity in P2P model; moreover, we discuss some trust models in P2P e-commerce. By analyzing the main features of P2P e-commerce, we sum up some design principles of trust model in P2P e-commerce. We provide a thorough overview about the network security issues that surround e-commerce and e-commerce applications and propose a corresponding research framework for security in e-commerce. We believe that as long as the security issues are adequately addressed, the P2P e-commerce would achieve great success in the future e-commerce markets in comparison to other security methods.

Keywords **- Communication Security, Network Security, P2P Model, E-Commerce Security**

1. Introduction

Security has become one of the most important issues that must be resolved first to ensure success of electronic commerce (e-commerce). The low cost and wide availability of the Internet for businesses and customers has sparked a revolution in e-commerce and an e-commerce application may address one or several phases of a typical business transaction, and there exist various possibilities to model these phases. For example, a possibility is to distinguish five phases of a business transaction [1]. First, the merchant makes an offer for specific (information) goods or services. Secondly, according to this offer, the customer may submit the request online. Thirdly, the customer makes a payment and the merchant delivers the goods or services to the customer. The handling of the payment may involve many ways, such as online banking, post office, cash on delivery (C.O.D) and so on [2]. Many organizations are exploiting the opportunities offered by e-commerce, and many more are expected to follow. Exemplary applications include online shopping, online banking and distance education, online game and virtual casinos, as well as Pay-TV and video-on demand services.

Many businesses and customers are still cautious about participating in ecommerce, and security concerns are often cited as being the single most important barrier. This loss of trust on exchange online is being fuelled by continued stories of hacker attacks on e-commerce sites and consumer data privacy abuse [3].

In this paper, we discuss some security related issues about e-commerce, especially the trust model that could be used in new generation of e-commerce (P2P e-commerce). In the rest of this paper, firstly, we discuss more recent technology and some basic definition. Next, we sum up some design principles of trust model in traditional e-commerce model and P2P e-commerce. We hope these principles will be helpful in establishing a wealthy and prosperous e-commerce platform based on traditional or new P2P technologies.

2. Web Service and Security

2.1. Web Service

The web service is a brand-new distributed computational model using the SOA (Service Oriented Architect) which composes of three participants and three basic operations. The three participants are the Service Provider, the Service Requester and the Service Broker. The three basic operations are Publishing, Searching and Binding. All these act on the component and software module of the web service and their description [4]. The framework of the SOA of web service is shown in Figure 1.

2.2. Security Specification in Web Service

Nowadays, the most authorized and comprehensive web service security standard is the (Web Services Security) WS-Security published jointly by Microsoft, IBM and

Verisign [5]. It is the foundation of the web service security and it also integrates the commonly accepted security models, mechanism and technical supports. The purpose of WS-Security is to ensure the completeness and confidentiality of the data processing with application programs by web service and to prescribe the extension and message header of the SOAP. The WS-Security combines diverse security models, configurations and technique. It is one of the service-oriented standard specifications. Any system is able to ensure to be mutually compatible with others through the platform and the method independent of language.

2.3. Client-side Security Issues

From the user's point of view, client-side security is typically the major concern. In general, client-side security requires the use of traditional computer security technologies, such as proper user authentication and authorization, access control, and anti-virus protection. With regard to communication services, the client may additionally require server authentication and non-repudiation of receipt. In addition, some applications may require anonymity (e.g., anonymous browsing on the Web).

The data analysis on common online banks in [6] shows that the client side security protection for online banking does need improvement. Most banks use single cipher security setting system is vulnerable to virus and cyber-attacks. One of the important characteristic of online banking is that it can offer safe and personalized customer service anytime, anywhere and anyhow. Without sound security protection will cause online banking transaction fail. Client side safety protection is the weakest part for online banking service providers [7]. The application of encryption to provide authentication and privacy of online transactions, strong cryptography provides the basis for achieving access control, transaction authorization data integrity and accountability.

2.4. Server-side Security Issues

Contrary to that, server-side security is typically the major concern from the service provider's point of view. Server-side security requires proper client authentication and authorization, non-repudiation of origin, sender anonymity (e.g., anonymous publishing on the Web), audit trail and accountability, as well as reliability and availability. The general server-side security system is depicted on Figure 2

2.5. Transaction Security Issues

Transaction security is equally important for both the client and the server side. Transaction security requires various security services, such as data authentication, access control, data confidentiality, data integrity, and non-repudiation services [4]. In addition, certain applications may also require transaction anonymity guarantees. Figure 3 shows the data process of general online banking system.

3. Existing E-Commerce Security Technologies

A number of useful e-commerce security technologies exist but are not well-known or well-distributed in mainline software projects. This initiative will complete, port, and distribute a number of existing security technologies to increase their effect on the security of e-commerce. In the past, several network security technologies have been developed and deployed. In addition to physical security measures, such as dedicated communication links and mechanical locks, network security technologies typically address access control and communication security.

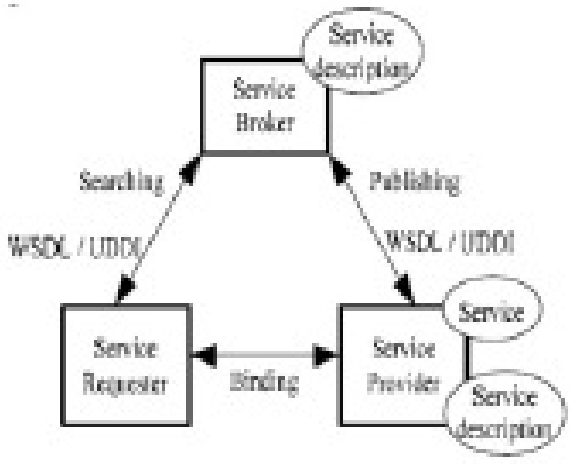

Fig. 1. Framework of web service

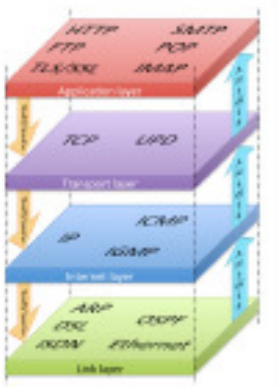

Fig. 2. General server-side security system

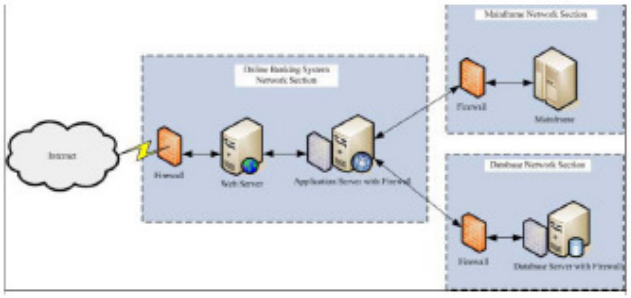

Fig. 3. General diagram of online banking system

3.1. Access Control

The first and most obvious network security concern addresses access control. In physical security, the term access control refers to the practice of restricting entrance to a property, a building, or a room to authorized persons. Physical access control can be achieved by a human (a guard, bouncer, or receptionist), through mechanical means such as locks and keys, or through technological means such as a card access system.

There are several technologies that can be used to control access to intranet and internet resources. Access control includes authentication, authorization and audit. It also includes measures such as physical devices, including biometric scans and metal locks, hidden paths, digital signatures, encryption, social barriers, and monitoring by humans and automated systems. In any access control model, the entities that can perform actions in the system are called subjects, and the entities representing resources to which access may need to be controlled are called objects. Subjects and objects should both be considered as software entities, rather than as human users: any human user can only have an effect on the system via the software entities that they control. Although some systems equate subjects with user IDs, so that all processes started by a user by default have the same authority, this level of control is not fine-grained enough to satisfy the Principle of least privilege. Access control systems provide the essential services of identification and authentication (I&A), authorization, and accountability where:

1) Identification and authentication: determine who can log on to a system and the association of users with the software subjects that they able to control as a result of logging in;

2) Authorization: determines what a subject can do;

3) *Accountability*: identifies what a subject (or all subjects associated with a user) did.

In summary, access control technologies and corresponding security mechanisms are well understood and widely deployed for many access control system [3].

3.2. Communication Security

Communications security (COMSEC) is that measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications security and physical security of COMSEC equipment.

1) Crypto security: The component of communications security that results from the provision of technically sound cryptosystems and their proper use. This includes insuring message confidentiality and authenticity.

2) Emission security (EMSEC): Protection resulting from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from crypto-equipment, automated information systems (computers), and telecommunications systems.

3) Physical security: The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons.

4) Transmission security (TRANSEC): The component of communications security that results from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis (e.g. frequency hopping and spread spectrum).

4. Classical Cryptography Techniques

Cryptography is the process of transforming plain text or original information into an unintelligible form (cipher text) so that it may be sent over unsafe channels or communications. The transformer process is controlled by a data string (key). Anyone getting hold of the cipher text while it is on the unsafe channel would need to have the appropriate key to be able to get to the original information. The authorized receiver is assumed to have that key. [4] Cryptography is study of methods of sending message in disguised form so that only the intended recipients can remove the disguised message. It is the art of converting message into different form, such that no one can read them without having access to 'key'. The message may be converted Using 'code' or a 'cipher'. Cryptosystems come in two main classes:

4.1 Asymmetric Cryptography

In asymmetric cryptography the problem of key distribution is solved. It uses a pair of keys for encryption as shown in figure no. 1: a public key, which encrypts data, and a corresponding private, or secret key for decryption. You publish your public key to the world while keeping your private key secret. Anyone with a copy of your public key can then encrypt information that only you can read.

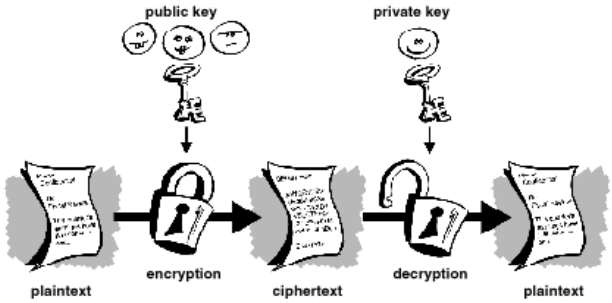

Figure1: Asymmetric Cryptography

4.2 Symmetric Cryptography

In symmetric cryptography, also called secret-key or symmetric-key encryption, [5] one key is used both for encryption and decryption. Figure 2 is an illustration of symmetric cryptography where plain text is encrypted and decrypted using same key (private key). This cryptography has disadvantage of private key distribution among sender and receiver.

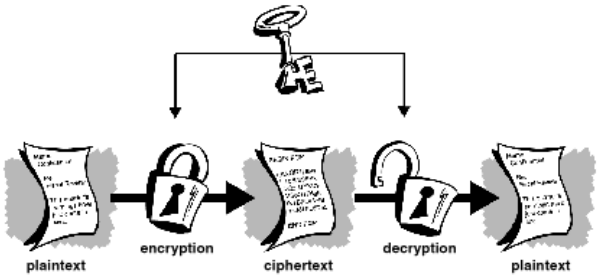

Figure 2: Symmetric Cryptography

Classical cryptographic systems are subject to a number of disadvantages and for that quantum cryptography is done:

5. Quantum Cryptography

Quantum Cryptography is composed of two words: Quantum and Cryptography. Quantum is the smallest discrete quantity of some physical property that a system can possess and Cryptography enables to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient. So, Quantum Cryptography is using the quantum for doing cryptographic tasks. Quantum Cryptography is based upon conventional cryptographic methods and extends these through the use of quantum effects. [6] Quantum Key Distribution (QKD) is used in quantum cryptography for generating a secret key shared between two parties using a quantum channel and an authenticated classical channel as shown in Figure: 3 The private key obtained then used to encrypt messages that are sent over an insecure classical channel (such as a conventional internet connection). Modern cryptosystem uses Quantum Cryptography that makes the key unconditionally secure with quantum mechanics.

For example: Heisenberg's Uncertainty Principle, Wave/Particle duality, Qubits and No cloning Theorem. Heisenberg's Uncertainty principle states that the more precisely one property is measured, the less precisely the other can be measured. Using this principle Quantum Cryptography successfully provides unconditional security. The concept of Wave/Particle Duality is being used in photon polarization. A qubit or quantum bit is a unit of quantum information. Like a bit a qubit can have values 0 or 1, a qubit can retain superposition state of these two bits. The no cloning theorem implies that a possible eavesdropper cannot intercept measure and reemit a photon without introducing a significant and detectable error in the reemitted signal. Thus, it is possible to build a system that allows two parties, the sender and the receiver, commonly called "Alice" and "Bob", to exchange information and detect where the communication channel has been tempered with. The key obtained using quantum cryptography can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can be transmitted over a standard communication channel. Once the secret key using Quantum Cryptography is established, it can be used together with classical cryptographic techniques such as the onetime pad to allow the parties to communicate meaningful information in absolute secrecy. In QKD, two parties, Alice and Bob, obtain some quantum states and measure them. A QKD system consists of a quantum channel and a classical channel. The quantum channel is only used to transmit Qubits (single photons) and must consist of a transparent optical path. The classical channel can be a conventional IP channel. The Key generation in QKD is done by communicating through quantum channels [3].They communicate through classical channel to determine which of their measurement results could lead to secret key bits. QKD [9] systems continually and randomly generate new private keys that both parties share automatically.

A compromised key in a QKD system can only decrypt a small amount of encoded information because the private key may be changed every second or even continuously. To build up a secret key from a stream of single photons,

each photon is encoded with a bit value of 0 or 1, typically by a photon in some superposition state, such as polarization.

These photons are emitted by a conventional laser as pulses of light so dim that most pulses do not emit a photon. This way of communication has the ability to create true random and secret key, which can then be used as seeds to conventional cryptographic methods for the generation of suitable keys.

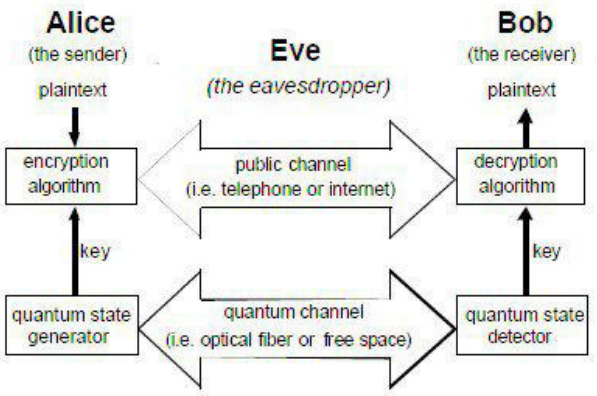

Figure 3: Quantum Cryptography

6. Protocols of Quantum Cryptography

A quantum (cryptographic) protocol is a data communications procedure which employ quantum phenomenon is designed to ensure secure communications. Quantum protocols such as BB84 were originally developed for the exchange of cryptographic keys only. If such a Cryptography that is perfect, such as one time pad, can be protocol is used to exchange cryptographic keys, the keys are guaranteed to be secure. A classical Cryptography that makes use of these keys can then be used to communicate data in secrecy. Indeed, a classical used once the keys have been exchanged. This means that probably unbreakable Cryptography is possible. The three main quantum cryptographic protocols proposed to date are as follows:

6.1 BB84 Protocol

BB84 is a quantum key distribution scheme developed by Charles Bennett and Gilles Brassard in 1984. It is the first quantum cryptography protocol. The protocol is provably secure, relying on the quantum property that information gain is only possible at the expense of disturbing the signal if the two states we are trying to distinguish are not orthogonal. It is usually explained as a method of securely communicating a private key from one party to another for use in one-time pad encryption.

6.2 E91 Protocol

The Ekert scheme uses entangled pairs of photons. These can be created by Alice, by Bob, or by some source separate from both of them, including eavesdropper Eve. The photons are distributed so that Alice and Bob each end up with one photon from each pair.

The scheme relies on two properties of entanglement. First, the entangled states are perfectly correlated in the sense that if Alice and Bob both measure whether their particles have vertical or horizontal polarizations, they will always get the same answer with 100% probability. The same is true if they both measure any other pair of complementary (orthogonal) polarizations. However, the particular results are completely random; it is impossible for Alice to predict if she (and thus Bob) will get vertical polarization or horizontal polarization. Second, any attempt at eavesdropping by Eve will destroy these correlations in a way that Alice and Bob can detect.

6.3 BB92 Protocol

Soon after BB84 protocol was published, Charles Bennett realized that it was not necessary to use two orthogonal basis for encoding and decoding. It turns out that a single non orthogonal basis can be used instead, without affecting the security of the protocol against eavesdropping. This idea is used in the BB92 protocol, which is otherwise identical to BB84. The key difference in B92 is that only two states are necessary rather than the possible 4 polarization states in BB84. As shown in figure 3, 0 can be encoded as 0 degrees in the rectilinear basis and 1 can be encoded by 45 degrees in the diagonal basis. Like the BB84, Alice transmits to Bob a string of photons encoded with randomly chosen bits but this time the bits Alice chooses dictates which bases she must use. Bob still randomly chooses a basis by which to measure but if he chooses the wrong basis, he will not measure anything; a condition in quantum mechanics which is known as an erasure. Bob can simply tell Alice after each bit she sends whether or not he measured it correctly.

7. Conclusion

A lot of research on e-commerce security is going on and many security products and systems of ecommerce are being developed and marketed. In this situation, it is important to note that security is a system property of the e-commerce. The best we can do is to show that a specific system is resistant against a set of well-known attacks. In addition, this paper has discussed some security related issues concerning authentication, authorization, confidentiality, non repudiation, and trust model in P2P e-

commerce. We summarize the future P2P e-commerce as follows:

i) The traditional authentication mechanism is based on identity to provide security or access control methods; in addition, traditional encryption and authentication algorithm require high computing power of computer equipment. Therefore, how to improve the authentication mechanism and optimize the traditional encryption and authentication algorithm may be the focus of P2P e-commerce.

ii) Effective trust models can facilitate in improving user trust in P2P e-commerce versus the traditional method that mentioned in this paper.

iii) Security related issues should be researched extensively for P2P e-commerce in comparison to traditional method.

Consequently, security engineering involves making sure things do not fail in the presence of an intelligent and malicious adversary who forces faults at precisely the wrong time and in precisely the wrong way. Also note that security is orthogonal to functionality. This is reflected in some evaluation and certification criteria, such as the ITSEC or the Common Criteria [4]. Just because a product functions properly does not mean that it's secure. Similarly, just because a product is secure does not mean that it's functional. Unlike functionality, security is not necessarily visible to the user and is particularly hard to market (the automobile industry has the same problem). For example, bad cryptography looks like good cryptography, and it's hard to tell the difference (even for an experienced expert). Quantum cryptography promises to revolutionize secure communication by providing security based on the fundamental laws of physics, instead of the current state of mathematical algorithms or computing technology. The devices for implementing such methods exist and the performance of demonstration systems is being continuously improved. Within the next few years, if not months, such systems could start encrypting some of the most valuable secrets of government and industry.

References

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

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

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

[4] Qi XIE, Lihong ZHAO. Research and realization of web services security. *Computer Engineering and Design*, 2007, **28**(1): 4366-4368.

[5] Zhu Lingxi. *E-Bunsiness Security. BeiJing*. Beijing Jiaotong University. 2006.

[6] W3C Working Group Note, "Web services architecture", http://www.w3c.org/TR/ws-arch, 2004.

[7] IBM,Microsoft,Verisign,"WS-Security Specification1.0",http://www.ibm.com/developerworks/library/wssecure, 2002.

[8] Sheila Frankel and Ray Perlner "Quantum Key Distribution (QKD) and Commodity Security Protocols: Introduction and Integration" International Journal Network Security & Its pplications (IJNSA), Vol 1, No 2, July 2009.

[9] C. Elliott, D. Pearson, and G. Troxel, "Quantum cryptography in practice," Karlsruhe, Germany: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications 2003.

[10] Alan Mink, dbart and S Wiesner, "Quantum cryptography or unforgeable subway tokens Advances in Cryptology"
Proceedings of Crypto.August 1982

[11] Nelson, B., Phillips, A., Enfinger, F., and Steuart, C. Guide to Computer Forensics and Investigations.Boston:Thomson Course Technology, 2004.articles/cryptography/introduction-to-modern.

[12] Charles H. Bennett, "Quantum Cryptography Using Any Two Nonorthogonal States",IBM Rearch Division,T.J. Watson Research Center, Yorktown Heights,New York 10598

[13] Gerald Scharitzer, "Basic Quantum Cryptography" Vienna University of technology, Institute of Automation.

[14] Bennett C H G Brassard S Brei[1] C.-H. F. Fung, K. Tamaki, and H.-K. Lo, "Performance of two quantum keydistribution Protocols," Phys. Rev.vol. 73, 2006.