Innovative Systems Design and Engineering
ISSN 2222-1727 (Paper) ISSN 2222-2871 (Online)
Vol 3, No 6, 2012

On Designing a Secure E-Commerce Transaction Management System – A UML Based Approach

Sanjay Banerjee
Department of Computer Science, University of Burdwan
PO Rajbati, Burdwan - 713104, WB
E-mail: sanjay.banerjee@yahoo.co.in

Sunil Karforma
Department of Computer Science, University of Burdwan
PO Rajbati, Burdwan - 713104, WB
E-mail: sunilkarforma@yahoo.co.in

Abstract
E-commerce gained popularity as a sophisticated transaction system for buying and selling of products and services efficiently through Internet. Due to lack of privacy and security, customers are unwilling to participate in E-commerce transaction system. To combat such inefficiency in transaction of E-commerce and to regain the customers trust an attempt is made here to design a prototype of a secure E-commerce transaction system that brings all components of the E-commerce into a common platform to offer a model of a unified integrated E-commerce system using DRM.
In the proposed system, the transaction manager generates single use token consisting information about the customer, merchant, product, and payment amount etc. and thereafter wrapped as a DRM package. The advantages of using such token are, after a single use the token will expire, which minimizes the possible loss in the transaction, also, as the token wrapped as a DRM package, therefore only the intended user and the specified application software can open the DRM package using special key. The application, thereafter, will take care of the rights imposed on the '*token*' and expires itself after the single use.
To design the model of the proposed system we have tried to use Unified Modeling Language (UML), which allows developing a very flexible model that facilitates maintainability, reusability, portability and other Object Oriented software engineering features inherent in the E-commerce transaction system.
Keywords: E-commerce, Object, Object Oriented Modeling (OOM), UML, DRM

1. Introduction

E-commerce is a cost and time effective method to promote a product to the worldwide customers. E-commerce transaction may require submitting customer's personal information such as username, password, credit card numbers and financial data etc. But due to different fraudulent activity on the Web, customers are not confident to submit their personal information. And due to lack of such security a significant portion of the customers are feel uncomfortable to send their respective identity over the Internet. In traditional business, customers accept the security risks in places like departmental stores because they can see and touch the products and make judgments about the store, which is almost absent in case of an E-commerce system.
In order to win customer's trust, the E-commerce transaction system should be competent enough to avail of the advantages of the appropriate technology to combat the Internet security threats caused by hackers. Thus, to get the opportunity of expanding the businesses by the firms an E-commerce system must be earn the confidence of the customer. The risk and the challenges of the trust that discourage the customer to participate in the E-commerce system are as follows:

- **Spoofing** - The ease of copying and creating the existing pages of a Website makes it too easy to create duplicate sites that pretend to be the original one published by different organizations for conducting fraudulent activities involving the collection of personal information illegally.
- **Interception of sensitive data -** When transaction information is transmitted through the Internet, hackers can intercept the transmission and obtain customers' sensitive information like credit card number, username, password etc.

- **Data alteration -** The content of a transaction may not only be intercepted, but also may be altered en route, either maliciously or accidentally. Customer names, credit card numbers, and amounts sent through the Web all are vulnerable to such alteration.
- **Denial of services -** The Website can be altered by the hackers so that it refuses service to the customers or may not function properly, such as SYN Flooding, DDoS etc.
- **Overcharge –** The fraudulent activities may include charging the customers at a higher than the agreed prices for the good or service ordered by the customer.

In order to offer solution to the aforesaid problems, various attempts have been made earlier (see Section 2) which include the following components-

- Digital certificates for Web servers that provide authentication, privacy and data integrity through encryption.
- Online payment management system that allows E-commerce Websites to securely and automatically accept, process, and manage payments through Internet.

The present paper has been organized as follows: Section 2 deals with prior research relevant to the security issues of transaction in E-commerce. Section 3 is devoted to identify the specific objective of our study. In Section 4 we have described the methodology to design the proposed system and finally, conclusions have been drawn in Section 5.

2. Prior Research

Sufficient security controls are required to reduce the associated risk in E-commerce transaction system. However, these controls should not be so restrictive that the overall performance of the system is degraded. Some of such controls are as follows:

- **Authentication:** This is the most primitive method of using a username and password combination for protecting contents of a Website from being accessed.
  Username and password combination are easy to detect, therefore it is not a good approach for Website protection.
- **Access Control:** This restricts different groups of authorized users to access subsets of information and ensures that only the intended user could access data and services offered by the system.
  Access control could only be a part of entire security system and therefore is not a full-fledged security control mechanism.
- **Encryption:** During the initial stage of digital data protection encryption is used, based on cryptographic algorithms. Cryptography is implemented by transforming the digital information into encrypted digital information which is thereafter inaccessible. Two major categories of encryption systems are symmetric key encryption and asymmetric key encryption.
  Encryption can be a way of protecting transmitted data over the Web based on cryptographic algorithms, but this is not sufficient. It doesn't prevent someone from copying a file but it prevents access to the content of a file. Encryption works only when a person holding a key is the one who wants to protect the digital file. Giving the key to anyone else negates the purpose of the encryption.
- **Firewall:** Firewalls are software or hardware security measure that filters information passing between an internal and external network. A firewall controls access to the Internet by internal users, and also prevents outsiders from access to the systems and the information stored on the internal network. A firewall typically could be one of the two forms: Software firewall and Network firewall.
  Firewalls are part of the overall security mechanism of an organization, therefore it should not be considered as the sole security system.
- **Intrusion Detection:** The software related to intrusion detection continuously monitors the system and the network activity to spot any attempt being made to gain access to the system. An alarm is generated when the detection system suspects an attack.
  Intrusion detection system only generates an alarm during suspicious attacks but it could not normalize the system activity.
- **Protecting from Viruses and Spywares:** Anti-virus software is used to protect against viruses. This software can detect viruses, prevent access to infected files, and quarantine infected files if any.
  The spyware can also be removed or quarantined.
  Anti-virus and Anti-spyware software require regular updates to combat the latest virus and spyware definitions available online.

- **Digital Signature:** In an E-commerce system, digital signatures are used to sign licenses between participating users for transmitting digital content over the Web. The licenses are thereafter used as a proof of usage rights. At the client side such licenses are verified for the verification of the usage rights.
  Digital signature has the limitation of distribution, i.e. once a customer purchases the usage rights he can distribute the rights over the Internet, which causes a violation of the copyright.
- **Digital Certificates:** Digital certificates are used to ensure the genuineness of the digital content and the valid authorization of the distributor. Digital certificates are an essential mechanism to authenticate various parties involved in digital data transmission.
  There is no prevention mechanism of distribution of digital certificates and its usage.

3. Objective of the present study

In view of the above, there is a strong justification to design a model that would fill the functional deficiency of the present E-commerce transaction system using the latest technology. From the present study it has been observed that the customer discloses their personal information along with other personal identification to the merchant in order for the merchants to use such information. To offers customers more control over their digital identities DRM can be used, which ensures that the distributed right is not violated. So, to improve the level of trust in the mind of the customers, our proposed system is a DRM based E-commerce transaction system.

To offers a generic prototype of the proposed system UML is used, which is very efficient to design the model of E-commerce system and is an Object Oriented system analysis and design paradigm developed by Grady Booch, James Rumbaugh, Ivar Jacobson in the Rational Software Corporation. UML facilitates graphically visualizing, specifying, constructing, and documenting a system's blueprints.

To model our proposed system we only consider the Use Case diagram, Sequence diagram and the Collaboration diagram [c.f. Appendix-A]. Use Cases are used to document the proposed system requirements and provides a useful technique which helps us to clarify exactly what the system is supposed to do.

4. Methodology

4.1 Identifications of Objects

In this section we first identify the participants who become involved in the transaction processing system in E-commerce. They are as follows:

- **Customer**: Customer is the person or organization who initiates the transaction by selecting product or services offered by the merchant online.
- **Merchant**: Merchant is the person or organization who sells goods or services to the customer through Web.
- **Payment Gateway:** A financial institution which processes payment authorizations and makes payments by electronic transfer of funds to the merchant's account from the customer's account over a secured payment network.
- **Transaction Manager:** Transaction Manager is a person or organization, who collects order information from the customer, wrapped the information into a DRM package along with the rights to use the same and send it to the payment gateway.

In our proposed system we represent a DRM based E-commerce transaction model. The model describes how the participants of E-commerce transaction system are interacting with each other. We use UML's Sequence Diagram in Figure 5 which describes the time dependent communication through message passing between the participants.

4.2 Use Cases

Given the above objects we propose the newly developed model, subdivide into a number of Use Cases. Here each Use Cases denotes a subsystem.

4.2.1 Use Case 1: Customer

As in Figure 1 there are five different use cases related to the Customer activity into the system, these are

- Browse/select items: In this, customer browse and select items from the merchant Website
- Make order: Customer make an order of those selected item and initiate a transaction
- Send order & Merchant info: Send collected information about the transaction from the merchant to the transaction manager
- Cancel order: Cancel selected transaction or all already ordered transaction
- Make payment: Make payment to the merchant through the payment gateway for a transaction

4.2.2 Use Case 2: Merchant

As in Figure 2 there are seven different use cases related to the merchant activity in the system, these are

- Place Item on the Web: Place products/items on the Web so that customer browse and select items to purchase
- Process order: Process all order transaction placed by the customer
- Send order info: Send the placed order information to the customer. This use case extends the *Process Order* transaction use case
- Collect DRM package: Collects DRM package from the transaction manager which includes transaction information
- Send DRM package: Send the DRM package to the payment gateway, this is an extended use case of the *Collect DRM Package*
- Confirm order: On receiving the DRM package merchant confirm order to the customer
- Collect payment: Collect payment through the payment gateway which conclude the transaction

4.2.3 Use Case 3: Transaction Manager

As in Figure 3 there are five different use cases related to the activity performed by the transaction manager in the system, these are

- Collect order info: Collect information about the order placed by the customer
- Validate Customer: Verify and validate the customer information
- Generate token: Process the submitted order and generate a single use *'token'*
- Create DRM package: Create the DRM package by wrapping the *'token'* along with it's usage rights
- Send DRM package: Send the DRM package to the merchant

4.2.4 Use Case 4: Payment Gateway

As in Figure 4 there are seven different use cases, these are

- Collect DRM package: Collect DRM package from the merchant
- Validate Merchant: Validate the authenticity of the merchant
- Unwrap DRM package: Process the DRM package and unwrap it
- Find Token: Collect the *'token'* from the unwrapped DRM package
- Validate Token: Validate the unwrapped *'token'*
- Transfer Fund: Transfer fund from the customer's account to the merchant's account.
- Send Fund Transfer Confirmation: Confirm fund transfer to the customer and merchant

4.3 Sequence Diagram

To describes the time dependent communication through message passing between the objects of the proposed transaction system Sequence Diagram is used. Figure 5 describes how the *Customer, Merchant, Transaction Manager* and the *Payment Gateway* are communicating with each other over time using Sequence Diagram.

The algorithm of our proposed transaction system is as follows:

Step 1: The customer places an order online by selecting items from the merchant's Website. The merchant replies to the customer with an order summary of the items, price, total value, order number etc.

Step 2: The customer redirects the order information along with the merchant information to the transaction manager.

Step 3: The transaction manager processes the order and generates a *token* based on the information submitted by the customer. The *token* is then *wrapped into a DRM package* along with the rights to use the same and stores the *token* for future reference along with the customer account. The DRM package is then send to the merchant for payment

Step 4: The merchant confirms the order and supplies the goods or services to the customer.

Step 5: The merchant requests payment to the payment gateway by sending the *DRM package*.

Step 6: On having the *token*, the payment gateway processes it i.e. *unwraps the DRM package* using specified application and key supplied to it and then the transaction is settled, electronic fund is transferred from the customer's bank to the merchant's bank.

The advantages of our proposed system are as follows:

- The *token* will be generated using the information order provided by the customer and about the merchants. This would ensure that only the specified merchant can use the *token*. Because on receiving the *token*, the payment gateway validates the customer as well as the merchant.

- Along with merchant information the *token* will also wrap the customer information which is stored as a future reference of the transaction.
- The package can be unwrapped only by using a specific application [such as Adobe Acrobat], that will take care of the rights imposed on the package and will restrict its use.
- As the token is expired after single use this minimizes the risk to the customer.

5. Conclusion

To ensure trust to the participated customers in the E-commerce transaction system lots of efforts have been made. In order to provide security to the participants of such system several considerations have been made. However, to fill the observed deficiency of the E-commerce transaction system no such efficient functional solution so far has been developed.

In our paper an attempt has been made to throw some light on the different security risks of E-commerce transaction system and also to offer a solution to fill such deficiency of the system. To offer a solution, we first consider the participants related to our system, followed by a sketch identifying the association and interaction of such participants of the proposed system.

The proposed model can be successfully applied by means of making a very little change in the current E-commerce transaction system. In future this proposed model may also be utilized for the purpose of managing transaction securely in the M-commerce system.

References

Lawrence, S. et al. (2001). Persistence of Web References in Scientific Research. *Computer*. 34, 26-31. doi:10.1109/2.901164, http://dx.doi.org/10.1109/2.901164

"The Technology of Rights: Digital Rights Management", Karen Coyle, Based on a talk originally given at the Library of Congress, November 19, 2003

"E-Commerce – An Indian Perspective", P.T.Joseph, S.J, PHI, 2nd Edn, 2006

http://www.epaynews.com.

http://www.nasscom.org.

"Building an E-Commerce Trust Infrastructure SSL Server Certificates and Online Payment Services", VeriSign Technical Brief, www.verisign.com

S.Banerjee, S.Karforma, S.Ghosh, "A DRM Based Credit Card Transaction in E-Commerce System", 41st National Convention of CSI, November 23-25, 2006, Tata McGraw-Hill, ISBN-0-07-062171-3, pp-107-110, 2006

S.Banerjee, S.Karforma, "A Prototype Design for DRM based Credit Card Transaction in E-Commerce", ACM Ubiquity, Vol. 9, Issue 18, pp. 6-12, ACM Press, USA, ISSN-1530-2180, May 2008

U.S.Pandey, R.Srivastava, S.Shukla, "E-Commerce and its Applications", S.Chand Publication, ISBN 81-219-2841-9, 2007

S.Garfinkel, E.H.Spafford, "Web Security & Commerce", O'reilly, ISBN 1-56592-269-7, 1st Edn., 2007

M.Stamp, "Information Security: Principles and Practice", Wiley, ISBN 13 978-0-471-73848-0, 2006

P.Koster, F.Kamperman, P.Lenoir, K.Vrielink, "Identity-Based DRM: Personal Entertainment Domain", LNCS, Vol. 4300, DOI. 10.1007/11926214_4, 2006

W.Zeng, H.Yu, C.Lin, "Multimedia Security Technologies for Digital Rights Management", Elsevier, ISBN 10: 0-12-369476-0, 2006

G.Booch, J.Rumbaugh, I.Jacobson, "Unified Modeling Language User Guide", Addison Wesley, 2nd Edition, ISBN: 0- 321-26797-4, 2005

P.Kruchten, "The Rational Unified Process", Addison-Wesley Longman Inc, 3rd Edition, 2004

IBM's Rational Rose: (http://www.rational.com)

K.Lee, D.E.Booth, "A Prototype System Developed for Digital Rights Management in Electronic Commerce", Jour. of Internet Commerce, Vol. 3, No. 4, pp. 93-117, ISSN 1533-2861, 2004

S. Banerjee, D. E. Booth, S. Ghosh, S. Mukhopadhyay, "A Prototype Design for Digital Intellectual Property Right Management in E-Commerce - A UML Based Approach", Journal of the Computer Society of India, Vol 36 No 4 (Oct-Dec 2006), pp-46-51, ISSN-0254-7813, 2006

"Unified Modeling Language User Guide-The ultimate tutorial to the UML from the original designers", Grady Booch, James Rumbaugh, Ivar Jacobson, Addison Wesley, 1998, ISBN: 0-201-57168-4

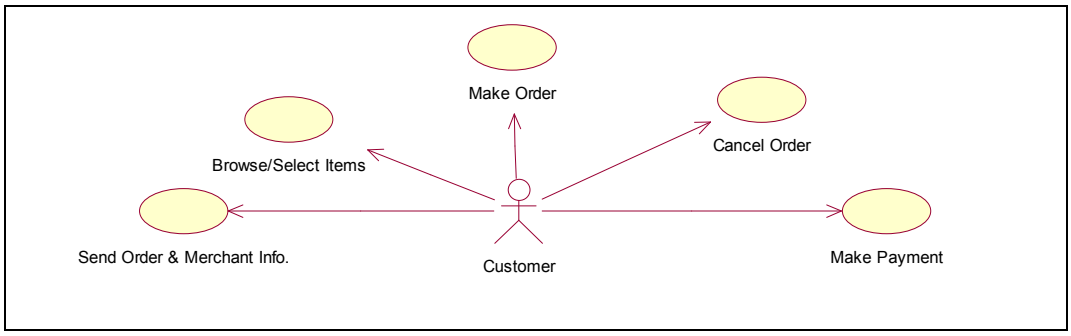

Figure 1: Use Case 1

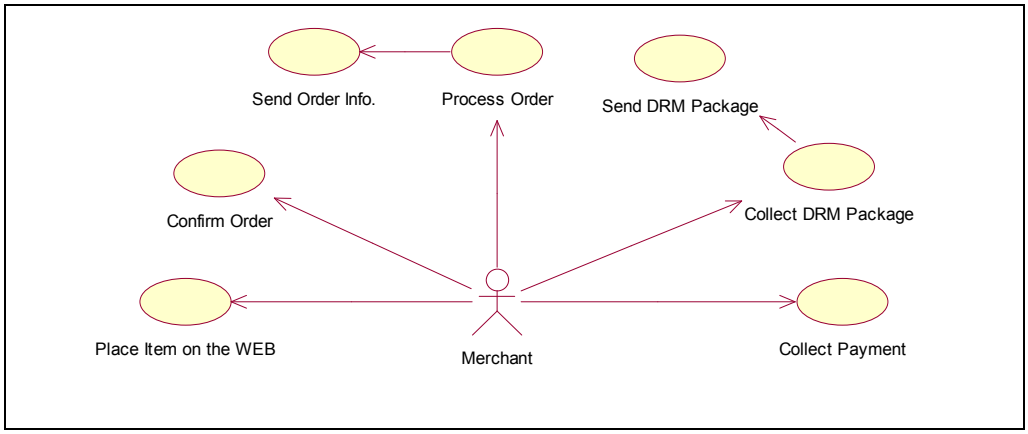

Figure 2: Use Case 2

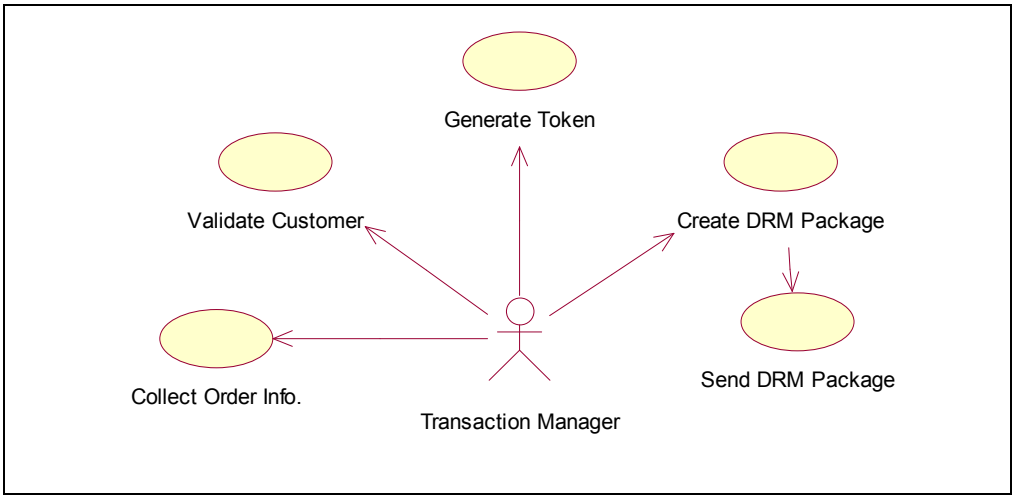

Figure 3: Use Case 3

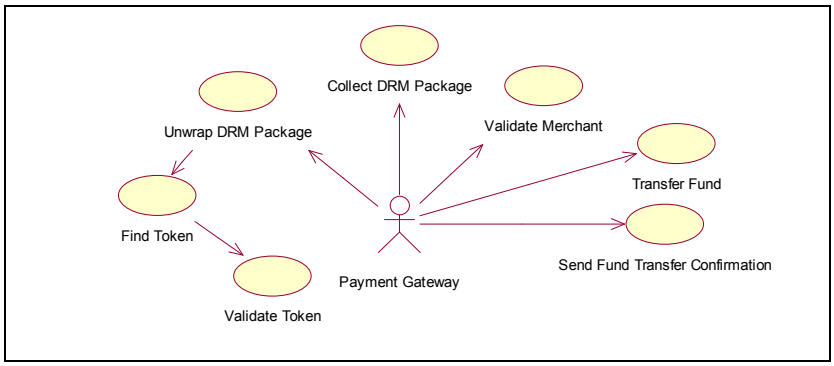

Figure 4: Use Case 4

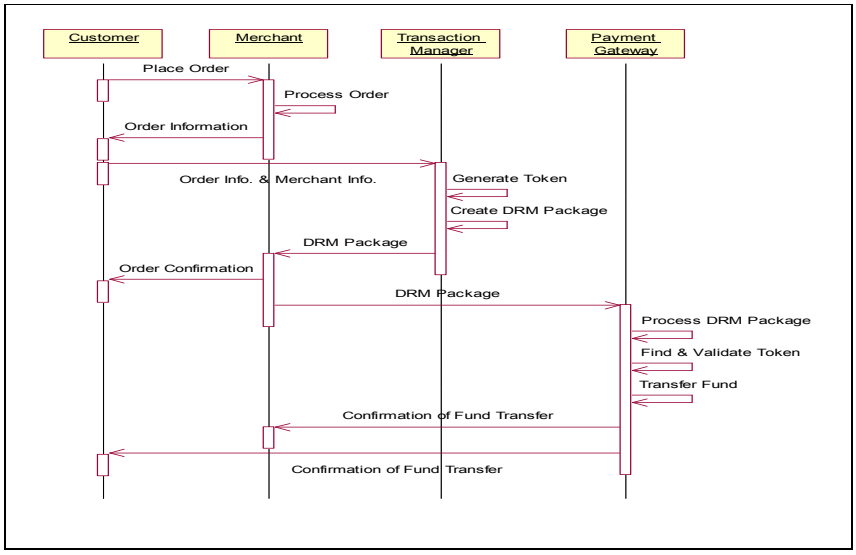

Figure 5: Sequence Diagram of the Secure E-commerce Transaction System

Appendix-A (Collaboration Diagram)