International Journal on Information Sciences and Computing, Vol.3, No.1, January 2009

A FRAMEWORK FOR E-COMMERCE TRANSACTIONS

Lalitha R[1], Dr.VenkataRama Raju[2] D, Sadhanandavel R[3]
[1]Research Scholar, Sathyabama University, Rajiv Gandhi Road, Chennai, India
[2]Reader, Pachyaippa's college, Chennai, India
[3]Project Manager, Sify Technologies Ltd, Chennai, India
Email: [1]lalitha.sadha@gmail.com

Abstract

All e-commerce environments require support for security properties such as authentication, authorization, data confidentiality, and non repudiation. Security is required to prevent theft, and to ensure revenue generation from authorized recipients. The secure e-commerce transactions for multicast Services (SETMS) architectural framework is proposed, to provide security in e-commerce sessions for multicast environments. The SETMS framework provides authentication of host through the HIP protocol, authorization of subscriber and his/her e-payments through a variant of the 2KP protocol. It supports non repudiation of principal parties through PKI.

Key words: Multicast Services, Authentication, Authorization, Protocol, Pki

I. INTRODUCTION

In modern commerce, consider the most basic trade, a client submitting an order for some goods or service. Different disputes may arise between the parties, e.g. regarding the quality of the goods or the time of delivery. Disputes may result from intentional attempts to cheat by either client or server, or from unintentional delivery problems. In simple trades, there is exchange of goods, or of goods for payment. In such cases, parties can use a trusted third party, ensuring fair exchange, and thereby avoiding disputes. However, often the server is obliged to provide the service or goods, upon receipt of appropriate order.

For example, it can be designed to carry the authentication and authorization of the subscribers to all the connecting web sites from the host site. The authentication is done in the host site alone and carried out through out the other sites. Hence, it is proposed to design the following:

- Provide Authorization of the merchants and subscribers.
- Provide Authenticated services].
- To replicate the secure service to all recipients in the multicast environment.

The major focus is on :

- The aspects of service security
- Reliability
- The provision of functionality to achieve liability
- Fair exchange for e-commerce interactions

II. PROPOSED SYSTEM

SETMS provides a development platform for the fast and cheap development of secure and reliable e-commerce services for the Internet as it is. It enforces provability using fair-exchange protocols relying on the SSL (Secure Socket Layer) [2] protocol. This make possible to prove that a transaction has been executed between the two parties. So the vendor interacts with the buyer through this intermediate host. This means that the vendor/buyer interaction can be through a simple internet connection, from home or work. An ecommerce service provider offers two interfaces for each service, one to buyer, and one to the vendor. The e-commerce service provider guarantees security as well as availability and acts as on-line.

The AAA [4] working group of IETF has presented a general AAA framework for securing an inter domain infrastructure. AAA represents Authentication, Authorization and Accounting Service. The AAA server provides distributed authentication, authorization and accounting services to subscriber's sessions. It has distributed AAA clients across networks, namely NAS, for providing the functionality of AAA services. The AAA services are shared securely with NAS through AAA protocol like RADIUS, DIAMETER etc.

III. METHODOLOGY

RADIUS [4] stands for Remote Authentication Dial-in User Service. RADIUS is a widely used protocol in network environments. It is commonly used for embedded network devices such as routers, modem servers, switches, etc. A summary of the RADIUS packet is below (from the RFC. The various codes and their description are as follows:

AUTHENTICATION PROCESS

For the SETMS framework [10], Identity authentication is a protocol whereby some principals can prove their identities to each other. It ensures that no principal can impersonate another principal. Identity authentication can be further classified into Merchant authentication and Purchaser authentication.

Purchaser authentication is required to allow only the identified purchase to have access to the multicast traffic. Merchant authentication is required to determine if a principal has the privilege to participate in an e-commerce transaction.

MERCHANT CONTENT PROVIDER

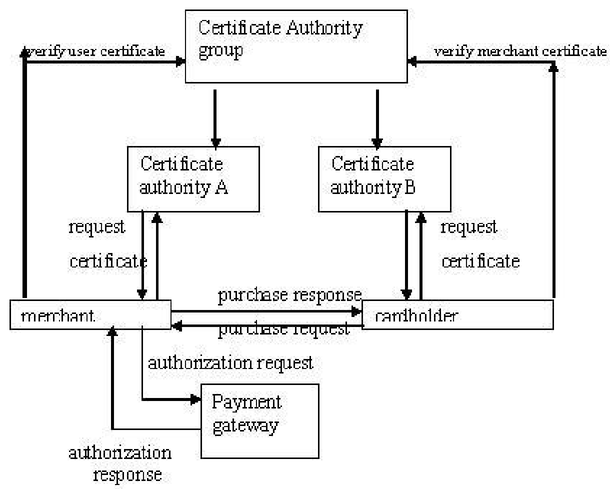
Merchant's Content Provider (MCP) [10] is a server that provides services of a merchant to its subscribers. Here the merchant maintains about the product details. They maintain the product name, price and the stock of each product. It validates the authorization requests of its subscribers. It defines the service policies for each of its multicast applications. These policies dictate the access control privileges of its subscribers.

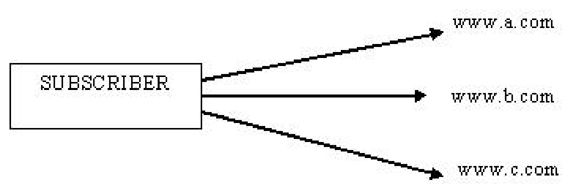
Value	Description
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access Challenge
12	Status-Server -experimental
13	Status-Client -experimental
255	Reserved

```
0      1    2    3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0
1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      | Code  |  Identifier |    Length      |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
+-+-+-+-+-+-+-+-+-+-+-+
                                                  |
                                                  |
                                                  |
                                                  |
               Authenticator                      |
                                                  |
                                                  |
                                                  |
 -+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
          Attributes ...
                   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
          -+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Authentication is done on the following pairs:

- Subscriber, AAA server
- Subscriber, MCP
- MCP, Policy Server (PS)
- PS, AAA server





The subscriber is automatically authenticated in the process of the payment authorization. Since the authorization details contain the user identity details such as the subscriber's name, address, and credit card details, MCP can authenticate the user once the payment authorization is validated.

In consumer authentication module, a subscriber is an end user who has requested a multicast service after agreeing with the service terms put forth by the merchant. The subscriber is required to possess a credit card to gain access to e-commerce services. The authentication

procedure is provided for maintaining the privacy and security of file. Before accessing the server, every vendor should give his user name and password for security confirmation.

In this process, the server gets the sender user name and password. Sometimes by mistake, if the user inputs are wrong; the server generates the warning to every mismatch input. The server performs matching of the user name and password in the database. If it is matched, then the server registers the user else quits the unauthorized person.

For Accounting purpose, the SETMS allows data to be sent at start or end of the session alone. It indicates the time, packet size, number of bytes used in each session etc. iKP protocols and SHA-1 and higher protocols can be used to provide authentication.

CONCLUSION

In our SETMS system framework provides solutions to the problems for multicast services in ecommerce infrastructure. The end-host authentication, subscriber and his e-payment authorization, and suggests a distributed accounting model for administering an efficient ecommerce system.

REFERENCES

[1] S. Deering, 1989, "Host extensions for IP multicasting", IETF RFC 1112, August 1989.

[2] IETF Authentication, Authorization and Accounting (AAA) working group charter at:http://www.ietf.org/html.charters/aaa/charter.html .

[3] SET business description, programmer's guide, formal protocol definition, protocol description

[4] M. Bellare, J. A. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik, E. V. Henreweghen, M. Waidner., "Design, implementation and deployment of the isecure electronic payment system", IEEE Journal on Selected Areas in Communications

[5] Anil Kumar Venkataihgari, J.William Atwood, Mourad Debbabi Secure E-commerce Transactions for Multicast Services

R.Lalitha

Research Scholar ,Sathyabama University. She is a Post Graduate in three disciplines- Computer Science, Information Technology and management.She has 15 years of Academic Experience and has presented several papers in national /international conferences.