e-Commerce and it's Security

Aiman H. Mufti, Saudi Aramco (*muftiah@aramco.com.sa*)

February 11, 2001

Abstract

This paper introduces e-commerce and its primitive framework design. e-Commerce security is the major and the most important issues in e-commerce. Confidentiality, integrity, and availability are the minimum e-commerce security requirements which provided by three different protocols: SSL, S-HTTP, and SET. Each protocol has its own design issues and use also which studied in details in this paper. A comparison study was provided in this paper also.

1. Introduction

Recent growth in Internet usage has prompted attention to a problem of *privacy*. Before, we do not ensure that the messages you send and receive have not been intercepted, read, or modified by somebody since no body really control the Internet. Second, the potential for fraud is far grater.

When the other person on a computer screen, how do you know they hold a valid account? How do you know you can trust a merchant you have never seen? And, how can real merchant feel comfortable accepting a Visa card account number without identification?

Security is the major concern in e-commerce, which is the subject of this paper. Section three of this paper is showing three known e-commerce security protocols applied on Internet these days: S-HTTP, SSL, and SET. In addition, you will find a comparison study between two major e-commerce security protocols: SSL and S-HTTP.

2. *e*-Commerce

It is the ability to do business on-line via the Internet. With Internet based e-commerce, new types of transaction are appear:

- Parties in the transaction such as business, consumers and government
- Things involved such as tangible and intangible good and services.

Also, it enhances the processes of the business and changes the way it delivers services to clients. In contrast, e-commerce comes also with some problems such as authentication and identification.

e-commerce is not just the presence of computer or absence of papers. It implies more, such as:

1- Using a non-proprietary open network, Internet, with its associated security and reliability issues.
2- Free client administration.
3- On going Service availability.
4- Geographically distributed parties.
5- Parties identity without physical contact.
6- Support of off-line contact between parties through email, voice, fax, ..etc.
7- The ability to collect data and parties profiles.

The typical e-commerce business application framework suppose to provide and support complete workflow function, where e-commerce has a massive workflow starts from account opening and end at payment protocol. Also, it should have a useful user interface foundation and service provision. Therefore, it is designed to consolidate three main sub-frameworks, and a service pool:

I. **Object Management Framework**: this is responsible for sorting and retrieving all objects in the application. It also responsible for isolating the application from the underlying database.
II. **Business Logic Framework**: the purpose of this to encapsulate the business rules and process independently of the user interface.
III. **User Interface Framework**: the usage of this framework is to isolate the basic notion of a form from the underlying window system and operating system.
IV. **Generic Service Pool**: This can be called a virtual machine provides services to all other frameworks in a sufficiently abstracted form. So, the services can be implemented in several ways.

3. e-Commerce Security

Security in e-commerce is very important part since communication can be easily intercepted, messages can be inserted, and the absolute identity of involved parties may be uncertain. There is a lack of a consistent and coherent set of protocols to cover the needs of merchants and consumers. However, one should minimize the effects of security failures on cyberspace for reliable electronic commerce systems. Security tries to accomplish the following tasks:

- Confidentiality: Only authorized users have access
- Integrity: Only authorized persons can change your data
- Availability: You can access your data when needed

The design of a complete e-commerce security solution (Hardware or Software) is a significant undertaking. Among other considerations, it needs to consider the following important issues:

1- **Electronic Identification Strategy:** It requires cryptographic security techniques to ensure transaction authentication and choose between secret key cryptography (SKC) MACing (Message Authentication Code) or public key cryptography (PKC) digital signatures.

2- **Level of Security:** The determination of a security level will have impact on the type of electronic identification means given to clients. The choice is between logical securities in software-based authentication, or physical security if a security device is introduced into the picture.

3- **Client Authentication Strategy:** With the PKC digital signatures, this issue is rooted in the PKI security model, and the role of certification authorities (CA). Where with SKC, the foremost options are the manual delivery of cryptographic keys or implied security model suggests the client enrolment.

4- **Confidentiality Requirements:** Even if the critical aspect of e-commerce security is transaction authentication, confidentiality requirements are a significant design issue. This confidentiality requirements issue is independent from the selection of a security model. Obviously, when the confidentiality mechanisms are considered, the selection of SKC or PKC does matter.

3.1 Chip-based Solution

IBM is a bigger provider of e-commerce solutions. They had been looking seriously at a chip-based solution about the time Intel announced it would introduce chip-tracking technology with the Pentium III processor Therefore, IBM developed new chip as standard equipment on the IBM PC 300PL commercial computer and IBM IntelliStation E Pro workstation. The chip enables users to encrypt data from the client system for security purposes or for use in electronic transactions, such as ordering products or signing contracts.

Hardware Design Issues:

Data-scrambling technology typically requires a separate piece of hardware, such as a smart card reader, or relies on cryptography provided with the operating system or third-party software. Using a security chip embedded on a computer's printed circuit board, or motherboard, is an innovation. This technology has the following design issues:

- Users get two layers of security as the system depends on the hard-coded security chip and a user PIN code entered using software.
- Key pairs themselves are never exposed in public because they're managed inside the chip.
- Security mechanism uses the public key, private-key encryption method commonly used for creating digital signatures. Scrambled numbers and characters keys created in matched pairs, are required to open an encrypted document or authenticate a digital signature.
- Offer 256-bit key encryption and 1024-bit signature.

3.2 E-Commerce Security Protocols

3.2.1 Secure Sockets Layer (SSL)

In 1994, Netscape developed its first standard of Secure Socket Layer (SSL) to implement secure environment to exchange the information over the Internet and made it public for implementation in fall 1994. SSL is a security protocol protects communications between any SSL-enabled client and server software running on a network that uses TCP/IP, Gopher, FTP, Telnet…etc.

SSL approach is to add a layer on top of the existing network transport protocol and beneath the application. This approach applied by adding an intermediate step, requiring negotiation of secure transmission options, to the establishment of a network connection. Data flowing between the client and the server on that connection is encrypted before transmission and decrypted before it can be used by the receiving system.

SSL advantages are:

- It can be applied to any Internet application, not just the World Wide Web.
- Once the SSL connection established, the resulting data communication channel is private, authenticated, and reliable.

SSL Secured Connection Steps:

SSL has four steps to establish a secured connection between the customer client and merchant server.

1- Initiating SSL Session: SSL session begins after the TCP session is initiated. This SSL session take place when the Internet user visits a web site address with https. The “s” here indicates the server is requiring SSL for the session.

2- The SSL Handshake: SSL session always begins with an exchange of messages called the SSL handshake. The handshake allows the server to authenticate itself to the client using public-key techniques, then allows the client and the server to cooperate in the creation of symmetric keys used for rapid encryption, decryption, and tamper detection during the session.

3- Server Authentication: SSL-enabled client goes through these steps to authenticate a server's identity:

I. Checks the server certificate's validity period by the client

II. Ensure the server certificates is accepted or not by checking the list of trusted Certificate Authority (CA) certificates.

III. Client validates the CA's digital signature on the server certificate using public key from the CA's certificate. At this point, the client has determined that the server certificate is valid.

IV. Client checks if the domain name matches the domain name of the server itself or not.

4- Client Authentication: SSL-enabled server goes through these steps to authenticate a user's identity:

I. Netscape Server checks the user's digital signature validity.

II. Netscape Server checks the certificate's validity period.

III. Netscape Server ensure if the client certificates is accepted or not by checking the list of trusted Certificate Authority (CA) certificates.

IV. Netscape Server validates the CA's digital signature on the certificate being presented using the public key from the CA's certificate.

V. Netscape Server checks what resources the client is permitted to access according to the server's access control lists (ACLs) and establishes a connection with appropriate access.

3.3.2 Secure Hyper Text Transfer Protocol

S-HTTP is the logical extension of the Hypertext Transfer Protocol (HTTP), which is the basis of the World Wide Web. Simply, Web browser sends requests for information stored on a Web server, and if that server is connected and the information is available, the server will respond by sending the information back to the browser.

The S-HTTP protocol was designed to add security at the application level. The objective was to add support for a wide range of security mechanisms on top of the interactions between Web browser and Web server. Protection mechanisms include the following: digital signature, message authentication, and message encryption. These mechanisms are used as negotiated between browser and server. Any one or more of these mechanisms may be used. The protocol also allows unprotected transmissions.

The S-HTTP specification includes:

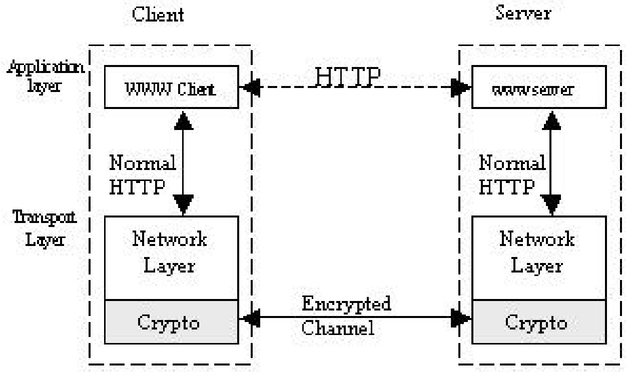
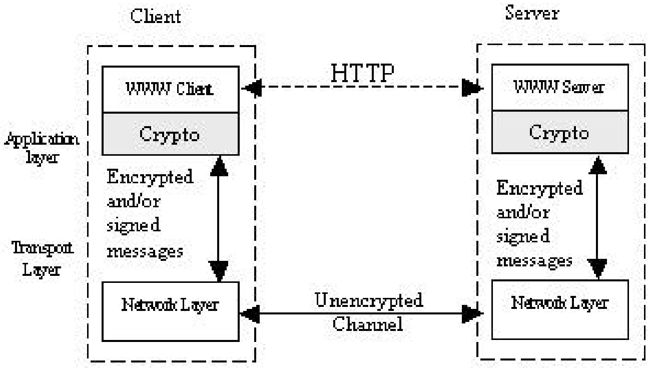
- Supporting for many cryptographic formats, including private key and public key cryptography, as well as key distribution schemes.
- Supporting use of prearranged and redistributed private keys between individuals, public key encryption in one direction, and two-way public key encryption. Each interaction between an S-HTTP browser/server pair is negotiated to determine what protection is available, needed, and capable of being used.

S-HTTP encapsulates the HTTP interactions between browser and server. This means that data being sent from browser to server (or vice versa) is contained within a special S-HTTP chunk of data. This chunk uses the same basic format as indicating the source and destination systems and other information required by TCP/IP.

Encapsulated data sent across the Internet is comparable to a package that has been wrapped in plain brown paper and addressed for delivery by an express service. The contents of the package are irrelevant, and intermediate handlers do not know exactly what is inside. However, the package will have delivery instructions printed on the outside. When a package of data arrives at its destination, the recipient program takes the headers off and interprets the data inside as appropriate.

SSL vs. S-HTTP:

S-HTTP and SSL are the two leading solutions for e-commerce security. Each one tries to make its protocol as a standard confirmed one. Because of this race, each one of them provides an e-commerce security solution in different way. Therefore, there are some differences between them in the way of solving e-commerce security issues. Main differences focused on the level they apply security process. As seen in figure below, SSL apply encryption on low-level transport layer. Where, S-HTTP applies it in application layer. Also, there are some differences on some other points. Below table shows these differences.

SSL	S-HTTP
 Client Server Application layer Transport Layer WWW Client HTTP www server Normal HTTP Normal HTTP Network Layer Network Layer Crypto Crypto Encrypted Channel	 Client Server Application layer Transport Layer WWW Client Crypto HTTP WWW Server Crypto Encrypted and/or signed messages Encrypted and/or signed messages Network Layer Network Layer Unencrypted Channel
Data security applied between application protocol and the network protocol TCP/IP. Operate on transport layer	Data security includes header directive, server side includes, and changing HTML document prosperities. Operate on application layer
Encryption only for integrity and confidentiality.	Encryption and digital signature to ensure privacy, integrity, and party's authentication.
Designed to establish secured connection between customer client and merchant server.	Designed to transmit individually messages securely.
Work with any communication protocol	Work only with World Wide Web protocol.
Application independent.	Application dependent.
Lack on supporting digital signature	Has powerful friendly use digital signature mechanism.
Provide point-to-point protection of the data during the connection process itself. Where in source and destination, data is in the clear format	Every group of data encrypted by its negotiated protocol. It is more secure than SSL at end points even after data transfer.
It depends on DES, RSA, RC-2, and RC-4 with different size of keys.	It is not tided to any particular cryptograph system, key infrastructure, or cryptographic format.
Security done at one step and directly messages exchanged between the client and the server.	Messages may encapsulated multiple times to achieve multiple security features.
It support block and stream encryption.	Encryption done using receiver public key and receiver privet key which used for decryption.
Optimum usage of this protocol depends on user consideration. If we have e-commerce with different communication protocols, SSL will be more secure and more powerful. User must consider the security at end points.	S-HTTP is strongly supporting HTTP communication protocol. It keep security event at end points and user do net need to bother himself with this issue.

Commons between SSL and S-HTTP

There are many points SSL and S-HTTP are agreed with. These commons take place to fulfill the security requirements of e-commerce systems. Commons are:

1. Web browsers and servers authenticate each other.
2. Permit web site master to control access to web servers, directories, and files.
3. Shared data exchanged between sender and receiver without third party involvement.
4. Ensure ability to uncorrupt the data exchanged between parties of e-commerce transactions.
5. Public key certificate to authenticate client and server to each other through third party called certificate authority (CA).

3.3.3 Secure Electronic Transactions (SET)

It is a standardized industry wide protocol specification designated to secure payment transactions and authenticate the parities involved in the transaction in any type of networks including Internet. VISA and MasterCard developed the SET standard with collaboration from leading software companies such as Microsoft, Netscape, RSA, VeriSign, and other.

SET was created to provide the trust needed for consumers. The protocol uses cryptography and digital certificates to provide confidentiality of the information, ensure payment integrity, and authenticate merchants, banks, and cardholders during SET transaction.

SET Specifications:

- SET uses RSA Data security public key cryptography in order to encrypt and decrypt transaction packets along with the use of digital certificates and digital signature for authentication of all parties to the transaction and validation that information has not been tampered with.
- SET makes online transactions even safer by using digital certificates to verify that consumers and merchants are both authorized to use and accept Visa cards. It's the electronic equivalent of a consumer looking for a Visa decal in a merchant's store window, and a merchant checking the consumer's signature on the back of a Visa card. Merchants worldwide are currently adopting SET.
- SET incorporates the use of public key cryptography to protect the privacy of personal and financial information. As a result, with SET, consumers' payment card information is protected all the way to the financial institution. The merchant cannot read this information in the payment transaction.
- With SET, cardholders can validate that the Internet merchant is legitimate through the merchant's digital certificate. SET software automatically checks that merchant has a valid certificate representing their relationship with their financial institution. This provides consumers with the confidence that their payments will be handled with the same Visa promise that they trust today.

SET Online Shopping steps:

Following are the steps of online shopping with SET.

- **Cardholders obtain digital wallets:** It establishes a connection with merchant's SET software to verify the merchant's certificate and a trusted financial institution.
- **Cardholders obtain digital certificates:** It contacts their financial institution for registration procedures. Visa provides digital certificates to a card-issuing financial institution, which then provides a digital certificate to the cardholder. At the time of the payment transaction, each party's SET software validates both the merchant and cardholder's digital certificate before payment information is exchanged.
- **Cardholders and merchants conduct a shopping dialogue:** Merchant sends an order form together with its merchant certificate. Cardholder selects the payment card, and your software application automatically sends the related certificate when you place your order. Payment instructions are created by the cardholder software and sent to the merchant fully disguised using public key cryptography so that the merchant cannot see the payment card information until the merchant's financial institution decrypts it.
- **Authorization and settlement process:** Merchant's financial institution requests an authorization from the cardholder's financial institution. Once authorized, the merchant can confirm the sale to the cardholder.

4. Conclusion

e-Commerce is the ability to do business through the Internet. It is not just present of computers and absence of papers. It has more than this. e-Commerce security is the major issue keeping many commerce organizations afraid from using Internet for their business. Secured Socket Layer (SSL), Secured Hyper Text Transfer Protocol (S-HTTP), and Secured Electronic Transactions (SET) are the major popular e-commerce security protocols. Each one of them has its domain of use, its products, its strategy, and its own encryption procedure. Doing a comparison study between SSL and S-HTTP is not an easy thing. There are many differences making each one of them as an e-commerce champion in security fields. Using SSL or S-HTTP depends on user consideration. SSL is the recommended one in case of different type of communications. Where, S-HTTP supports only HTTP communication protocol.

A comparison study shows the design issue of each one, its way of securing e-commerce, authenticate parties, using key exchange, and its encryption methodologies. While there are still lots of efforts focused on e-commerce security, it is not an easy decision to use Internet to exchange critical data such as credit card number, passwords, or any sensitive private information.

References

1. Aviel D. Rubin, Daniel Geer, and Marcus J. Ranum. *Web Security Source Book*. Page 273-299. 1997
2. Scot Hamilton. *E-Commerce for the 21st Century*. IEEE Computer, May 1997.
3. Gloria Yan and Joseph C. Paradi. *Success Criteria for Financial Institution in Electronic Commerce*. Proceedings of the 32nd Hawaii International Conference on System Sciences, 1999.
4. Anup K. Ghosh. *Certifying E-Commerce Software for Security*. National Institute for Standards and Technology (NIST), 1999.
5. Anup K. Ghosh. *Securing E-Commerce: A systematic Approach*. Journal of Internet banking and commerce, January 1998.
6. G. Alonso, U. Fiedler, C. Hagen, A. Lazcano, H. Schuldt, N. Weiler. *WISE: Business-to-Business E-Commerce*. Proceedings of ninth international workshop on Research issues in data engineering - IEEE, 1999.
7. Garry Froehlich, Wendy Liew, H. James Hoover, Paul G. Sorenson. *Application Framework Issues When Evolving Business Applications for Electronic Commerce*. Proceedings of the 32nd Hawaii International Conference on System Sciences, 1999.
8. Asuman Dogac, *Electronic Commerce*. Journal of Database Management, Fall 1999.
9. Reid Goldsborough, *Feeling Safe When Shopping Over the Internet*. BYTE, July/August 1998.
10. Marcus J. Ranum. *Electronic Commerce and Security*. V-One Corporation, White Paper. Http://www.v-one.com
11. Shannon Matthews. *Survey Reveals E-Commerce Security Systems Are Not Convincing Internet Users*. World Research Inc. Aug. 20, 1999. http://www.techmall.com
12. Anup K. Ghosh. *Securing Electronic Commerce: Moving Beyond Cryptography*. Journal of Electronic Commerce, 1999.
13. Anup K. Ghosh. *Certifying Security of Components Used in Electronic Commerce*. National Institute for Standards and Technology (NIST), 1999.
14. Marcus Goncalves. *Industrial Networks Are Not Ready for E-Commerce*. ARC Insights, Issue: 99-023, March 1999.
15. Mayu Mishina. *Is electronic commerce a good idea for you?* AS/400 Systems Management, July 1998.
16. Netscape Corp. *Appendix E, Introduction to SSL*. Page 213-229.
17. Taher Elgamal. *The Secure Sockets Layer Protocol (SSL)*. Danvers IETF Meeting, April 1995.
18. Nikos Drakos. *Security & Electronic Commerce: SSL Protocol*. Security & Electronic Commerce Appendix, University of Leeds. 1997.
19. Marvin A. Sirbu. *Credits and debits on the Internet*. IEEE-Spectrum, Feb. 1997
20. Andrew Cormack. *Web Security Report*. University of Wales, Cardiff. Jan. 1997. http://www.jisc.ac.uk
21. *Secure Electronic Transactions Protocol*. BYTE Magazine, June 1997. Http://www.byte.com
22. Terriza Inc. *S-HTTP Manual*. Intent Draft Document. http://www.cs.unc.edu.
23. Steve Klingler. *S-HTTP Secures Web Browsing*. Internet Week Magazine, 1/5/1998.