Development of a Secure SET-Based E-Commerce System

Sufyan T. Faraj
College of Computers, University of Anbar, Iraq
E-mail: sufyantaih@yahoo.com

Media A-R Ali
College of Engineering, Al-Mustansiriya University, Iraq

ABSTRACT

This study presents the design and implementation of a business to consumer e-commerce system that provides the basic e-commerce security requirements including confidentiality, integrity, non-repudiation, replay protection and the most important entity authentication. The above security features are obtained by adopting the Secure Electronic Transaction (SET) Protocol. The system is based on the modular Three Tier client\server architecture and guarantees portability across any hardware and software platform. This feature is basically provided by the cross-platform capability feature of the Java language. Indeed, Java Servlet technology gives the system the very important multithreading feature. MySQL database along with the HTML language were also used for system implementation. The system had been successfully installed and tested.

Key Words: E-commerce, E-payment, Java Servlet, Network Security, SET

1. Introduction

The best way to characterize e-commerce security requirements is by examining the overall process, beginning with the consumer and ending with the commerce server. Considering each link in the "commerce chain", web commerce security can be defined as a" set of procedures, practices and technologies for assuring the reliable and predictable operation of the web server, web browser and other data that is in communicate with the web server and the surrounding Internet infrastructure" [1],[2]. Accordingly this study concentrates on web transaction security as the communication channels are the major assets to be protected.

A number of approaches for providing web security are possible. These approaches are similar in the services they provide and to some extent in the mechanisms that they use, but they differ with respect to their scope of applicability and their relative location within the TCP/IP protocol stack [3], [4].

However, application level security services are more suitable and have much more benefits for our concern because these are embedded within a particular application, having the big advantage of being tailored to the specific needs of that application. In the context of e-commerce these are called the e- payment protocols. The most important such protocol is the Secure Electronic Transaction (SET) protocol.

2. SET Background

SET is an e-commerce protocol jointly developed by *Visa* and *Master-Card* as a method to secure payment card transactions over open networks. Industrial interest in the protocol is high as witnessed by the participation of *GTE*, *IBM*, *Microsoft*, *Netscape*, *RSA*, and other companies in the protocol's development [5]. SET is arguably the only currently available scheme for providing security for *entire* e-commerce transactions. Although there was a criticism of SET particularly regarding its complexity of

implementation, it can be shown that this issue can be addressed, and that SET still has the potential to overcome the barriers that restrict its implementation. In particular the various extensions (see for example [6] and [7]) to SET seem to both enhance its security and reduce the complexity of SET implementation [8].

The SET network architecture has basically a number of components, which are: the cardholder, the merchant, the issuer, the acquirer, the payment gateway, and the certification authority. Some important SET key features are [2], [9]:

1. *Data Confidentiality-The Usage of Digital Envelope;* SET obtains the benefits of both public and secret key cryptography schemes by employing the Digital Envelope cryptographic technique. The RSA-OAEP (Optimal Asymmetric Encryption Padding) 1024-bits and 128 bit AES algorithm is used.
2. *Data Integrity-Usage of Dual Signature;* SET introduces a new application of digital signature namely the concept of Dual Signature (DS). This approach prevents the SET merchant from obtaining the account details of their consumers. DS provides a linkage between two messages needed to be linked securely in order to be sent to two parties, each has to read only one of the pair. SHA-1 hashing and HMAC algorithm is used.
3. *Entity Authentication-The Usage of Digital Certificates;* SET relies upon a hierarchical (tree structure) arrangement of nine components for the management of digital certificates.

SET is a set of security protocols and formats that enables users to employ the existing credit card payment infrastructure on an open network such as the Internet in a secure fashion. Since all the provided protocols cannot be covered in this work, only the main protocols were implemented, these considered as the main and the most important protocols for general e-commerce systems [10], [11].

3. The Proposed System Architecture

The proposed design follows the three-tier architecture model. This model breaks the application into three distinct layers or tiers: user presentation, business logic, and data services tier; each with its own goals and design constraints:

1. *The user presentation tier;* it is the client side layer that hosts the front-end tool with which the end user interacts at a client PC. Basically it contains a Graphical User Interface (GUI) and some additional application specific business rules.
2. *Business logic tier;* this tier performs the business operations that the application designed to automate, through interacting with the data service tier, its resident on a computer called the management or the application server.
3. *Data service tier;* this tier supports the business logic tier in fulfilling the user requests through providing the data and information necessary to compete a transaction.

Based on the three-tier model, and according to the shopping and SET payment working procedure, the general architecture of the proposed SET-enabled e-commerce system was developed. The following four sections contain a more detailed description of the design and software implementation for each of the participants involved in the e-commerce process.

4. Server-Side Architecture

The SET merchant software consists of the server side applications that implement the business logic of the web system. The modular approach for the design calls for the separation of work on dedicated servers each has its own functionality. Distributing the work in this way assures the highest availability of resources and meets the scalability needs. Accordingly, the merchant environment consists of three essential servers: the merchant web server, merchant database server, and merchant

payment server. As shown in Figure 1, these three servers together form a logical entity which can be called the merchant.

4.1 Merchant Web Server

Java web server was used in this work as the merchant web server, due to the valuable features it has and especially being Servlets enabled. These features include cross-platform, simplicity, local and remote administration, session support, flexible security model, being standard based technologies, and extensibility. The web server is built as a multithreaded Servlets container responsible for implementing the merchant required tasks, managing the web site, establishing the connection with the payment service server and the database server, and handling the new clients tasks. There are essentially three Servlets chained together to perform the above tasks. The Servlets are built using the Java Servlet programming language, SQL database instructions, and the HTML language.

4.2 Merchant Payment Service Server (PSS)

The PSS is where SET-related work is performed. This is the computer that loads the required SET software, placing these components into separate server, permits their sharing usage by more than one merchant server software on the network. The PSS can be configured being the server side analogous of the cardholder e-wallet handling the required cryptography, managing the merchant digital certificates and the communication with the Payment Gateway Service Server (PGWS) to log the transaction authorization and settlement operations. The designed PSS consists of the following components:

1. *The PSS\Web Listener:* This Payment listener is the entry point to the PSS for the merchant's web server.
2. *The Payment Intializer:* This component is responsible for handling the new client required management processing.
3. *The PSS\Wallet Listener:* This component is responsible for listening to the wallet dedicated port waiting for the corresponding SET messages to arrive, to forward them to the PSS application for processing.
4. *The PSS Application:* This software is the core component of the PSS. It is responsible for performing the entire required SET message processing at the merchant level.

5. The Payment Gateway Service (PGWS) Server

The PGWS software is the application that provides the acquirer payment gateway function of SET protocol. It functions as an intelligent router for incoming and outgoing messages to and from the Internet. It interfaces between the legacy credit card processing systems and the SET protocol. The designed PGWS has three main components as follows:

1. *The Payment Gateway Listener:* This is the entry point to the PGWS for the merchants. It listens on a dedicated IP port and collects requests from the merchant PSS and presents them to the payment gateway application to process them.
2. *The Payment Gateway Application:* This is the software that performs all the required SET processing operations through providing the encryption services and message handling services.
3. *The Payment Gateway Legacy Application:* The role of this component is to serve the request sent by the payment gateway application, to process them by interacting with the connected financial institution.

6. The Certificate Authority Service Software

The SET protocol relies on the certificates to validate all the parties in a transaction. The software that provides the registration function is the certificate server software; it provides a certificate management infrastructure for cardholders, merchants, and acquirers to facilitate secure payment

over the Internet using the SET protocols. The designed Certificate Authority (CA) server consists of the following components:

1. *The CA Web Server:* Similar to the merchant web server, this CA component receives client requests for the registration purpose. Its operation is also built using the Servlet technique. Essentially, there are three web servlets, the *CAHome Page* which represents an introduction web site to the CA, the *CAPolicy* which contains the CA registration policy, and finally the *CAReg* Servlet which passes the requester the IP address of the CA server to perform the SET registration protocol.
2. *The CA Certification Server:* This CA component consists of the following:
   - The CA server listener: This component is responsible for listening to the dedicated SET port, collecting requests from the SET participants requesting to be certified, and forwarding these requests to the CA registry application to process it.
   - The CA Administrator: This is the application and associated interface responsible for the operational management of the server, handling the brand registration forms, establishing the root brand policies, etc.
   - The CA Approver: This component is the application that is responsible for validating the user authentication information.
   - The CA Registry Application: This is the software that handles and processes all the SET registration messages, including the registration component and the certification component.

7. Consumer Application Part

In order for the SET protocol to be successful, it is imperative that the cardholder is protected from the underlying complexity of the protocol, and to solve this problem, the client side in the cardholder is developed as two parts: the *Client Web Browser* as a universal client to visit and shop, and the *Cardholder E-Wallet Application*. The E-wallet is a fundamental requirement. This component carries out the cardholder part of the SET protocol in a salient manner. It embodies the SET required operations and provides a means to store and manage the certificates to digitally sign the required messages, along with the security aspects consumer demands to keep private data. It also communicates with SET complaint merchant servers.

The security of E-wallet is very essential, it must be safe as least as safe as a real wallet. Accordingly the designed wallet is secured using two pairs of UserID and password. The designed E-wallet (see Figure 2) consists of the following components:

1. *The Wallet\Web Server Listener:* This component of the wallet is responsible for listening to the merchant web server waiting for a wakeup wallet to launch and activate the cardholder wallet, starting the SET protocol.
2. *The Wallet* Administrator*:* This is the software and associated interface responsible for operational management of the wallet.
3. *The Wallet/ PSS Connector:* This component is responsible for establishing the required connection with the PSS during the processing and terminating when the purchasing operation is complete.
4. *The Wallet Application:* This component supports processes and manages all SET messages at the cardholder level through handling the cardholder transactions providing cryptographic functions and communicates with the merchant PSS. It basically consists of two components: the wallet purchasing application and the wallet registry application.

8. System Performance

During the experimental verification of the system, the system had been subjected to different scenarios of security attacks. The system had successfully withstood these attacks with a high robustness and a good level of performance. It is acceptable that the higher security services provided by the system pose some price that must be paid. Lag times up to 60 seconds have been noticed for the typical cardholder initiated purchase request to the approved response from the acquirer and the finalization of the transaction by the merchant server. The heavier processing load may be due to the 1024-bit RSA cryptography required in the processing of messages exchanged. Elliptic curves approach can be suggested as an alternative public key cryptography that appears to offer an equal security for a smaller key size, thereby reducing the processing overhead. Smart cards can also be used as an alternative of the disk storage of the certificates, which would free the cardholder from his local computer and make the system portable.

9. Conclusion

The design of the system follows the three-tiered architecture, which makes the system more flexible and easier to expand and scale out because any modification performed on any tier does not affect the other. The system also has the important features of multithreading and portability. The dual signature technique used by the SET protocol distinguishes it from the rest of the security payment protocols and more, solves the confidentiality and integrity problems associated with the SSL protocol. However, the SET protocol do not give any privacy to the order information. The suggestion here is that to apply the SSL protocol during the initiation phase, and when the customer agrees to buy, the SET protocol begins its operation.

References

[1] G. Schenider and J. Perry, *Electronic Commerce Course Technology*, Thomson Learning, 2001.

[2] S. Garfinkel and G. Spafford, *Web Security Privacy & Commerce*. O'Reilly Pub., 2002.

[3] W. Stallings, *Cryptography and Network Security Principles and Practice***.** 3rd edition, Prentice Hall, 2003.

[4] M. Merkow, J. Breithaupt, and K. Wheeler, *Building SET Application for Source Transactions*. Wiley Pub., 1998.

[5] S. Lu and S. Smolka, "Model Checking the Secure Electronic Transaction (SET) Protocol", Proceedings of the 7th IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS'1999), USA, October 1999, pp. 358-365.

[6] P. Jarupunphol and C. Mitchell, "Measuring 3-D Secure and 3D SET against e-commerce end-user requirements", Proceedings of the 8th Collaborative electronic commerce technology and research conference, National University of Ireland, June 2003, pp.51-64.

[7] P. Jarupunphol and C. Mitchell, "Implementation aspects of SET/EMV", in J. Monteiro, P. Swatman and L. Tavares (eds.), Towards the Knowledge Society: eCommerce, eBusiness and eGovernment, The 2nd IFIP Conference on e-commerce, e-business and e-government, IFIP I3E 2002, Portugal, October 2002, pp.305-315.

[8] P. Jarupunphol and C. J. Mitchell, "The future of SET" Proceedings of UKAIS 2002, Leeds, UK, April 2002, pp.9-17.

[9] SET Co., *Secure Electronic Transaction Standard Glossary, SET Specification Book1: Business Description*, 1998. http://www.setco.com.

[10] SET Co., *Secure Electronic Transaction Standard Glossary, SET Specification Book2: Programmer's Guide*, 1998. http://www.setco.com.

[11] SET Co., *Secure Electronic Transaction Standard Glossary, SET External Interface Guide*, 1998. http://www.setco.com.

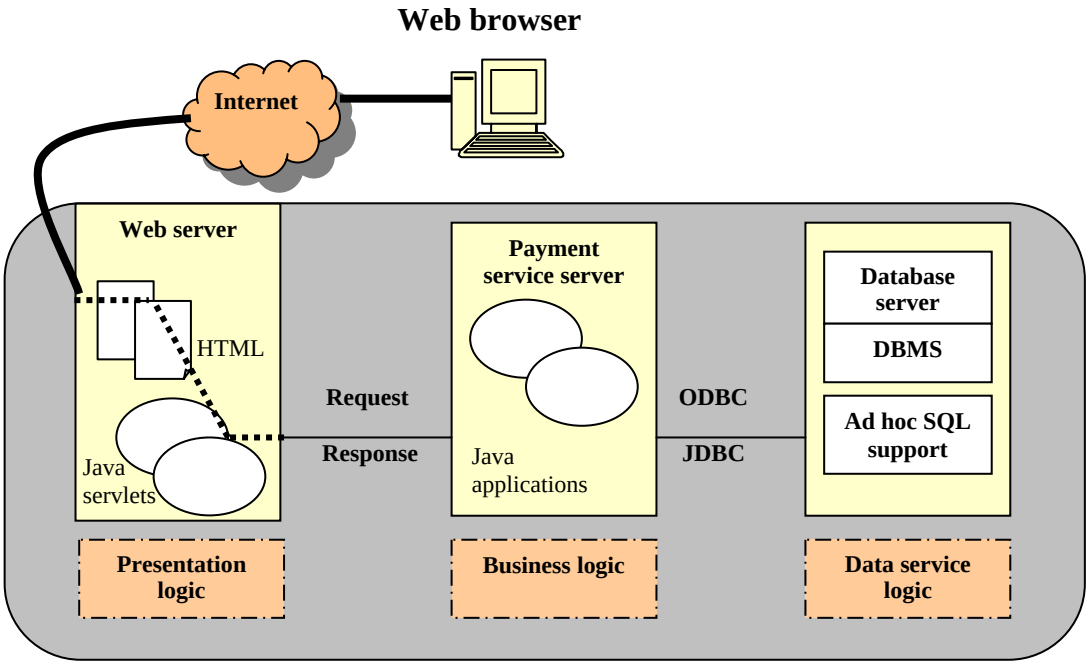

Figure 1: The Merchant Software

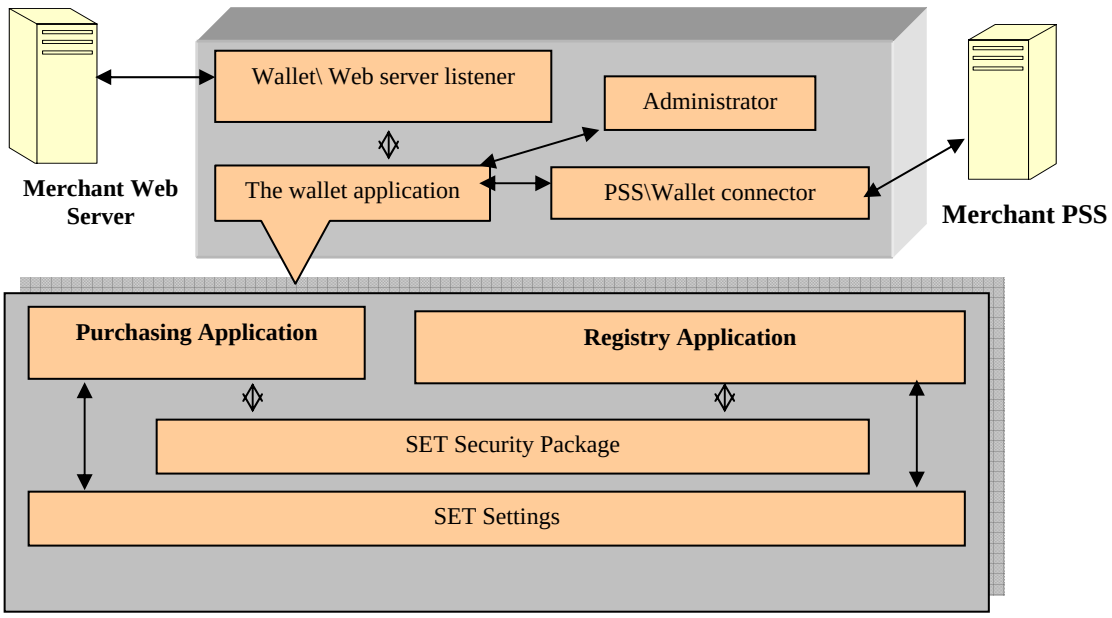

Figure 2: The Cardholder E-Wallet.