IJEE 0973-7383 Volume-9 • Number-1 Jan -June 2017 pp. 49-53 available online at www.csjournalss.com
A UGC Recommended Journal http://ugc.ac.in/journallist

Analyzing Risks of Security and its challenges in E-Commerce

Divya Shree

Abstract: With the emergence of the Economy, and with an ever-increasing percentage of consumers doing their business primarily via e-commerce, is fast being regarded as the way to go global at the touch of a button. Hence, developing an effective E-Commerce model is becoming vital for any modern business. E-Commerce Security has some main issues. They are interception of data, redirection of data, identification of parties, exploitable program errors, and being the weakest point in security. When administrating a secure e-commerce site, it is important to remember that you are part of a link of systems.This paper presents the conceptual components of the e-commerce in general, and identifies and classifies the different types of security challenges and risksin e-commerce.

Keywords: E-commerce security, security challenges, risks.

INTRODUCTION

Security is the challenge and the main problem for successful e-commerce implementation, as stated by many researchers. However, there is wide agreement between academic researchers that security is not only a technical challenge; rather it involves managerial, organizational and human dimensions to be more effective. Most current e-commerce transactions are conducted by users in fixed locations using workstations and personal computers. Soon, we expect a significant portion of e-commerce will take place via wireless, Internet-enabled devices such as cellular phones and personal digital assistants. Wireless devices provide users mobility to research, communicate, and purchase goods and services from anywhere at anytime without being tethered to the desktop. Using the Internet from wireless devices has come to be known as mobile e-commerce, or simply "m-commerce," and encompasses many more activities than merely online purchasing. One of the major wireless applications is Web access for retrieval of real-time information such as weather reports, sport scores, flight and reservation information, navigational maps, and stock quotes. While email will continue to dominate wireless applications, innovative online applications that, for instance, use location reference information of end users will drive new areas of mobile e-business growth.

E-commerce 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. E-commerce security has its own particular nuances and is one of the highest visible security components that affect the end user through their daily payment interaction with business. In spite of the seemingly unlimited potential to drive new applications and markets in mobile e-commerce, new security and privacy risks particular to the wireless medium and devices abound in m-commerce applications. Integrating security and privacy into online m-commerce applications will enable a projected $25 billion market in wireless software, content, and commerce. On the other hand, failing to provide a secure system of m-commerce will significantly dampen consumer adoption rates.

The Internet has allowed for very low cost access to a giant network of people and businesses. This combination of low cost technology and pervasive access to the Internet provides the basis for a radical transformation of the way everybody will conduct business. E-Commerce offers the opportunity to integrate external and internal processes and to lower transaction costs, thus expanding distribution channels and increasing sales and profits. However, internet has introduced new security issues and challenges for E-Commerce. Even as the general form factor of mobile computing devices has been drastically reduced, the computing capacity has grown significantly. Today's handheld devices have computing power equivalent to their desktop-computing counterparts of only one generation earlier. This phenomenon, while driving more and more functionality into handheld wireless Internet-enabled devices, is also driving security risks endemic to desktop computing into wireless devices.

Therefore, understanding (and acting upon) the customer's perception of security is vital to successful e-commerce interactions, because even when a company uses the best technical solutions that provide full security, without the underlying perception and awareness from customers that their particular website is secure, then these technical solutions may mean nothing.

CHALLENGES AND SECURITY RISKS IN E-COMMERCE

The advent of e-commerce was touted as an incomparable solution to traditional business premise that only had the ups and no downs. But soon business organizations realized that like every solution there are two sides of the coin.Ecommerce has its own set of challenges and issues. In a e-Commerce system security hardware, software, and environment are the main critical and vulnerable points. Hardware security includes any devices used in running the e-Commerce website like network devices, web servers, database servers and client's computer. Securing the network with a properly configured firewall device that is only allowing ports needed for accessing the e-Commerce website is an essential part of network security. While the Web and the internet technologies offer a powerful platform for launching new virtual stores and instant access to millions of consumers around the world, e-businesses are subject to the traditional security issues and to a variety of new security challenges. Many companies now have large e-business departments and some like amazon.com base their entire business model around e-business. Breaking into the online sales world can be extremely profitable, but it also has its fair share of security issues.

Before implementing an e-Commerce plan, you have to address the security of your systems and data to ensure that people who shouldn't be accessing data can't get at it and to ensure that your system will be available despite attempts at a denial-of-service attack which is one of the most troublesome security issues facing e-businesses. A denial of service attack can make e-Commerce systems inaccessible to thousands or millions of consumers. In addition, no one will deal with an e-Commerce that may distribute, accidentally due to a security attack, sensitive consumer data such as credit card number, personal information, financial and account information, or other access information like user id and password. To elaborate more on these vulnerability issues, consider this simplified e-commerce scenario where a user uses a web site for an e-Commerce system and gives his/her credit card number and address information for buying and shipping the purchased items.

Even this is a simple on-line transaction, it has many potential security vulnerabilities that are related to the number of systems and networks involved which include the following:

- Security problems in client/home computers where data stored in web "cookie" can be stolen and cracked by hostile web-sites, or mail-borne viruses that can steal the user's financial data from the local disk.
- Rather than an attacker needing to pursue a target, targets can come to attackers in wireless networks simply by roaming through the attacker's zone.
- Eavesdropping and data stealing due to ineffective encryption or lack of encryption in home wireless networks.
- Malicious hackers can compromise wireless connections even without exploiting cooperative ad hoc networks at the transport level.
- Eavesdropping and data stealing from the user's keystrokes at Point-of-Sale (POS) terminals in brick-and-mortar stores.
- Risk of loss or theft: Without physical perimeter security provided by buildings, locks and guards, mobile computing devices are at increased risk of theft and loss, particularly given their small size. While the data stored on a misplaced device might be irreplaceable or proprietary, other risks of lost Internet-enabled devices include the ability for finders of lost devices to access proprietary corporate systems, including email servers and file systems. One of the key problems with the current generation of handheld devices is the lack of good mechanisms to authenticate a particular user to a particular device.
- Eavesdropping and data stealing from the user's mobile and handheld devices.

- In addition to the issue of security, m-commerce applications introduce new and significant privacy risks to end users.

- Eavesdropping and data stealing from networks and different intermediate communication links.

- The wireless medium also provides excellent cover for malicious users. Users of wireless devices can be difficult to trace because wireless devices roam in and out of wireless zones, have no fixed geographic point, and can go online and offline easily.

- In addition to contending with the usual Internet security threats in online applications, wireless devices introduce new hazards specific to their mobility and communication medium.

- Firewall problems or insecure merchant's web and database servers or third party fulfillment servers and other processing agents that leads to hacking the archives of recent and old purchasing orders with all the financial and personal information.

- Location-oriented services provide the ability for online Web sites, including marketers, to determine your geographic location with a certain degree of precision. Combining this data, an online marketer will know not only a user's personal preferences such as cuisine and music, but also the user's precise geographic location at all times.

Although we have discussed some of the security measures like data encryption, authentication, and authorization may alleviate some of the above security problems; there are still lots of vulnerabilities in other areas.

Wireless devices pass through many different, potentially non-trustworthy networks from which service is derived and data is exchanged. Information can be stolen or altered without the end user's knowledge. Service can be, and is often, easily denied, whether inadvertently or not. Transactions can be interrupted and then reinstated, often without re-authenticating principals. Simply "refreshing" a browser to reestablish the connection may inadvertently introduce risks. Reestablishing connections and transactions without re-authenticating principals on both sides of the transactions can be dangerous. Requests can be redirected and malicious code surreptitiously downloaded with expected Web data. Most Web sites are not currently configured to deal with intermittent service failures, as is common with wireless connections. Most vendor implementations of the Secure Sockets Layer (SSL) or its wireless counterpart (WTLS) do not re-authenticate principals or recheck certificates once a connection has been established. Attackers can use this vulnerability to their advantage in wireless networks.

In summary, mobile e-commerce systems will introduce new security and privacy risks beyond those currently found in desktop e-commerce systems. Using wireless devices for m-commerce will result in new vulnerabilities and potentially represent a new weak link in e-commerce. Since attackers tend to exploit the weakest link in a chain, the security risks of wireless devices must be carefully analyzed and addressed.

RISKS IN SOFTWARE SECURITY IN E-COMMERCE

Much ado has been made about the security of wireless transport protocols such as the Wireless Application Protocol (WAP). The WAP advocates argue that the Wireless Transport Security Layer (WTLS) provides a secure infrastructure for m-commerce applications. Critics have decried the infamous "WAP gap" where wireless requests to Web pages are translated at the WAP gateway from the WTLS protocol to the standard SSL protocol widely used in secure HTTP requests. In the process of translating one protocol to another, the data is decrypted and then re-encrypted. If an attacker is able to compromise the WAP gateway, then simply capturing the data when it is decrypted can compromise the secure session. In reality, these issues are red herrings that draw attention away from the more substantive vulnerabilities in m-commerce systems: the software systems that run on both ends of the session. Some of the addressing for software security are:

- Security risks of wireless devices must be carefully analyzed and addressed.

- “WAP gap”

  - Wireless requests to web pages are translated at the WAP gateway from the WTLS protocol to SSL protocol, widely used in HTTP requests.
  - If an attacker compromises the WAP gateway, could capture data when decryption is done.

- WAP gap problem
  - Should be solved by simple modifications to existing protocols.
- Low level languages
  - In handheld devices cause the continuation of basic flaws like Buffer overflow etc.
- Application developers may forgo security features like encryption etc
  - Due to Limited power, lack of Processing cycles, memory and bandwidth of the devices
  - To increase online performance.
- Interesting software development
  - The ability to send & execute mobile code.
- WML script is used to overcome software application risks.

The "WAP gap" problem will likely be solved in the near future by simple modifications to existing protocols. Traditionally speaking, data encryption over communication channels has been the strongest perceived security element in the system. As a result, malicious hackers tend to ignore the security provided by encryption protocols and simply attack the weakest links in the system, such as servers and clients. The problem of providing server-side security for wireless Web access closely mirrors the problem of providing server-side security in fixed-wire e-commerce and is well understood and documented. One exacerbating factor in wireless Web server security, however, is the fact that there are currently few wireless gateways or portals to the wired Web. Thus, those few gateways present ideal targets of opportunity or single points of failure for an attacker to bring down a significant portion of the wireless Web by selective denial-of-service attacks.

To prevent a number of cybercrimes and simple mistakes, such as not insuring that all traffic into and out of a network pass through firewall, security of e-commerce systems should be considered from the very beginning, i.e. early stage of the e-commerce software development. This is due to software vulnerabilities are a huge security problem. Therefore, to enhance security of e-commerce software, we propose the use of multi-agent system. The research in this paper is focused mainly on the design of agents that provide support to engineers during development process. Moreover, the multi-agent system, presented in this research, supports implementation of patterns and extraction of security information, and provides traceability of security requirements in the engineering process. For several reasons, scripting will also have ample uses in the wireless Web. First, client-side processing is attractive for reducing the number of communication hits necessary on extremely bandwidth-limited wireless links. For instance, client-side form validation reduces unnecessary server-side error reports and reentry messages. Second, some server-side processing can be off-loaded to clients using mobile code that will increase the availability of servers to more simultaneous connections. Third, scripting will be pervasive in wireless Web computing for the same reason it has become ubiquitous in wired Web pages: Web page development heavily leverages JavaScript for display functions and client-side transaction processing.

CONCLUSION

While many of the risks of desktop Internet-based commerce will pervade e-commerce, e-commerce itself presents new risks. The best strategy for addressing the challenges and security risks of Internet-based content is to build security into the platform and applications themselves, rather than attempt to introduce security patches afterward. For instance, Java provides type safety, memory protection, and sandboxing for un-trusted content. While history has shown that various implementations of the Java virtual machine have not been perfect, its model of secure computation is relatively good. The device manufacturers and the language developers for wireless applications should leverage the decades of progress in secure operating system models and secure models of computation before going forward with business-critical and privacy-related wireless applications. Hacking, identity theft, credit card stealing, bank information stealing, etc. are some of the greatest security issues that hinder the consumer from trusting online businesses. Eventually, this means loss of potential business for organizations.Ecommerce security challenges are however, not limited to consumers. Businesses and corporate firms also face security challenges as their vital information, records and most importantly their reputation is at stake.

REFERENCES

[1]. S. Y. Hui and K. H. Yeung, "Challenges in the Migration to 4G Mobile Systems," IEEE Communication Magazine, vol. 41, no. 12, Dec. 2003, pp.54-59.
[2]. Bill Krenik ," 4G Wireless Technology: When will it happen? What does it offer?", IEEE Asian Solid-State Circuits Conference, November 3-5, 2008 / Fukuoka, Japan
[3]. Zhang Jian, The Development Trends of 4G Technology, GUANGDONG COMMUNICATION TECHNOLOGY,2004
[4]. N. M. A. Al-Slamy, "E-commerce security," IJCSNS, vol. 8, no. 5, 2008.
[5]. King, Brett (2014), Breaking Banks – The innovators, rogues, and strategists rebooting banking, Singapore: Wiley.
[6]. Krishnan, Sankar (2014), The power of mobile banking, New Jersey: Wiley.
[7]. M. Yenisey, A. Ozok, and G. Salvendy, "Perceived security determinants in e-commerce among Turkish university students," Behaviour & Information Technology, vol. 24, no. 4, pp. 259-274, 2005.
[8]. C. Centeno, "Soft Measures to build security in e-Commerce payments and consumer trust," Communications & Strategies, vol. 51, 2003.
[9]. S. M. Furnell, "Considering the Security Challenges in ConsumerOrientedeCommerce," The 5th IEEE International Symposium on Signal Processing and Information Technology, Athens, Greece, 2005, pp. 534-539.
[10]. A. Strauss, and J. Corbin, Basics of qualitative research: grounded theory procedures and techniques. SAGE Publication, London, 1990.
[11]. S. L. Jarvenpaa, N. Tractinsky, and M. Vitale, "Consumer trust in an - internet store," Information Technology and Management , vol. 1, no. (1/2), pp. 45–72, 2000.
[12]. B. Suh and I. Han, "The impact of customer trust and perception of security control on the acceptance of electronic commerce," International Journal of Electronic Commerce, vol. 7, no. 3, pp. 135-161, 2003.
[13]. Rappaport, "Wireless communication", Third edition Jun-zhao Sun ， .Features in Future ： 4G Visions from A TechnicalPerspective[C].IEEE Global Telecommunications Conference 2001.Vol 6.
[14]. V. Gazis, "Evolving Perspectives of 4th GenerationMobile Communication Systems," IEEE PIMRC 2002,Coimbra, Portugal, Sept.2002.
[15]. Li Weiwei, Comparison and Transition of Key Technologies on 3Gand 4G,GUANGDONG COMMUNICATION TECHNOLOGY,2004.
[16]. Marcus L. Roberts, Michael A. Temple, Robert F. Mills, and Richard A. Raines, "Evolution of the air interface of cellular communicationssystems toward 4G realization", IEEE Communications Surveys & Tutorials, vol. 8, no. 1,1st Quarter 2006, pp. 2-22.
[17]. Mishra, Ajay K. "Fundamentals of Cellular NetworkPlanning and Optimization, 2G/2.5G/3G…Evolution of 4G", John Wiley and Sons, 2004.
[18]. Pereira, Vasco & Sousa, Tiago. "Evolution of Mobile Communications: from 1G to 4G", Department of Informatics Engineering of the University of Coimbra,Portugal 2004.
[19]. Kamarularifin Abd Jalil, Mohd Hanafi Abd. Latif, MohamadNoormanMasrek, "Looking Into The 4G Features",MASAUM Journal of Basic and Applied Sciences Vol.1,No. 2 September 2009
[20]. Fumiyuki Adachi, "Wireless past and Future: Evolving Mobile Communication Systems". IEICE Trans. Findamental, Vol. E84-A, No.1, January 2001.
[21]. E. Awad, "Electronic commerce: From vision to fulfillment," Prentice Hall, 2002.
[22]. Y. Wen and C. Zhou, "Research on e-commerce security issues," International Seminar on Business and Information Management, 2008.
[23]. Litan, Avivah. "Visa's Long-Overdue US EMV Move Will Improve Security, but Do little to Alleviate PCI Compliance Work", Gartner, September 13, 2011.
[24]. Mills, Elinor. "Google now scanning Android apps for malware", February 2, 2012.