International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 9, Sept.-2014, pp: (90-96), Impact Factor: 1.252, Available online at: www.erpublications.com

E-Commerce Software Security based on Risk Management Perspective: A Literature Survey

Sumeer Kumar, Sumit Kumar

Abstract: In the past, the majority of the computer security officers had difficulty in convincing management to allocate financial resources for IT security. However, with the emergence of electronic commerce and varied legislation, organizations appear to have understood the necessity for computer security, especially data security. Electronic commerce can help enterprises reducing costs, obtaining greater market and improving relationships between buyers and sellers. At the same time, new risks and threats have also occurred, such as, mutual trust, intellectual property, network att3.acks and so on. This paper analyzes the threat classification and control measures in E-commerce softwares and on this basis, a conceptual risk management framework is provided. Enterprises engaged in e-commerce can use the framework to improve their security.

Keywords: E-commerce, Security, software, issues.

I. Introduction

Security threats in mobile commerce can range from passively eavesdropping into others' message to actively stealing user's data. In a radio frequency operated mobile commerce, with minimum difficulty it is possible to listen to one's conversation. This has an impact for consumers because they are concerned about their data and voice messages from unauthorised access. On the other end of the problem is the inherent security risk involved in transferring information over the networks.

In addition to the above, other security concerns in e-commerce arise due to the new development in technology itself. The mobile technology is envisaged in such a way that the services offered will eventually warrant payment for the type of services offered. This is already emerging in the domain of mobile telephones. For instance, when mobile telephone users access other network carriers, a special charge is levied on the users. Therefore, it is safe to assume that there will not be any "free services" in the future. The technology is developing in such a way that the payment for such services will be through some form of "smart cards." The details stored in the smart cards need to be transmitted via the networks for validation and verification in order to determine service levels. If these networks are not fully secure, security breaches may occur. In addition to those traditional security issues, we observe that many general-purpose sensor network techniques (particularly the early research) assumed that all nodes are cooperative and trustworthy. This is not the case for most, or much of, real-world wireless sensor networking applications, which require a certain amount of trust in the application in order to maintain proper network functionality. Researchers therefore began focusing on building a sensor trust model to solve the problems beyond the capability of cryptographic security. In addition, there are many attacks designed to exploit the unreliable communication channels and unattended operation of wireless sensor networks. Furthermore, due to the inherent unattended feature of wireless sensor networks, we argue that physical attacks to sensors play an important role in the operation of wireless sensor networks. Thus, we include a detailed discussion of the physical attacks and their corresponding defenses topics typically ignored in most of the current research on sensor security. One major security breach that can happen in mobile commerce is when the user details are transferred from one mobile network to another.

When this transformation occurs, any encrypted data needs to be decrypted for transparency. In mobile commerce, when mobile devices make requests to web pages of a network server, a four-stage process is followed.

II. Software Security Threats that can Impact Financial Transactions

Security risks in a mobile commerce environment associated with financial transactions can be rganizatio into traditional risks and non-traditional risks. Traditional risks usually involve loss or damage to tangible physical assets and resulting economic loss. For example, loss of computer hardware may have an impact on incomplete transaction. Alternatively, a data disk, which is not fully protected from theft, can place an rganization into some form of risk. Treatment of traditional risks is usually addressed in risk management policies. Protecting tangible assets from traditional perils, even when those assets are devoted to mobile commerce, does not involve new and different techniques. These security treats are beyond the scope of this paper.

Non-traditional security breaches also include any rganization access or use of a company's computer system and data by an outsider or insider. For example, a hacker could break into a company's computer system and steal or destroy data. Widespread use of mobile commerce enhances the possibility of an outsider invading an rganization's computer system. Due to businesses reliance on computers for their daily operations, breaches of a company's computer or information security system are a risk to almost all functional components of businesses. Use of software to encrypt and, thus, safeguard communications provides some protection, but also adds a risk that a virus or other bug could damage equipment or data. Further, according to Dang, theft of information such as critical electronic files that include financial data, customer information, marketing and new product data, trade secrets, and personnel data may provide competitors with a strategic advantage, criminals with the means to commit fraud, and others the opportunity to disparage the company.

Addressing the Software Risks

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.

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.

In the remainder of this article, we focus on the software security risks of wireless devices that present the most significant and least-understood security and privacy risks in m-commerce applications.

III. A Model for Threat Classification and Control Measures of e-commerce

This part will provide a model to analyze the threat classification and control measures of e-commerce. Firstly, we consider threats from two points of view: threat agents and threat techniques. Then we analyze the security control measures.

Threat Agents

Threat agents include 3 parts: environmental factors, authorized users and unauthorized users.

A. Environmental Factors

Environmental factors are common sense. It is more prone to certain environmental influences and natural disasters than others in some areas. For example, fire is not geographically dependent. However, tornadoes and floods can be predicted in specific areas. In addition to the natural disasters, the danger of mechanical and electrical equipment failure should be paid to more attention. So is the interruption of electrical power.

B. Authorized users

There are some potential threats when authorized users and personnel are engaged in supporting operations. Especially they exceed their privileges and authorities. It may affect the ability of the system to perform its mission. Personnel should be considered as potential threats, when they have the access to a system or occupy positions of special trust. Because they have the capability or opportunity to abuse their access authorities, privileges or trusts. And it may bring danger to the system.

C. Unauthorized users

An unauthorized user can be anyone who is not engaged in the system. It can attempt to interrupt the operation of the system overtly or covertly. It may sabotage hardware and associated equipment. And it also could be accomplished through the manipulation of software.

Threat Techniques

Techniques can be classified into 5 types: physical, personnel, hardware, software, and procedural.

A. Physical

It implies to use a physical means to enter into restricted areas, for example, building, compound room or other areas.

B. Personnel

Personnel are the people who have authority or privilege to access a system, either as users or operators. Penetration techniques and methods generally deal with them. Threat agent may recruit them to penetrate the system, operation or facility. They themselves can become motivated to make an attack.

C. Hardware

Attacks using the characteristics of the hardware may involve a physical attack against the equipment, a bug implanted within a hardware controller or an attack against the supporting utilities. The purpose of it is to subvert or deny use of the system [9]. In this category, hardware generally includes any kind of equipment of the system, such as power supplies, air conditioning systems and so on.

D. Software

Software attacks have a large scope from discreet alterations to less discreet changes. The discreet alterations are subtly imposed for the aim of compromising the system. And the less discreet changes intend to bring the result of destruction of

data or other system features. Techniques can penetrate the software, application programs or utility routines to threat the system.

E. Procedural

If the system is lack of adequate controls or existing controls are failure, authorized or unauthorized users can penetrate the system. For example, if former employees retained the used valid passwords, unauthorized personnel may pick up output. This is a procedural penetration.

IV. Security Counter Measures

There are some detailed security control measures in the ISO 7498-2 Standard lists. For example, there are involving authentication, access Control, data confidentiality data integrity and non-repudiation. Computer security experts widely accept this classification. And they are also recommended by the authors good control measures [11]. The threat agent, threat technique and security measures are shown in Figure 1.

In this section, we discuss some of the counter measures. For example, access control is one of the security measures. It can face the threats that may be caused by an unauthorized user through hardware. Totally, there are combinations with agents, threat techniques, and security measures. However, not all of these combinations are available. We just utilize this three-dimensional view for a better security risk management.

Outsider attacks and link layer security

The majority of outsider attacks against sensor network routing protocols can be prevented by simple link layer encryption and authentication using a globally shared key. Major classes of attacks not countered by link layer encryption and authentication mechanisms are wormhole attacks and HELLO flood attacks because, although an adversary is prevented from joining the network, nothing prevents her from using a wormhole to tunnel packets sent by legitimate nodes in one part of the network to legitimate nodes in another part to convince them they are neighbors or by amplifying an overheard broadcast packet with sufficient power to be received by every node in the network.
Link layer security mechanisms using a globally shared key are completely ineffective in presence of insider attacks or compromised nodes. Insiders can attack the network by spoofing or injecting bogus routing information, creating sinkholes, selectively forwarding packets, using the Sybil attack, and broadcasting HELLO floods. More sophisticated defense mechanisms are needed to provide reasonable protection against wormholes and insider attacks. We focus on countermeasures against these attacks in the remaining sections.

The Sybil attacks

An insider cannot be prevented from participating in the network, but she should only be able to do so using the identities of the nodes she has compromised. Using a globally shared key allows an insider to masquerade as any (possibly even nonexistent) node. Identities must be verified. In the traditional setting, this might be done using public key cryptography, but generating and verifying digital signatures is beyond the capabilities of sensor nodes. One solution is to have every node share a unique symmetric key with a trusted base station. Two nodes can then use a International Journal of Next-Generation Networks (IJNGN),Vol.1, No.1, December 2009 Needham-Schroeder like protocol to verify each other's identity and establish a shared key. A pair of neighboring nodes can use the resulting key to implement an authenticated, encrypted link between them. In order to prevent an insider from wandering around a stationary network and establishing shared keys with every node in the network, the base station can reasonably limit the number of neighbors a node is allowed to have and send an error message when a node exceeds it. Thus, when a node is compromised, it is restricted to (meaningfully) communicating only with its verified neighbors. This is not to say that nodes are forbidden from sending messages to base stations or aggregation points multiple hops away, but they are restricted from using any node except their verified neighbors to do so. In addition, an adversary can still use a wormhole to create an artificial link between two nodes

to convince them they are neighbors, but the adversary will not be able to eavesdrop on or modify any future communications between them.

Leveraging Global Knowledge

A significant challenge in securing large sensor networks is their inherent self organizing, decentralized nature. When the network size is limited or the topology is well structured or controlled, global knowledge can be leveraged in security mechanisms. Consider a relatively small network of around 100 nodes or less. If it can be assumed that no nodes are compromised during deployment, then after the initial topology is formed, each node could send information such as neighboring nodes and its geographic location (if known) back to a base station. Using this information, the base station(s) can map the topology of the entire network. To account for topology changes due to radio interference or node failure, nodes would periodically update a base station with the appropriate information. Drastic or suspicious changes to the topology might indicate a node compromise, and the appropriate action can be taken. We have discussed why geographic routing can be relatively secure against wormhole, sinkhole, and Sybil attacks, but the main remaining problem is that location information advertised from neighboring nodes must be trusted. A compromised node advertising its location on a line between the targeted International Journal of Next-Generation Networks (IJNGN),Vol.1, No.1, December 2009 node and a base station will guarantee it is the destination for all forwarded packets from that node. Probabilistic selection of a next hop from several acceptable destinations or multipath routing to multiple base stations can help with this problem, but it is not perfect. When a node must route around a "hole", an adversary can "help" by appearing to be the only reasonable node to forward packets to. Sufficiently restricting the structure of the topology can eliminate the requirement for nodes to advertise their locations if all nodes' locations are well known.

Authenticated Broadcasting

If we have base stations trustworthy, adversaries must not be able to spoof broadcast or flooded messages from any base station. This requires some level of asymmetry: since every node in the network can potentially be compromised, no node should be able to spoof messages from a base station, yet every node should be able to verify them. Authenticated broadcast is also useful for localized node interactions. Many protocols require nodes to broadcast HELLO messages to their neighbors. These messages should be authenticated and impossible to spoof. Proposals for authenticated broadcast intended for use in a more conventional setting either use digital signatures and/or have packet overhead that well exceed the length of typical sensor network packet. TESLA is a protocol for efficient, authenticated broadcast and flooding that uses only symmetric key cryptography and requires minimal packet overhead. SPIN and gossiping algorithms are techniques to reduce the messaging costs and collisions which still achieve robust probabilistic dissemination of messages to every node in the network.

V. Discussion on Security Requirements

When a financial transaction is facilitated in a mobile commerce environment, usually the consumer accesses the organisation’s computer to search for appropriate details. Once the consumer is satisfied with his/her order, an order is placed. The consumer places an order using the infrastructure provided by the Internet storefront and using his or her payment method of choice. Once the order reaches the organisation, the transaction is processed. A number of security issues such as verifying the credentials of the consumer arise at this point. Provision for real-time security and connectivity to authorise payment via the Internet or wireless medium forms an integral component of the transaction. The organisation involved in the transaction channels the transaction through various financial networks such as banks, ensuring that customers are authorised to make their purchase.

For the purposes of transaction authorisation, the client software establishes a secure link with the processing server over the Internet using an SSL connection, and transmits the encrypted transaction request. The server, which is a multi-threaded processing environment, receives the request and transmits it over a private network to the appropriate financial processing network. Depending upon the consumer’s financial status, the transaction is approved or denied. When the authorisation

response is received from the financial network, the response is returned via the same session to the client on your site. The client completes the transaction session by transparently sending a transaction receipt acknowledgement to the server before disconnecting the session. The whole transaction is accomplished in few seconds, including confirmation back to the customer and the organisation. If the transaction is approved, funds will be transferred to the organisation's account. Once the transaction is confirmed, the transaction will be securely routed and processed. As proof of a securely processed transaction, both the customer and the organisation will receive a transaction confirmation number.

Data Integrity

With the implementation of confidentiality, an adversary may be unable to steal information. However, this doesn't mean the data is safe. The adversary can change the data, so as to send the sensor network into disarray. For example, a malicious node may add some fragments or manipulate the data within a packet. This new packet can then be sent to the original receiver. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, data integrity ensures that any received data has not been altered in transit.

Data Freshness

Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when there are shared-key strategies employed in the design. Typically shared keys need to be changed over time. However, it takes time for new shared keys to be propagated to the entire network. In this case, it is easy for the adversary to use a replay attack. Also, it is easy to disrupt the normal work of the sensor, if the sensor is unaware of the new key change time. To solve this problem a nonce, or another time-related counter, can be added into the packet to ensure data freshness.

Self-Organization

A wireless sensor network is a typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security as well. For example, the dynamics of the whole network inhibits the idea of pre-installation of a shared key between the base station and all sensors [21]. Several random key predistribution schemes have been proposed in the context of symmetric encryption techniques [13, 21, 37, 53]. In the context of applying public-key cryptography techniques in sensor networks, an efficient mechanism for public-key distribution is necessary as well. In the same way that distributed sensor networks must self-organize to support multihop routing, they must also self-organize to conduct key management and building trust relation among sensors.

Time Synchronization

Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor's radio may be turned off for periods of time. Furthermore, sensors may wish to compute the end-to end delay of a packet as it travels between two pairwise sensors. A more collaborative sensor network may require group synchronization for tracking applications, etc. In [24], the authors propose a set of secure synchronization protocols for sender-receiver (pairwise), multihop sender-receiver (for use when the pair of nodes are not within single-hop range), and group synchronization.

Software Application Risks

While the operating system provides the basic platform for wireless applications, the software applications that run on the device are equally important. Assuming that basic platform services listed previously are provided to applications, it is

possible to design and develop secure wireless applications using good software engineering and assurance methods. The relation between software flaws and security vulnerabilities is well understood. The daily software bug postings to the BugTraq list provide ample evidence of security holes introduced by software flaws.

Software development for wireless devices will be no different in this respect. Flaws in the logic and implementation can certainly result in security holes that will be exploited by attackers or malicious Web sites. Low-level languages typically used for development in handheld devices will ensure the continuation of basic flaws such as buffer overflow flaws. Furthermore, the physical limitations of a device often force application developers to make security and performance trade-offs. For instance, limited power, processing cycles, memory, and bandwidth will force application developers to forgo security features such as encryption in an effort to improve online performance. Security features in advanced languages such as Java may be omitted in vendors' JVM implementations. For instance, runtime checking of type safety is expensive, as is implementing fine-grained sandboxes and stack-introspection security features implemented in current desktop JVMs.

One of the most interesting software-related developments in wireless devices is the ability to send and execute mobile code. In the wired world, mobile code is used pervasively in Web pages. Though Java applets brought mobile code to the forefront, by far the most common form of mobile code is JavaScript or Microsoft JScript. Scripting is used extensively in Web pages to validate forms and create the look and feel of Web pages.

Conclusions

E-commerce is widely considered the buying and selling of products over the internet, but any transaction that is completed solely through electronic measures can be considered e-commerce. Day by day E-commerce and commerce playing very good role in online retail marketing and peoples using this technology day by day increasing all over the world. E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction.

Dimensions of e-commerce security; Integrity: prevention against unauthorized data modification, No repudiation: prevention against any one party from reneging on an agreement after the fact. Authenticity: authentication of data source. Confidentiality: protection against unauthorized data disclosure. Privacy: provision of data control and disclosure. Availability: prevention against data delays or removal.

References

[1]. C. Mazumdar Sengupta and M. S. Barik, “E-commerce security-a life cycle approach”, Sadhana, vol. 30, no. 2-3, (2005).
[2]. F.-Y. Leu, C.-H. Lin and A. Castiglione, “Special issue on cloud, wireless and e-commerce security”, Journal of Ambient Intelligence and Humanized Computing, vol. 4, no. 2, (2013).
[3]. M. Xiangsong and H. Fengwu, “Design on PKI-based anonymous mobile agent security in e-commerce”, Wuhan University Journal of Natural Sciences, vol. 11, no. 6, (2006).
[4]. G. Antoniou and L. Battern, “E-commerce: protecting purchaser privacy to enforce trust”, Electronic commerce research, vol. 11, no. 4, (2011).
[5]. R. Smith and J. Shao, “Privacy and e-commerce: a consumer-centric perspective”, Electronic commerce research, vol. 7, no. 2, (2007).
[6]. D. Good and R. Schultz, “E-commerce stratD. Liu and P. Ning. Multilevel µTESLA: Broadcast authentication for distributed sensor networks. Trans. on Embedded Computing Sys., 3(4):800–836, 2004.
[7]. D. Liu, P. Ning, and R. Li. Establishing pairwise keys in distributed sensor networks. ACM Trans. Inf. Syst. Secur., 8(1):41–77, 2005.