2011 International Conference on Software and Computer Applications
IPCSIT vol.9 (2011) © (2011) IACSIT Press, Singapore

Study of Security Issues on Traditional and New Generation of E-commerce Model

Seyyed Mohammad Reza Farshchi[1+], Fariba Gharib[2], Reza Ziyaee[3]

[1] Department of Artificial Intelligence, Islamic Azad University, Mashhad Branch.
[2, 3] Department of Business Management Laboratory, Sadjad University, Mashhad, Iran.

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.

[+] Seyyed Mohammad Reza Farshchi. Tel.: +989153081125.
E-mail address: *farshchi@mshdiau.ac.ir.*

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.

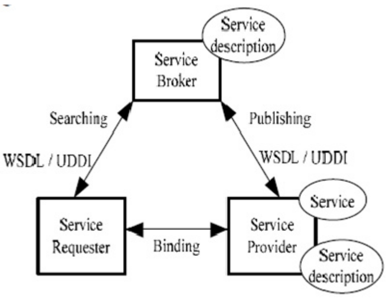

Fig. 1. Framework of web service

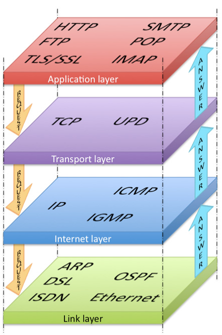

Fig. 2. General server-side security system

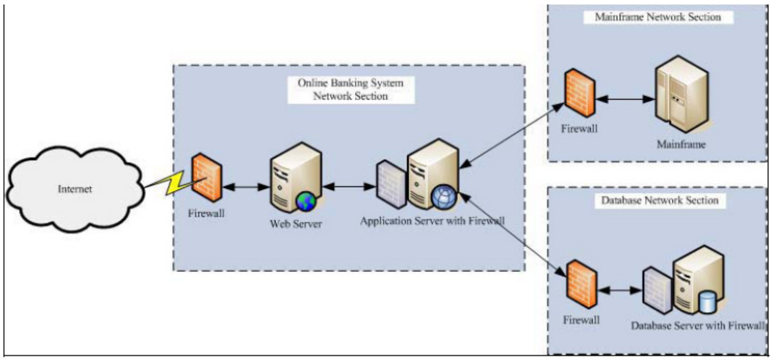
Mainframe Network Section
Online Banking System Network Section
Firewall
Mainframe
Internet
Firewall
Web Server
Application Server with Firewall
Database Network Section
Firewall
Database Server with Firewall

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.

Communications security includes crypto security, transmission security, emission security, traffic-flow 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. P2P E-Commerce

The goal of P2P e-commerce is to present a long perspective on the evolutionary a new, fine grained type of ecommerce on the Internet. In P2P e-commerce, the users are not just "buyers", but "sellers" too.

Trust establishment between strangers is particularly important in the context of e-commerce. In P2P e-commerce, how to build an effective trust model in user nodes and help user nodes to prevent transaction with malicious peers are imperative before P2P e-commerce can be truly realized. Trust plays a very important role in P2P networks for enabling peers to share resources and services credibly, and trust reflects a comprehensive evaluation of one user to another user's behaviors as well as ability.

There are many definitions of trust. In this paper, trust is the confidence of an entity (trustor) on another entity (trustee) based on the expectation that the trustee will perform a particular action important to the trustor, irrespective of the ability to monitor or control the trustee [5]. There are many ways to category trust models [3]:

i) According to *different trust mechanism*, the trust model can be classified into identity-based trust model, role-based trust model, automated trust negotiation model, and reputation based trust model.

ii) According to *collection methods of trust value*, the trust model can be divided into two categories: partially peer reputation model and wholly peer reputation model.

iii) According to *algorithms that compute trust*, the trust model can be classified into different models, such as multi-factor based trust model, Bayesian-based trust model, and neural network based trust model.

5. E-Commerce Security Research Framework

Referring to the additional requirements that address the complexity and availability of cryptographic applications, the anonymity of participating peers, the autonomy of mobile code, and the manageability of trust, the following research framework of security of e-commerce may be derived.

5.1. Complexity

First and foremost, a framework must be developed in which possible attacks against cryptographic primitives (algorithms, protocols, and applications) can be explored and systematically investigated. Note that the coexistence of multiple parties and multiple protocols in an ecommerce application offers new possibilities to attack the systems involved [5]. In addition, provably secure cryptographic primitives must be developed, and it must be clarified what provably secure actually means in this framework. Finally, research must address and elaborate on new security technologies, such as quantum cryptography, and study the implications of evolving technologies, such as quantum computing or DNS computing, to the crypt analytical strength and security of existing cryptographic primitives.

5.2. Anonymity

For certain e-commerce applications, it will be necessary to develop techniques that can be used to provide:

1) *Receiver anonymity services* (e.g., anonymous browsing on the Web);

2) *Sender anonymity services* (e.g., anonymous publishing on the Web);

3) *Transaction anonymity services* (e.g., military applications and stock trade broker systems);

There are several techniques under investigation that can be used to provide the anonymity services mentioned above. These techniques must be further refined and explored in real-world applications. Furthermore, it will be important to study the relationship between anonymity services and other security services, such as access control and peer-entity authentication services.

6. Conclusion

A lot of research on e-commerce security is going on and many security products and systems of e-commerce 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).

7. 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.