ISSN: 2321-7782 (Online)
Impact Factor: 6.047

Volume 4, Issue 6, June 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

An analysis of E-Commerce Security Threats and Its Related Effective Measures

Varsha Jotwani[1]
Research Scholar of Computer Science Dept
AISECT University
Bhopal – India

Dr. Amit Dutta[2]
Deputy Director
AICTE
Delhi – India

Abstract: E-commerce Security is a part of the Information Security framework and is specifically applied to the components that affect e-commerce that include Computer Security, Data security and other wider realms of the Information Security framework. Authentication of an e-commerce smart card transaction is the process through which a merchant verifies the validity of the payment information provided by the customer. The process involves the verification of both the cardholder's identity and the card's authenticity. Address Verification Service enables merchants who accept credit card payments in a non-face-to-face setting to compare the billing address (the address to which the card issuer sends its monthly statement for that account) provided by a customer to the billing address on the card issuer's file before processing a transaction. Ecommerce offers the banking industry great opportunity, but also creates a set of new risks and vulnerability such as security threats. Information security, therefore, is an essential management and technical requirement for any efficient and effective Payment transaction activities over the internet.

Keywords: Data Security Threats, Smart Card, E-Commerce, Authentication.

I. INTRODUCTION

Authentication is the process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system E-commerce application and individuals are assigning progressively greater amounts of security-sensitive data to computers, both their individual and those of third parties. To be admirable of this expectation, these computers must ensure that the data is handled with care (e.g., as the user expects), and protected from external threats. A progressively more IT-based and virtual mode of human contact in the business and private world as they enable services such as payment, access and multimedia-based communication. They are becoming important enablers in the identification of individuals. Further, internet-based services are increasingly provided through mobile devices. Hence, the security and privacy issues that already exist in the World Wide Web gain importance for the mobile world too.The combination of current business practices, consumer fears, and media pressure has combined to make privacy a potent problem for electronic commerce. Tackling privacy, however, is no easy matter. If nothing else, privacy discussions often turn heated very quickly. Some people consider privacy to be a fundamental right; others consider it to be a tradable commodity.

E-commerce transactions can be categorized into business to business (B2B), business to consumer (B2C), consumer to consumer (C2C), and public/private sectors to government [1].The main focus of this paper is on threats directly related to e-commerce systems. Attacks applicable to authentication in the domain of E-Commerce systems.

II. AUTHENTICATION AND RELATED SECURITY THREAT

Authentication can be accomplished in many ways. The importance of selecting an environment appropriate authentication Method is perhaps the most crucial decision in designing secure systems. Authentication protocols are capable of simply authenticating the connecting party or authenticating the connecting party as well as authenticating itself to the connecting party. Authenticationis the process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system [2] .The identity of a certain user or process is challenged by the system and proper steps must be taken to prove the claimed identity. This section provides a description of the above authentication-related security attacks. For each attack, enablers are then derived, and proper counter measures are prescribed.

A) Sniffing attacks

Sniffing attacks[1],[2],[3],[4] are the digital analogues to phone tapping or eavesdropping. This type of attacks captures information as it flows between a client and a server. Usually, a malicious user attempts to capture TCP/IP transmissions, because they may contain information such as usernames and passwords. A sniffing attack is often classified as a man-in-the-middle attack because in order to capture packets from a user, the machine capturing packets must lie in between the two systems that are communicating. The *attack enabler* in this case is the process of sending data across communication channels in clear text format. Preventing access to the communication channel is not a valid countermeasure in this case due to the open nature of the Internet. By encrypting the communication channel between the user/process and the system, sniffing attacks can be defeated, i.e., sniffing cannot retrieve any useful information.

B) Phishing Attacks

One of the biggest threats to your E-Commerce customers is that of Phishing. Specifically, Phishing can be defined as "the act of sending anE-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft."

All Phishing e-mail contains a link, or a web address, in which the customer clicks on thinking that they are going to secure and legitimate site (people who launch Phishing schemes [also known as "Phishers"] can copy the HTML code from your E-Commerce site, making it look authentic in the eyes of the customer). The truth is, all of the confidential information submitted is collected by the "Phisher", who is bent upon creating havoc and damage to your E-Commerce business.

C) Brute-force attacks

A Brute-force attack [2], [4], [7] is any form of attack against a credential information file that attempts to find a valid username and password in succession. This type of attack is *enabled* by gaining access to the credentials' (user names and passwords) storage medium. The attacker retrieves a copy of the database system or system file preserving credential information. If the credential information is encrypted, a brute-force attack tool will try all possible combinations of user names and passwords. For each combination, the user name and password that was originally used to encrypt the credential information. Then, the encrypted credential data are compared to the retrieved copy of original credential data. Different types of encryption algorithms are used and the attack proceeds until both credentials (user name and password) match. The countermeasure for this type of attacks is to enforce access permissions through a strong access control policy at the operating system level.

D) IP Spoofing

The intent here is to change the source address of a data packet to give it the appearance that it originated from another computer. With IP Spoofing, it is difficult to identify the real attacker, since all E-Commerce server logs will show connections from a legitimate source. IP Spoofing is typically used to start the launch of a Denial of Service Attack.

E) Trapdoors/Backdoors

In developing the code for an E-Commerce site, developers often leave "trapdoors" or "backdoors" to monitor the code as it is developed. Instead of a implementing a secure protocol in which to access the code, backdoors provide a quick way into the code. While it is convenient, trapdoors can lead to major security threats if they are not completely removed prior to the launch of the E-Commerce site. Remember, an attacker is always looking first for vulnerabilities in the E-Commerce server.

Trapdoors provide a very easy vulnerability for the attacker to get into, and cause system wide damage to the E-Commerce server.

F) Other Security threats

Other Security threat [8] Denial of service, Unauthorized access, Theft and fraud Security (DOS): Denial of Service (DOS),Two primary types of DOS attacks: Spamming and Viruses, Sending unsolicited commercial emails to individuals,E-mail bombing caused by a hacker targeting one computer or network, and sending thousands of email messages to it. Surfing involves hackers placing software agents onto a third-party system and setting it off to send requests to an intended target.

- DDOS (distributed denial of service attacks) involves hackers placing software agents onto a number of third-party systems and setting them off to simultaneously send requests to an intended target
- Viruses: self-replicating computer programs designed to perform unwanted events. Worms: special viruses that spread using direct Internet connections.
- Trojan Horses: disguised as legitimate software and trick users into running the program Security*(unauthorized access)*
- Illegal access to systems, applications or data.
- Passive unauthorized access –listening to communications channel for finding secrets.
- May use content for damaging purposes.
- Active unauthorized access.
- Modifying system or data–Message stream modification.
- Changes intent of messages, e.g., to abort or delay a negotiation on a contract
- Masquerading or spoofing –sending a message that appears to be from someone else.
- Impersonating another user at the name(changing the ―From field) or IP levels (changing the source and/or destination IP address of packets in the network).
- Sniffers–software that illegally access data traversing across the network. Software and operating systems ‘security holes *Security (theft and fraud).*
- Theft of software via illegal copying from company‘s servers
- Theft of hardware, specifically laptops.

III. Secure Electronic Payment Protocol Design

Our main idea is to design a secure and efficient solution to protect online payment transactions against the fraud without involving the third party, our protocol respond to the requirements of e-payment security: confidentiality, integrity, authentication and non-repudiation.

In the services industry – and particularly in services which are based on electronic devices – a new paradigm seems to be emerging: The conscious management of identity in a secure service context. Quality of Service (QoS) has already become an indispensable attribute as a foundation to this understanding. Hence, QoS is already defined in the deployment of any service architecture. Treating Security of Service (SoS) [9] as a similarly crucial attribute of a service calls for an exploration and definition of the term. It is obvious that security needs a kind of trust secure. Such a security attach allows the user:

To define a secure domain, which also is context-dependent (home/family, friends, work, travel).To deal with the user's individual background so that the management of the user's device base is both secure and easy. To define which of his devices can be publicly or restrictedly accessed and how interactions occur. A secure client in combination with a trusted component in a mobile device can serve as a security anchor in the overall SoS concept [10] and system architecture. The Security of Service (SoS) concept can be expected to expand alongside three phases. These phases are not only significant to await the distinctiveness of upcoming security constraints, but can also assist to pin-point the definition of the concept alongside its anticipated path of development. Therefore, essential the SoS-concept [10] could be accomplished in 3 steps. These match the respectively needed capability tiers:

Security requirements in a static environment: This will consider fixed and concrete client and server components, actors and scenarios. The definition of SoS will result in fixed security requirements for the given circumstances. At this stage, SoS behaviour can be increased and modified in the client and server component.

Security rules in a dynamic environment: This will consider the heterogeneity of scenarios. The definition of SoS will result in security rules. The equipment, context-aware, will know rules of behaviour under unusual circumstances. The SoS will be transformed in a condition-definite manner according to the rules defined during the pre-expansion. For this reason, the SoS is dynamic and co-develops with the isotropic and steadily changing context into which it is embedded. This move toward is comparable to the technique in which Euro pay, MasterCard, and Visa (EMV4) consider security in different and continuously changing scenarios.

Security policies in an adaptive environment: This will consider unidentified tools, actors, and heterogeneity of gap. The explanation of SoS will consequence in security policies. The client and the server will know the policies. Both will consider whether a given service is to be continued or blocked for a dedicated actor in definite circumstances. In an adaptive environment, QoS and SoS take a "flexible and safe", "pervasive and protected", "resilient and sheltered", "recoverable and safe" character, depending on the condition. The user and the server components will deploy an adaptive SoS and QoS ad hoc by negotiating the SoS according to the agreed security policies.

IV. Security Goals and its Measures

There are some detailed security control measures in the ISO 7498-2 Standard lists [11]. For example, there are involving authentication, access Control, data confidentiality data integrity and non-repudiation.

Security hinges on two very simple goals:

1. Keeping unauthorized persons from gaining access to resources
2. Ensuring that authorized persons *can* access the resources they need

There are a number of components involved in accomplishing these objectives. One way is to assign access permissions to resources that specify which users can or cannot access those resources and under what circumstances. (For example, you may want a specific user or group of users to have access when logged on from a computer that is physically on-site but not from a remote dial-up connection.) Access permissions, however, work only if you are able to verify the identity of the user who is attempting to access the resources. That's where authentication comes in. In this Daily Drill Down, we will look at the role played by authentication in a network security plan, popular types of authentication, how authentication works, and the most commonly used authentication methods and protocols.

Authentication and security Authentication is an absolutely essential element of a typical security model. It is the process of confirming the identification of a user (or in some cases, a machine) that is trying to log on or access resources. There are a number of different authentication mechanisms, but all serve this same purpose. Security Authentication process can be shown through figure1.

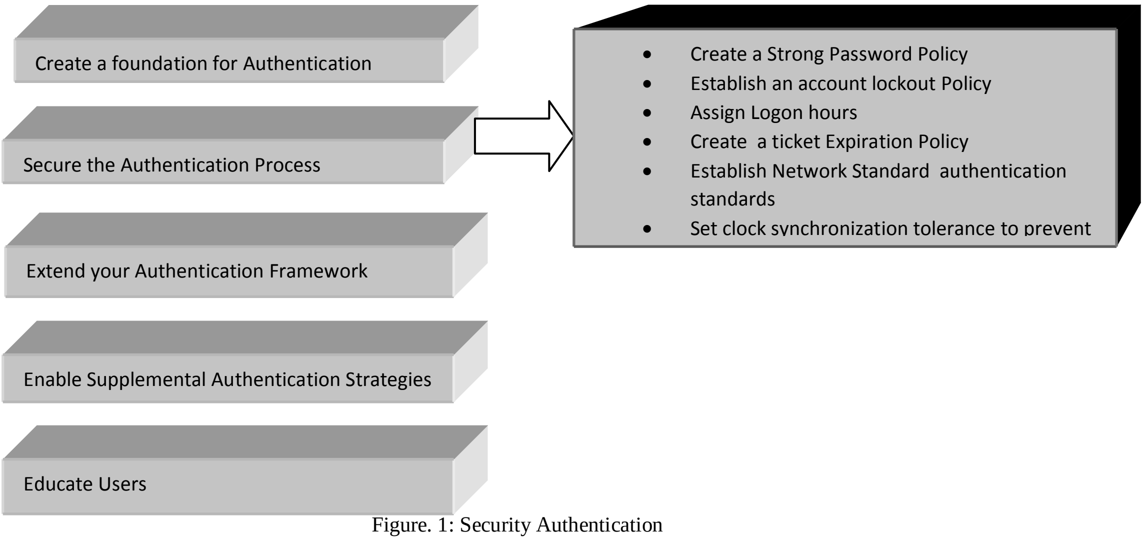
Create a foundation for Authentication
Secure the Authentication Process
Extend your Authentication Framework
Enable Supplemental Authentication Strategies
Educate Users
Create a Strong Password Policy
Establish an account lockout Policy
Assign Logon hours
Create a ticket Expiration Policy
Establish Network Standard authentication standards
Set clock synchronization tolerance to prevent

Figure. 1: Security Authentication

V. Smart Cards Capability and Token Technology

The main usage of Smart Cards is the storage of highly confidential information, for example cryptographic keys, and the implementation of safety measures critical processes, such as an authentication to prove the identity of a person or device. Classical Smart Card use cases are [12], [13]:

- Authorization in announcement networks, such as mobile phone networks or the Internet,
- Execution of security-critical processes with banking and payment applications, e.g. credit and debit operations on an electronic purse,
- Storage of sensitive personal information, e.g. on health and identity cards,
- Physical and logical access control.

Major Smart Card milestones in the past were the introduction of the SIM (Subscriber Identity Module) as the security device in mobile networks and the invention of Java on Smart Cards, i.e. the JavaCard™ Standard. With JavaCard™ the flexibility of Smart Cards amplified, because it was the initial time achievable to develop Smart Card applications in an interoperable format. The so-called JavaCard™ Applets can be executed in an almost interoperable manner on different JavaCards™ from different Smart Card vendors. With the ever-increasing computing capability of µProcessor Smart Cards new opportunities appear. Newer Smart Cards, connected to a host over the USB interface, present a full TCP/IP stack in the operating system. These Internet-Smart Cards no longer depend on a PC to be able to communicate because they can act independently as a network node in a global network like the Internet. So, they possibly will provide as a good security mechanism for personal data in combination with information exchange in a cross-domain network. A person can determine, which information about her/him/is published by help of the communication gateway Internet-Smart Card that supports standard Web technologies like HTML (hypertext markup language) pages and HTTP (hypertext transfer protocol). Therefore, the Internet-Smart Card [14] hosts a Smart Card Web Server (SCWS) which acts as graphical user interface for the individual token. The Internet-Smart Card expertise and SCWS also appear in the future USIMs in mobile networks. On the client side, a web-like look and think simplifies information exchange with a Smart Card. such as, clients browse a phone book or FAQ list based on HTML pages stored directly on the Smart Card Web Server (SCWS) hosted on the (U) SIM. On the provider side, an HTTP-based keep informed mechanism simplifies the exchange of content with previously issued (U) SIMs. In conjunction with the Internet technology on Smart Cards, the assortment of dissimilar data types accumulated on the Smart Card and delivered by the SCWS is considerably increasing.

VI. Trusted Computing and its Platform module

Trusted computing initiatives intend to solve some of today's safety measures crisis of the fundamental computing platforms from side to side hardware and software transforms. The most important initiative for a new generation of computing platforms is the TCG, a grouping of a large amount major IT companies. Trusted computing is a rather new technology driven by the Trusted Computing Group (TCG) [15]. Its goal is secure personal computing. Unlike the usual procedure of finding a fixing bugs which allow an attacker access to a system trusted computing uses cryptography to measure a systems condition. The system's condition depends on the software components which are executed as well as on the sequence of implementation. Any situation transform designates revolutionize in software system. An alteration in software system can be generated by a regular software update as well as by a piece of injected malicious code. The foundation of the scheme circumstances transform has not to be known.

VII. Conclusion

The market analysis of various e-commerce application we did gave us an suggestion on what a protection component is, what it does, how it does what it does, how high-speed computing and safe it does what is does, and on the collision of expenditure. The information draw together showed an opening e-commerce application advertises. Business modules are also low-cost or high-cost and less make safe or more protected correspondingly.

References

1. HASSLER, V. (2001). Security fundamentals For E-Commerce. ARTECH HOUSE, MASSACHUSETTS
2. NIST, National Institute of Standards and Technology, 2001. “Underlying Technical Models for Information Technology Security”, 2001. Special Publication 800-33. Retrieved from: http://csrc.nist.gov/publications/
3. Herzog, P. 2001. “The Open Source Security Testing Methodology Manual”, version 1.5.Retrieved from http://ideahamster.org/
4. Viega, J. and McGraw, G. 2002. “Building Secure Software”, Addison-Wesley.
5. Nguyen, H. 2001. “Testing Applications on the Web”, 285-310, John Wiley & Sons.
6. Schneier, B. 2000. “Secrets and Lies: Digital Security in a Networked World”, John Wiley & Sons
7. Anderson, R. 2001. “Security Engineering: A Guide to Building Dependable Distributed Systems”, John Wiley & Sons. ISBN: 0-471-38922-6
8. Randy C. Marchany, Joseph G. Tront, "E-Commerce Security Issues "Proceedings of the 35th Hawaii International Conference on System Sciences – 2002
9. Sailer, R., Zhang, X., Jaeger, T., and van Doorn, L. Design and Implementation of a TCG-based Integrity Measurement Architecture. In 13th USENIX Security Symposium (2004), USENIX, pp. 223–238.
10. A. D. Keromytis, V. Misra, and D. Rubenstein. SOS: Secure overlay services. In Proceedings of ACM SIGCOMM, 2002.
11. F. Farahmand, S. B. Navathe, G. P. Sharp and P. H. Enslow, “A Management Perspective on Risk of Security Threats to Information Systems”, Information Technology and Management, vol. 6, (2005).
12. Rankl, W.; Effing, W. (2002) Handbuch der Chipkarten, 4th edition, Munich, Carl Hanser Verlag.
13. Swoboda, J., Spitz, S., Pramateftakis, M. (2008) Kryptographie und IT Sicherheit, Wiesbaden, Vieweg-Teubner, ISBN 978-3-8348-0248-4.
14. InspireD (2005) D6 Communication Architecture Definition (Draft), forthcoming on http://www.inspiredproject.com,.
15. Trusted Computing Group. http://www.trustedcomputinggroup.org/ (05 April 2010).