Application-Level and Database Security for E-Commerce Application

Pradnya B. Rane
Computer Department
Veermata Jijabai Technological Institute,
Matunga, Mumbai

B. B. Meshram
Computer Department
Veermata Jijabai Technological Institute,
Matunga, Mumbai

ABSTRACT
E-commerce applications are becoming popular day by day as they are working like a virtual shop. Today's distributed e-commerce applications typically rely upon various technologies in their realization, including the web, scripting languages, server-side processing and an underlying database. The combination of these technologies creates a system that requires attention to the security issues of each component and the system as a whole. Hence security related to authentication, authorization and transaction database need to be managed carefully.

General Terms
Security, Authentication, Authorization

Keywords
Encryption, Watermarking, Steganography, Salt, Hashing

1. INTRODUCTION
Electronic commerce lets companies integrate internal and external business processes through information and communication technologies. E-commerce applications are categories into different types

- B2B – Business to Business E-commerce
- B2C – Business to Consumer
- C2C-Consumer to Consumer
- B2E – Business to Employee
- C2B-Consumer to Business
- G2G- Government to Government

Clearly, the online transaction requires consumers to disclose a large amount of sensitive personal information to the vendor, placing themselves at significant risk. Understanding (indeed, even precisely defining) consumer trust is essential for the continuing development of e-commerce. . This litany of evolutionary phases masks a number of growing technical challenges, including [1][2]

- security and authentication;
- content management and publication;
- reliable systems, messaging, and data;
- complex interactions and transactions;
- business model implementation and business process enactment; and
- distributed processing and distributed data.

Too often E-commerce security is framed solely as a communications security problem. Cryptography is seen as the essential security technology. Encryption algorithms and digital signatures provide the basic building blocks, protocols like SSL constitute the next layer of mechanisms that in turn support applications like secure E-mail e .g. SIMIME, electronic payment schemes like SET (secure electronic transfer), a protocol for payment-card transactions developed by Visa and Master-card. The final ingredients are public key infrastructures (PKIs) that tic cryptographic keys to user. From this point of view, current export restrictions on equipment and software implementing cryptographic algorithms are the obstacles that has to be removed before universally deployed strong cryptography facilitates secure E-commerce. Often, industry analysts cite trust and security as the main hurdles in growing e-commerce[1][4][5].

This paper is organized as follows. Section I is introduction which gives brief ides about E-commerce applications. Section II focused on security challenges in the E-commerce Applications. Also it focuses on attacks related to authentication and authorization, their attack enablers and their countermeasures. Section III explains the proposed system architecture for securing e-commerce application. This proposed system does not include any network related issues. Paper concludes in section IV with overall dimensions of e-commerce and network security.

2. RELATED WORK
Web-based e-commerce applications commonly employ multiple tiers (3-tier client server architecture) and a combination of technologies such as HTML, XML, JavaScript, Java (JSP, Servlets), ASP, dynamic html, CGI, and relational databases, as shown in Figure 1. Each of these technologies have separate and in some cases incompatible approaches to protection against intrusion or attacks[3].

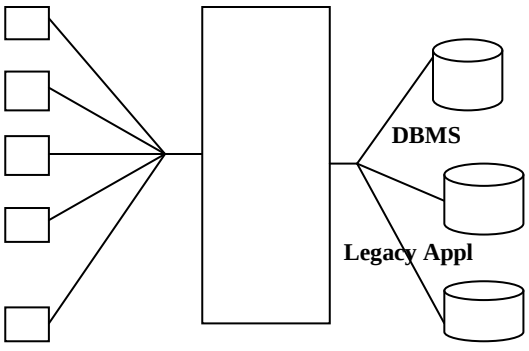

Fig 1: 3-tier client-server architecture[3].

For e-commerce applications, the communication between clients and the middle-tier is via web protocol http. Clients may employ any number of technologies such as applets, html, xml, and scripts. The middle-tier is business logic using WebObjects, ASPs, Java J2EE, servlets and JSP. The combination of different technologies at each tier, presents special challenges to security of the overall application[3].The purpose of Web security is to meet the security expectations of users and providers. To that end, Web security is concerned with

- client-side security,
- server-side security, and
- secure transmission of information.

Client-side security is concerned with the techniques and practices that protect a user's privacy and the integrity of the user's computing system.
Server-side security is concerned with the techniques and practices that protect the Web server software and its associated hardware from break-ins, Web site vandalism and denial of service attacks.
Secure transmission is concerned with the techniques and practices that will guarantee protection from eavesdropping and intentional message modification. Secure e-business can be broken down into four areas:
1. Authentication – ensuring that both the sender and recipient are who they say they are;
2. Data privacy – guaranteeing the confidentiality of information as it moves around the public Internet;
3. Data integrity – ensuring that authenticated users in a transaction are not able to deny actions they have taken;
4. Authorization – denying unauthorized users access to information they're not supposed to see.

As shown in Figure 2,there are various types of problems can occur at each of the 3-tiers. In case of client side computer viruses, line taps, loss of machine can affect user's privacy and integrity of user's computer system. In case of internet or network connection tapping, sniffing, message alteration, theft of data can occur. At server side hacking, computer viruses, theft of data, line taps, denial of service attacks are the major issues. Finally at database side sniffing attacks , DBMS exploits can cause theft of data, copying of data or alteration of data.

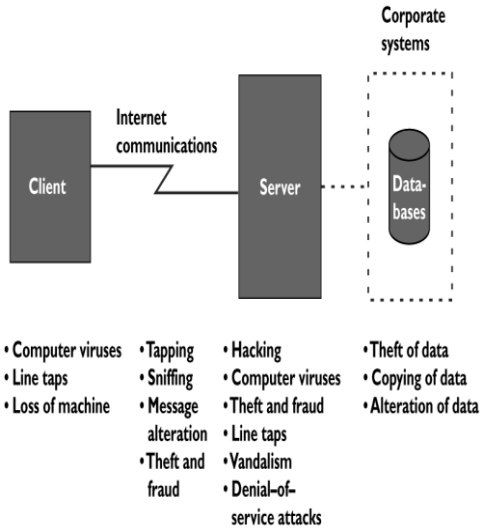

Fig 2: Security Areas of E-commerce Application

The above are the different security issues in any web-application which needs to be addressed. E-commerce lets businesses reduce costs, attain greater market reach, and develop closer partner relationships. However, using the Internet as the underlying backbone network has led to new risks and concerns. Too often E-commerce security is framed solely as a communications security problem. Cryptography is seen as the essential security technology. Encryption algorithms and digital signatures provide the basic building blocks, protocols like SSL constitute the next layer of mechanisms that in turn support applications like secure E-mail e .g. SIMIME, electronic payment schemes like SET (secure electronic transfer), a protocol for payment-card transactions developed by Visa and MasterCard. The final ingredients are public key infrastructures (PKIs) that tic cryptographic keys to user. From this point of view, current export restrictions on equipment and software implementing cryptographic algorithms are the obstacles that has to be removed before universally deployed strong cryptography facilitates secure E-commerce. Often, industry analysts cite trust and security as the main hurdles in growing e-commerce[17].

3. PROPOSED SYSTEM

The purpose of Web security is to meet the security expectations of users and providers. To that end, Web security is concerned with

- client-side security,
- server-side security, and
- secure transmission of information.

In this paper we are concentrating on application-level security and database security for e-commerce application
Basic concerns of transaction security of e-commerce are:
1) Authenticity
The ability to verify the parties on both ends of a communication link
2) Integrity
The ability to verify that all data transmitted and received has not been tampered with or changed
3) Confidentiality
The ability to ensure that all transmitted data over a communication link cannot be read by unintended parties.
For e-commerce application the security concerns are given for application level security and database security, and not for network security. These two major parts of the system are explained as follows.
E-commerce applications are becoming popular day by day as they are working like a virtual shop. Writing good E-commerce application is tedious task and complex also. The applications if made complex are very difficult to maintain. Usability is a very basic concept in the E-commerce application. User has to get the information at one click and with proper feedback. As these are web based applications efficiency matters a lot for this application.
Hence security is important in e-commerce application. After identifying all trust model and their drawbacks, we can add some other security concerns to transaction security of e-commerce applications. The major concerns of security are given to the transactional data which is stored in the database. The steps are as follows

1. Studying the attacks and trust models for e-commerce application.
2. Designing security measures to overcome these attacks on database system and to build strong trust mechanism.
3. Testing the mechanism
4. Increasing the performance of e-commerce application.

In this system we are concentration on application-level security (i.e. authentication and authorization) and database security. We are not concentrating on network related part. Designing these third-party components is done by the parties that develop them and, therefore, cannot be controlled by e-commerce system providers.

3.1 Client Side security

It is provided by using proper authentication, authorization and access control enforcement. The following are the different modules of application level security.

3.1.1 User Authentication Module

Services and users use the two-way certificate authentication .Only when the services think the user as legitimate users, the user can access business applications systems. For authentication we can use encryption of password to provide confidentiality. Before using digital signature, the password is salted. Salt is just a string of random characters that get appended to the password before hashing. Salt should be a random string of characters at least as long as the output of the hash function. Each password should be hashed with a different salt. When passwords are changed, the salt must be changed.

3.1.2 User Authorization module

It define a general authorization evaluation service that computes whet her a set of credentials and samples are authorized to perform a specific operation on a specific object.

3.1.3 User Access Control Enforcement

It defines access control list for a particular customer whether that customer has rights to access the specific part of the system or not.

3.2 Database module

It provide stable storage for security-related data objects, including cryptographic keys, user information, customer transactional data etc.

3.2.1 Data Encryption

After users log on after authentication. All the data transmitted between the user and service on the network is encrypted, until the user quit the system. And encryption key of each session is generated randomly. So it is very difficult for the attacker to get the message from network.

3.2.2 Digital Signature

The message is encrypted by the sender's private key. The digital signature is submitted to the server together with the original data. Digital signatures rely on certain types of encryption to ensure authentication. Encryption is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode. Authentication is the process of verifying that information is coming from a trusted source. These two processes work hand in hand for digital signatures. The digital signature scheme done in the following sequence:

1. The sender creates a message.
2. SHA-1 hashing code is used to generate a 160-bit hash code of the message.
3. The hash code is encrypted with RSA using the sender's private key, and the result is prep ended to the message.
4. The receiver uses RSA with the sender's public key to decrypt and recover the
5. The receiver generates a new hash code for the message and compares it with the decrypted hash code. If the two match, the message is accepted as authentic. The combination of SHA-1 and RSA provides an effective digital signature scheme. Because of the strength of RSA, the recipient is assured that only the possessor of the matching private key can generate the signature. Because of the strength of SHA-1, the recipient is assured that no one else could generate a new message that matches the hash code and, hence, the signature of the original message. Instead of SHA-1 we can use SHA-256 hashing code to create hash code of 256-bit.

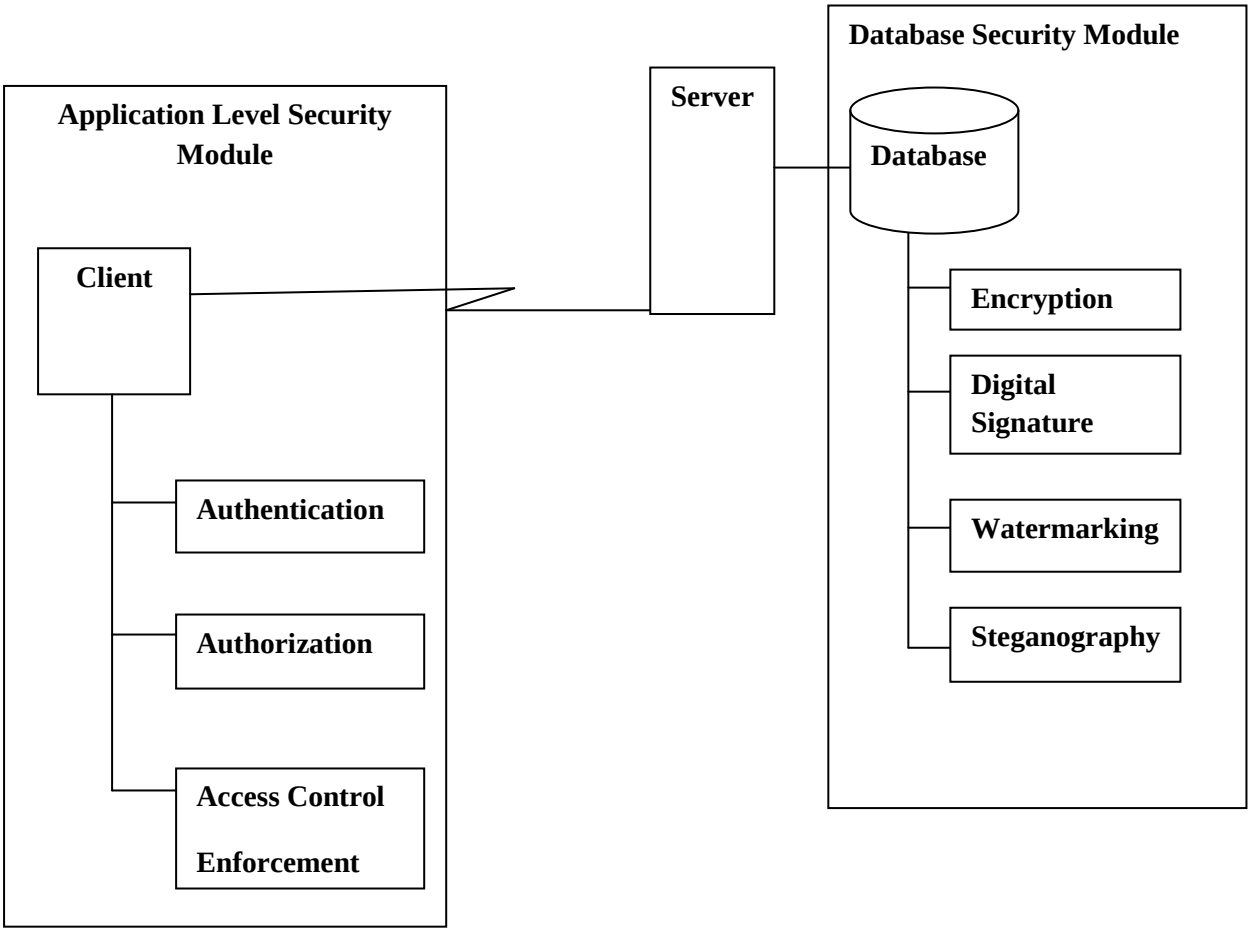

Fig 1: Proposed System Architecture

3.2.3 Watermarking

We can provide copyright protection for database using relational database watermarking. In server side system the original relational tables are extracted from the database to apply watermarking. This data is partitioned and we can embed watermark bits in the least significant bits(LSB) using single bit encoding algorithm. Before sending it to the client side system we apply the encryption algorithm to the watermarked data for providing security. If attacker copies the watermarked relational data he/she never read the content.

3.2.4 Steganography

By using staganography, we can hide the encrypted watermarked relational database in image. Hence by using combination of all the above security measures, it will be difficult for attacker to steal or modify any data. At client side first the data is retrieved from the image which is encrypted watermarked database which is further goes into decryption process to get original watermarked relational data

Table I Comparison Table for Dimensions of E-Commerce & Network Security

SECURITY DIMENSION	ASPECT OF SECURITY PROVIDED	HOW IS IT ACHIEVED?
Integrity	Protects from Alteration	Hash Coding
Non-Repudiation	Proof Transaction Occurred	1-Server Log Files 2 - Digital Signature – Provides a Time Stamp (can use a Digital Time Stamp

		Service)
Authenticity	Proof of Identity	Digital Signature
Privacy & Confidentiality	Keeping Messages Private	Encryption
Availability & Authorization (Necessity)	Controlling Access	Passwords, Access Levels, Policies & Procedures

4. CONCLUSION

Successfully integrating security technologies into a trust infrastructure is the key to ensuring secure e-commerce: This is the first step in establishing trust. Here security is provided at various levels. Authentication is done by using salt with hash value which is difficult to break. Also encryption and decryption process will be done to securing the watermarking relational database. And again the encrypted watermarked relational database is stored in an image using steganograpphy. Hence even an attacker copy the watermarked relational data it is not in human readable format.

5. REFERENCES

[1] Vijay Ahuja," Building Trust in Electronic Commerce", IEEE/2000

[2] Stuart Feldman, "The Changing Face of E-Commerce: Extending the Boundaries of the Possible", IEEE INTERNET COMPUTING, MAY • JUNE 2000

[3] Timothy E. Lindquist, "Security Considerations for Distributed Web-Based e-commerce Applications in Java", IEEE/2002

[4] Adam Jolly, "The Secure Online Business" (Great Britain and the United States- Kogan Page Limited 2003)

[5] Donal O.Mahony, Michael Peirce Hitesh Tewari, "Electronic Payment Systems for E-Commerce" (Artech House computer security series-Boston 2001)

[6] Rafae Bhatti, Elisa Bertino, Arif Ghafoor, "XML-Based Specification for Web Services Document Security", IEEEE 2004

[7] Sung-Ming Yen and Chi-Sung Laih, "Improved Digital Signature Algorithm", IEEE TRANSACTIONS ON COMPUTERS, VOL. 44, NO. 5. MAY 1995

[8] L. Harn," Enhancing the security of EIGamal's signature Scheme," IEEE Vol. 142, No. 5, September 1995

[9] Simson L. Garfinkel, "Public key cryptography", June-1996

[10] Ingemar J. Cox, Senior Member, IEEE, and Jean-Paul M. G. Linnartz, "Some General Methods for Tampering with Watermarks", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 16, NO. 4, MAY 1998

[11] Jana Dittmann, "Using Cryptographic and Watermarking Algorithms", IEEE/2001

[12] Kjell Orsborn, "E-COMMERCE and SECURITY", Spring 2008

[13] PATRICIA BEATTY, IAN REAY, SCOTT DICK, and JAMES MILLER, "Consumer Trust in E-Commerce Web Sites: A Meta-Study", ACM Computing Surveys, Vol. 43, No. 3, Article 14, Publication date: April 2011

[14] PETER C. CHAPIN, CHRISTIAN SKALKA, and X. SEAN WANG," Authorization in Trust Management: Features and Foundations", ACM Computing Surveys, Vol. 40, No. 3, Article 9, Publication date: August 2008.

[15] Nagarjuna. Settipalli,, R Manjula, "Securing Watermarked-Relational Data by Using Encryption and Decryption", Volume 1 No. 2, MAY 2011 , ARPN Journal of Systems and Software.

[16] Dieter Gollmann, "E-commerce security", COMPUTING AND CONTROL ENGINEERING JOURNAL, JUNE 2000

[17] Radu Sion, Mikhail Atallah, Fellow, IEEE, and Sunil Prabhakar, "Rights Protection for Relational Data", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 16, NO. 12, DECEMBER 2004

[18] Yingjiu Li, Member, IEEE, Vipin Swarup, and Sushil Jajodia, Senior Member, IEEE," Fingerprinting Relational Databases:Schemes and Specialties", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 2, NO. 1, JANUARY-MARCH 2005

[19] Shiuh-Jeng Wang, Jia-Hung Huang, Concerns about Hash Cracking Aftereffect on Authentication Procedures in Applications of Cyberspace , IEEE A&E SYSTEMS MAGAZINE, JANUARY 20073

[20] Xiangrong Xiao Xingming Sun Minggang Chen, Second-LSB-Dependent Robust Watermarking for Relational Database , 0-7695-2876-7/07 $25.00 © 2007 IEEE DOI 10.1109/IAS.2007.25

[21] Haiting Cui, Xinchun Cui, Mailing Meng, A Public Key Cryptography Based Algorithm for Watermarking Relational Databases* , 978-0-7695-3278-3/08 $25.00 © 2008 IEEE DOI 10.1109/IIH-MSP.2008.194

[22] Jianhua Sun,Zaihui Cao, Zhongyan Hu ,Multiple Watermarking Relational Databases Using Image , 978-0-7695-3556-2/08 $25.00 © 2008 IEEE DOI 10.1109/MMIT.2008.211