ISSN No. 0976-5697

Volume 1, No. 4, Nov-Dec 2010

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Striking the Security Issues in E-commerce: A Conceptual Framework

Umesh Kumar Singh
Reader,
ICS, Vikram University,
Ujjain(M. P.) India

Shreeram Gupta*
Reader,
Shri Vaishnav Institute of Management
Indore (M. P.) India
gupta_shreeram@rediffmail.com

Abstract: Without trust, most prudent business operators and clients may decide to forgo use of the Internet and revert back to traditional methods of doing business. To counter this trend, the issues of network security at the ecommerce and customer sites must be constantly reviewed and appropriate countermeasures devised. These security measures must be implemented so that they do not inhibit or dissuade the intended e-commerce operation. This paper focuses on major network and computer security issues which are specific to eCommerce and Internet.

Keyword: E-commerce, Computer Security,Internet,Network Security

I. INTRODUCTION

Commercial activities over the Internet have been growing in an exponential manner over the last few years.
The eradication of trust in Internet commerce applications may cause prudent business operators and clients to forgo use of the Internet and revert back to traditional methods of doing business. This loss of trust is being fueled by continued stories of hacker attacks on e-commerce sites and consumer data privacy abuse [1].

When it comes to payment, one needs to establish a sense of security. Customers must be able to select a mode of payment and the software must verify their ability to pay. This involves credit cards, electronic cash, encryption, and/or purchase orders. The more of these techniques are supported by an E-commerce package, the more secure the system can be, and therefore the more customers are benefits from E-commerce abilities [2], [3].

For the effective operation of the web and e-commerce applications, security is a key issue. The security threats include access control violations, integrity violations, sabotage, fraud, privacy violations, as well as denial of service and infrastructure attacks. All of these threats collectively have come to be known as cyberwar or cyberterrorism. Essentially cyberwar is about corrupting the web and all of its components so that the enemy or adversary's system collapses. There is currently lot of money being investigated by the various governments in the US and Western Europe to conduct research on protecting the web and preventing cyberwars and cyberterrorism [12].

E- Commerce business has 4 different elements consists of components to build business to consumer, All of these elements combined give the store a personality & the end uses a true shopping experience [3].

A. Product Catalog.
B. Shopping Cart.
C. Transaction Security.
D. Order Processing.

II. SECURITY AND E-COMMERCE

It is clear that electronic commerce will revolutionize businesses, and customers will be offered new and exciting services. As E-commerce businesses are growing, more secure technologies are being developed and improved every day. The current Internet security polices and technologies fail to meet the needs of end users. The success or failure of an E-commerce operations hinges on myriad factors, including but not limited to the business model, the team, the customers, the investors, the product, and the security of data transmissions and storage. Any business that wants to have a competitive edge in today's global marketplace should adopt a comprehensive security policy in consultation with partners, suppliers, and distributors that will provide safe environment for the coming proliferation of E-commerce [2][6].

III. MAIN SECURITY ISSUES?

Accountability -- Security relevant activities on a system can be traced to individuals who may be held responsible for their actions.
Availability -- System resources are safeguarded from tampering and are available for authorized users at the time and in the format needed
Access Control -- Access to the system resources is limited to authorized individuals, entities, or processes
Confidentiality -- Information is not accessed by or disclosed to unauthorized individuals, entities, or processes
Identification and Authentication -- Verification that the originator of a transaction is the originator
Integrity -- Information is not undetectably altered or destroyed by an unauthorized person or process
Non-repudiation-- Undeniable proof of participation by the sender and/or receiver in a transaction
Privacy – individual rights to nondisclosure

IV. DIFFERENT PERSPECTIVES OF SECURITY

A. User's point of view(Client-side security)

B. Server's point of view(Server-side security)
C. Both parties(Document confidentiality)

Client-side security

Measures to protect the user's privacy and the integrity of his computer Example technological solutions

[a] Protection from computer viruses and other malicious software
[b] Limit the amount of personal information that browser's can transmit without the user's consent. Any others?

Server-side security

Measures to protect the server and the machine it runs from break-ins, site vandalism, and denial-of-service attacks.

Solutions range

[a] installing firewall systems
[b] tightening operating systems security measures

Document confidentiality

Measures to protect private information from being disclosed to third parties.

Solutions range

[a] Password to identify users
[b] Cryptography

V. LISTING OF MAJOR SECURITY ISSUES AND THEIR COUNTER EFFECTS OF NOT IMPLEMENTING THE SAME

A. User Authentication

Customers must be identified through the use of a User ID and password, as a minimum. Strong authentication mechanisms such as digital certificates and hard tokens should be used for proprietary or highly restricted systems.

Insecure access to a customer account could result in misuse of customer specific information and it is very dangerous.

B. Inter-process/Inter-machine communication and authentication

E-Commerce infrastructure must be built to ensure secure inter-process/inter-machine communication and authentication.

Insecure inter-process/inter-machine communications and authentication are security threats and could be used to compromise the systems.

C. Software and security patches

All necessary recommended vendor software and security patches should be installed and properly configured for E-commerce systems.

Failure to install the latest recommended security patches could result in the systems becoming vulnerable to new attack methods.

D. System and configuration file security

System and configuration files for all E-commerce systems should only be viewable by the Administrator.

Failure to properly secure system and configuration files could result in modifications by unauthorized personnel that could result in the addition of significant security vulnerabilities.

E. Physical security

All E-commerce related hardware components should be in a physically secure environment, such as a card-access data center.

The lack of adequate physical security around the E-commerce components could result in unauthorized changes to the systems.

F. Three tier architecture

E-commerce architecture must be separated physically and logically into three separate components: the Web server; the Application server; and the Database server (E-commerce systems). The data should be stored behind a firewall and accessed through an application proxy A single tier E-commerce architecture exposes the web server as a single point of attack.

G. Web server placement

The web server must be placed behind a firewall, and the firewall must be configured to allow connections to the web server only on ports and services required for business reasons. The Web server should reside on its own segment, separate and distinct from other servers.

Not having the web site behind a firewall exposes the web site to direct attacks.

H. Web server access

Ensure no update or write access is allowed to the web server file system.

Update or write access could be misused to hack the web site. The compromised web server could then be used to launch attacks on the other E-commerce systems.

I. Critical and confidential data Encryption

Proprietary data traveling between the web browser and web server must be encrypted.

Information could be compromised if it passes unencrypted over the Internet.

J. Stored transaction data Encryption

Ensure that transaction data is encrypted as it is stored.

If transaction data, which is comprised of customer specific confidential information, is not stored securely, an unauthorized user could access this information in a readable format.

K. Transaction processing

Transactions must initiate and complete on the application server, not the web server.

Transactions contain critical data and if not secured could result in unauthorized access of that data. If the web server sits in the unsafe zone, it is considered to be in an insecure environment.

L. Session security and timeouts

Session keys must be indecipherable, have unique values, and should provide for secure sessions to be logged out by the user or to time out automatically.

Sessions are not terminated properly they may allow a user to connect to a session without getting authenticated again, which can be misused to gain access to a customer's account.

© 2010, IJARCS All Rights Reserved

M. Content management

The content management system must ensure that no erroneous information, such as incorrect product pricing, inaccurate customer data, or proprietary product details, is published. Also ensure that content management access is configured securely.

Liabilities of erroneous content delivery could be enormous, and an insecure content management access could result in compromise of the systems and its critical data.

N. Domain Name Server (DNS) configuration

The DNS must be properly configured to not advertise internal hosts. Configure the DNS to only advertise hosts to which you wish to allow access from the Internet. No other hosts should appear in the Internet accessible DNS tables. Do not allow zone transfers from the Internet to internal zones.

Failure to properly configure the DNS often results in information leakage about the corporate network. Information gathering is typically the first step a hacker will use when attacking a network. Misconfigurations in the DNS could also result in a denial of service attack.

O. Account management

Minimize the number of administrator and system accounts on E-commerce systems.

The greater the number of system administrator accounts, the greater the possibility of unauthorized access to a highly privileged account. This can result in unauthorized access to all information in the system.

P. Backup and restoration procedures

E-commerce systems should be backed up regularly, and restoration procedures should regularly be tested to validate the integrity of the backups.

Failure to properly backup the E-commerce systems could result in the loss of configuration information as well as system files, security log files, and data.

Q. System and configuration file security

System and configuration files for all E-commerce systems should only be viewable by the Administrator.

Failure to properly secure system and configuration files could result in modifications by unauthorized personnel that could result in the addition of significant security vulnerabilities.

R. Conflicting software

The web server should only be running web server software. No other software packages should be installed unless a sufficient business need exists.

Rogue processes could compromise security not only of the web server, but also the internal hosts, through the introduction of back doors. Unnecessary processes could also strain the operating system resources thereby affecting web server performance.

S. Remote administration

Remote administration should be performed through appropriate vendor software by a small number of administrators. The remote solution should support two-factor authentication such as secure IDs or digital certificates. Additionally, the entire session should be logged.

The use of inappropriate software for remote administration could introduce programs into the system that compromise the integrity of the commerce systems. Inappropriate software also could inadvertently turn on insecure services for remote administration.

T. Vulnerability scanning

The E-commerce systems should periodically be scanned with vulnerability scanners to determine if the system is vulnerable to new exploits.

Without periodic vulnerability scanning, a new vulnerability or exploit may be introduced into the system without the system administrator's knowledge.

U. Redundancy

Where necessary, redundant fail-over systems and procedures should exist for all E-commerce-supporting systems.

Redundant systems are necessary to improve the availability of the E-commerce-supporting systems, and to reduce the time necessary to recover from a system failure.

V. Operating system security

E-commerce systems must be installed on a securely configured and maintained operating system.

Weak operating system level controls could lead to compromise of the systems or denial of service.

W. Intrusion detection & Incidence response procedures

The E-commerce infrastructure must include a real time intrusion detection system. This must also be supported with incidence response procedures to ensure incidences are responded to and escalated in an appropriate and timely manner.

Lack of an Intrusion detection system and incidence response procedures may result in unauthorized activities being undetected. Undetected intrusions are likely to result in increased damages due to a longer period of unauthorized access.

X. Privacy policy

If the web site collects personally identifiable information the web site's privacy policy should notify users of what information is collected by the web site; with whom the information may be shared; and what kind of security procedures are in place to protect the information.

Consumer data privacy is an extremely sensitive issue in today's business world. Consumers are becoming increasingly aware of their privacy rights and hence increasingly reluctant to give out personal details on the Internet. Lack of a privacy policy may result in litigation.

Y. Cyber Process Certification

An E-commerce web site must have a Seal of Trust or a Cyber Process Certification performed. This helps build web site credibility and customer trust, thus increasing the value of the site. The certification process is usually performed by a trusted third party.

This will help mitigate customer's fear of operating in an insecure environment.

Z. Customer Service functions

Customer Service functions must only be accessed via the internal network and access should be secured. Also, if a customer requests a reset of their password, a confirmation of their new password should be sent only to the address of record.

If the customer service function is not secured it could be misused to get unauthorized access to customer data.

[a] Logging and monitoring

Logging must be enabled on all E-commerce systems. In addition to meeting regular logging requirements, all Customer Service activity should also be logged.

Failure to enable logging for customer service activity could result in security breaches going undetected.

[b] Service Level Agreements

E-commerce services managed by the service providers should have comprehensive service level agreements ensuring security.

Service level agreements define the quality of service, which if not specified clearly could result in poor service support.

VI. CONCLUSIONS

The e-commerce industry is slowly addressing security issues on their internal networks. There are guidelines for securing systems and networks available for the ecommerce systems personnel to read and implement. Educating the consumer on security issues is still in the infancy stage but will prove to be the most critical element of the e-commerce security architecture.

Complete Training programs, orientation programs, Guest lectures on eCommerce security will increase the general awareness of security on the Internet.

IT and financial control/audit groups within the ecommerce site should form an alliance to overcome the general resistance to implementing security practices at the business level.

VII. REFERENCES

[1] Randy C.Marchany and Joseph G. Tront, E-Commerce Security Issues**,** Proceedings of the 35th Hawaii International Conference on System Sciences – 2002

[2] David J. Olkowski, Jr., “Information Security Issues in ECommerce”, SANS GIAC Security Essentials, March 26, 2001.

[3] Paul A. Greenberg, “In E-Commerce We Trust…. Not”, E-Commerce Time, February 2, 2001, URL: http://www.ecommercetimess.com/perl/story/id=7194

[4] William Stallings, “Cryptography and network Security”, 3rd edition, Prentice Hall,2003.

[5] Michall E. Whitman and Herbert J. Maiiord, “Information Security”, Thomson, Inc. 2003.

[6] Dave Chaffey, “E-Business and E-Commerce”, 2nd, Prentice Hall, 2005

[7] Mark Merkow. Jim Breithaupt, "Information Security Principles and Practices", Pearson Prentice Hall, 2006.

[8] A. Coulibaly & A. Inam .” Security Issues Facing E-Commerece”,From Internet http://WWW.ACM.COM

[9] Peter Keen. Ensuring E-Trust. ComputerWorld, 3/13/00 issue"Distributed System Intruder Tools - Trinoo and Tribe Flood Network", Computer Incident Advisor Capability, Lawrence Livermore National Laboratory, CIAC 00.040,12/21/99

[10] Ravi Kalakota, Andrew B. Whinston. Electronic Commerce: A Manager’s Guide, Addison-Wesley, ISBN: 0-201-88067-9

[11] William Safire. The Phantom of the Internet. New York Times Service, article appeared in 6/4/00 issue of the Roanoke Times.

[12] B.Thuraisingham, Chris Clifton, Amar Gupta, Elisa Bertino & Elena Ferrari. Direction for Web an E-Commerce Application Security

[13] Protiviti Inc. e Com Sec Best Practices. Available at http://www.knowleader.com

© 2010, IJARCS All Rights Reserved