SECURITY ISSUES IN THE WEB COMMERCE

M. Gnana Sri, G. Vinni Sheethal, K. V. Sneha Priya

E.C.M., KLUniversity
E.C.M., KLUniversity
E.C.M., KLUniversity

Abstract- WEB commerce security is an important issue that has been leading to negative or adverse effects on the further development and growth of WEB-commerce. We discuss objectives such as security goals integrity, confidentiality, availability and we discussed the security services and how these are related to the three security goals. Here we took the example service namely SET(Secure Electronic Transaction) and in this case study we have discussed some security techniques to avoid this manipulation of the credential data which would guarantee an increased customer base and eventually prove to be very profitable.

Index Terms- Availability, Confidentiality, Integrity, SET;

I. INTRODUCTION

Web is now widely used by business, government and individuals. But both internet and web are vulnerable. So it has a variety of threats such as integrity, confidentiality, denial of services and authentication. Therefore there is a need of added security mechanisms. The utilization of the internet is increasing rapidly every year; availability of low cost peripheral devices and wider internet accessibility options are key contributing factors. This raises a number of risks and issues including technological, security, privacy, trust, legal and other related issues. The following research focuses on the security issues. The factoring of Security in web-commerce models is of considerable importance to consumers, businesses, and regulators. The majority of customers feel insecure towards the existing policies and guidelines with respect to security online. Such insecurities have a negative impact upon any economical model. That said, online security breaches can be considered as a spreading menace in current day economical settings around the world.

Here in this case study, a customer places a request to the merchant to purchase any item. Remember as these are the transactions that are going to takes place through online, we need to purchase the item by using our credit cards or debit cards which are to be linked through the bank. To make the payment we need to use this credit card information. Here is a chance to manipulate this information. So, here in this case study we have discussed some security techniques to avoid this manipulation of the credential data.

Until a few decades ago, the information collected by the organizations are stored on the physical files. The confidentiality of the files is achieved by restricting the access to the few authorized and trusted people in the organization.

Similarly only a few authorized people are allowed to make changes to the content of the files. Availability was achieved by designating at least one person who would have access to the files at all times [1].

II. Security goals

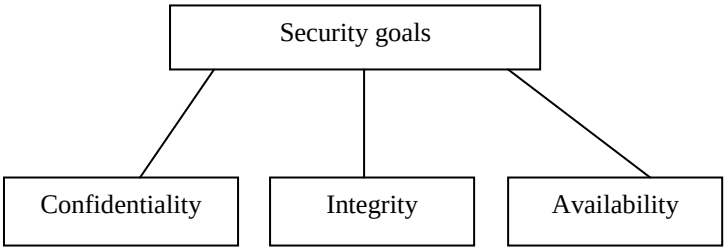

Figure 1: Taxonomy of security goals

A. Confidentiality

Confidentiality refers to limiting information access and disclosure to authorized users "the right people" and preventing access by or disclosure to unauthorized ones "the wrong people." Underpinning the goal of confidentiality are authentication methods like user-IDs and passwords that uniquely identify a data system's users, and supporting control methods that limit each identified user's access to the data system's resources. Also critical to confidentiality and data integrity and availability as well are protections against malicious attacks [2].

B. Integrity

Integrity refers to the trustworthiness of information resources. It includes the concept of "data integrity" namely, that data have not been changed inappropriately, whether by accident or deliberately malign activity. It also includes "origin" or "source integrity" -- that is, that the data actually came from the person or entity you think it did, rather than an imposter. Integrity can even include the notion that the person or entity in question entered the right information -- that is, that the information reflected the actual circumstances (in statistics, this is the concept of "validity") and that under the same circumstances would generate identical data (what statisticians call "reliability"). On a more restrictive view, however, integrity of an information system includes only preservation without corruption of whatever was transmitted or entered into the system, right or wrong [3].

C. Availability

Availability refers, unsurprisingly, to the availability of information resources. An information system that is not available when you need it is at least as bad as none at all. It may be much worse, depending on how reliant the organization has become on a functioning computer and communications infrastructure. Almost all modern organizations are highly dependent on functioning information systems. Many literally could not operate without them. Availability, like other aspects of security, may be affected by purely technical issues (e.g., a malfunctioning part of a computer or communications device), natural phenomena (e.g., wind or water), or human causes (accidental or deliberate). While the relative risks associated with these categories depend on the particular context, the general rule is that humans are the weakest link. (That's why each user's ability and willingness to use a data system securely are critical) [4].

III. Secure Electronic Transaction (SET)

SET is an open encryption and security specification. It protects the credit card transactions on the internet. Companies involved are:

Master card, Visa, IBM, Microsoft, Netscape, RSA and VeriSign. SET is not a payment system. It is a SET of security protocols and formats architecture. As the name implies, the secure electronic transaction (SET) protocol is used to facilitate the secure transmission of consumer credit card information via electronic avenues, such as the Internet. SET blocks out the details of credit card information, thus preventing merchants, hackers and electronic thieves from accessing the information. SET allows merchants to verify their customers' card information without actually seeing it, thus protecting the customer. The information on the card is instead transferred directly to the credit card company for verification. It will protect buyers by providing a mechanism for their credit card number to be transferred directly to the credit card issuer for verification and billing without the merchant being able to see the number [5].

A. SET Services

SET provides a secure communication channel in a transaction. SET ensures the privacy. It provides trust by the use of digital certificates. The SET protocol addresses the payment phase of a transaction from the individual, to the merchant, to the acquirer (the merchant's current bankcard processor). It can be used to help ensure the privacy and integrity of real time bankcard payments over the Internet. In addition, with SET in place, everyone in the payment process knows who everyone else is.

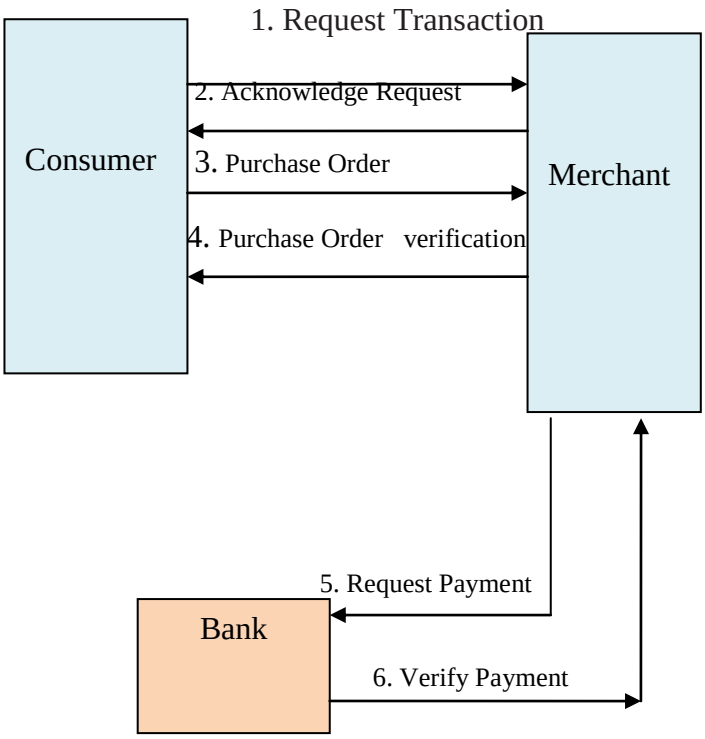

Figure 2: Scenario of SET

The card holder, the merchant, and the acquirer can be fully authenticated because the core protocol of SET is based on digital certificates. Each participant in the payment transaction holds a certificate that validates his or her identity. The public key infrastructure allows these digital certificates to be exchanged, checked, and validated for every transaction made over the Internet. The mechanics of this operation are transparent to the application.

Under the SET protocol, every online purchase must be accompanied by a digital certificate which identifies the card-holder to the merchant. The buyer's digital certificate serves as an electronic representation of the buyer's credit card but does not actually show the credit card number to the merchant. Once the merchant's SET application authenticates the buyer's identity, it then decrypts the order information, processes the order, and forwards the still-encrypted payment information to the acquirer for processing. The acquirer's SET application authenticates the buyer's credit card information, identifies the merchant, and arranges settlement. With SET, the Internet becomes a safer, more secure environment for the use of payment cards [6].

B. Key features of SET

To meet the business requirements, SET incorporates the following features [7]:

- Confidentiality of information
- Integrity of data
- Cardholder account authentication
- Merchant authentication

IV. Security vulnerabilities in web commerce

There are many points of failure, or vulnerabilities, in an web-commerce environment. Even in a simplified web-commerce scenario, a single user contacts a single web site, and then gives his credit card and address information for shipping a purchase many potential security vulnerabilities exist. Indeed, even in this simple scenario, there are a number of systems and networks involved. Each has security issues [8]:

A user must use a web site and at some point identify, or authenticate, himself to the site. Unfortunately, security problems in home computers offer hackers other ways to steal web commerce data and identification data from users. Some current examples include a popular home-banking system that stores a user's account number in a Web "cookie" which hostile web-sites can crack ineffective encryption. While these specific security problems will be fixed by some software developers and web-site administrators, similar problems will continue to occur. Alternatives to the home computer include Point-of-Sale (POS) terminals [9].

The user's web browser connects to the merchant front-end. When a consumer makes an online purchase, the merchant's web-server usually caches the order's personal information in an archive of recent orders. This archive contains everything necessary for credit-card fraud [10].

The merchant back-end and database. A site's servers can weaken the company's internal network. This not easily remedied, because the web servers need administrative connections to the internal network, but web server software tends to have buggy security. Here, the cost of failure is very high, with potential theft of customers' identities or corporate data. Additionally, the back-end may connect with third party fulfillment centers and other processing agents. Arguably, the risk of stolen product is the merchant's least-important security concern, because most merchants' traditional operations already have careful controls to track payments and deliveries. However, these third parties can release valuable data through their own vulnerabilities [11].

V. Recommended steps for security

There are many relevant technologies, including cryptographic technologies that can overcome the above vulnerabilities. The most visible security technologies are the encryption algorithms.

- Public key infrastructure (PKI) systems are one such encryption technology [12]. The PKI is a flexible key-distribution system in which every participant carries two cryptographic keys, one for encryption and one for decryption; together these two keys make up what is called an asymmetric *key pair* [13]. A performance advantage of PKI is that it does not require a centralized, highly available intermediary for every secured transaction; however, this also makes it difficult to know when another party's key has been stolen or otherwise compromised.
- A digital signature [14] is the salient application of public-key cryptography, and is an analog of a handwritten signature. A digital signature is a cryptographic tag that only one author can calculate; the tag can be combined with any kind of data that the author might create (e.g., financial, entertainment, medical); and the tag's validity can be checked by anyone who can access the data.
- Other technologies can be used to perform both authentication and data protection. For example, smart cards can be used to store data about the bearer of the card, including financial data, medical records, identification credentials. Because those data are so sensitive, it is critical to store the associated encryption keys in tamper-resistant hardware. Further, the smartcard shouldn't ever have to share the bearer's personal data or his keys with a POS terminal [15].
- Software developers must develop software to enhance safety and security and provide safety measures like encryption, digital signatures, biometrics, virus protection, etc. Introducing security seals is also advisable. Moreover, educating customers on security issues and how to protect their computers is also a major part of the security implementation process [16].

Therefore, as can be seen, in order for e-commerce security to blossom, it is important to look at it from many different angles, and focus on not only the company's guarantees, but also on customer's needs and the initial software development process. Security must also be achieved in a collective manner rather than individualistic in order to improve the worldwide perception of online security [17].

VI. DISCUSSION

A review of the impact of security issues on web-commerce development reveals that with today's rapid growth and expansion of e-commerce, security concerns are increasing amongst customers. This research tells how customers' perception of possible risks and threats to the security of their personal information affects their online purchasing behavior. Due to the increase in warnings by the media from security breaches like identity theft and financial fraud, and the elevated awareness of online customers about the threats of performing transactions online, e-commerce has not been able to achieve its full potential. Many customers refuse to perform online transactions and relate that to the lack of trust or fear for their personal information. Therefore, in order for e-commerce to expand and achieve its full potential, companies need to understand these needs collectively try and develop systems would ensure the private and secure communication of information between buyers and sellers.

VII. CONCLUSION

The research introduced the issues in the current e-commerce environment, here in this example service namely SET , we have discussed some security techniques to avoid this manipulation of the credential data. This was all done in order to facilitate the further expansion and development of e-commerce. We are living in the information age. Information need to be secured from the attacks. To be secured, information need to be hidden from the unauthorized access (confidentiality), protected from unauthorized change (integrity) and available to authorized entity when it is needed (availability). It elaborated its effect on e-commerce growth, reasons behind it and the importance of providing secure

communication networks and we expect that these studies will bring greater clarity and proficiency.

Acknowledgment

We would like to thank our mam AnuRadha for giving her full support in producing this journal and to our Research group named WEB TECHNOLOGIES which gave us idea to present on this topic. And also we would like to thank our head of the department (H.O.D.) for giving chance to participate in research activities. We are also thankful to our family who gave us a wonderful support in making this.

References

[1] Cryptography And Network Security by Behrouz A.Forouzan, Special Indian Edition, The McGrawHill Companies.

[2] http://en.wikipedia.org/wiki/Confidentiality

[3] http://en.wikipedia.org/wiki/Integrity

[4] http://it.med.miami.edu/x904.xml

[5] http://en.wikipedia.org/wiki/Secure_Electronic_Transaction

[6] Cryptography And Network Security by Behrouz A.Forouzan, Special Indian Edition, The McGrawHill Companies.
[7] http://en.wikipedia.org/wiki/Secure_Electronic_Transaction

[8] Privacy and Security Issues in E-Commerce, Review chapter for the New Economy Handbook (Jones, ed.), in
Mark S. Ackerman and Donald T. Davis, Jr.

[9] Borisov, N., I. Goldberg, and D. Wagner. 2001. Intercepting Mobile Communications: The
Insecurity of 802.1. *Proceedings of the Seventh Annual International Conference on Mobile*
Computing and Networking : 180-189.

[10] Brands, Stefan. 1996. Electronic Cash. Invited talk, RSA Cryptographer's Colloquium.

[11] Brehl, B. 1997. Security of `Cash Cards' Questioned. *Toronto Star*, October 6, 1997, E1-2.

[12] Adams et al. 2001,CCITT 1988, Housley et al. 2002, Polk, Housley, and Bassham 2002
CCITT . 1988. Recommendation X.509: The Directory - Authentication Framework. Data
Communications Network Directory, Recommendations X.500-X.521.

[13] Diffie and Hellman 1976, Rivest, Shamir, and Adelman 1978, Clarke, Roger. 1999. Introduction to Dataveillance and Information Privacy, and Definition of Terms. http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html.

[14] Rabin 1978, Rivest, Shamir, and Adelman 1978
Chaum, David. 1985. Security Without Identification: Transaction Systems To Make Big Brother
Obsolete. *Communications of the ACM*, 28 : 1030-1044.

[15] Rankl and Effing 1997, Anderson and Kuhn 1996, Anderson and Kuhn 1997
Clarke, Roger. 2001. Of Trustworthiness and Pets: What Lawyers Haven't Done for e-Business.
http://www.anu.edu.au/people/Roger.Clarke/EC/PacRimCL01.html.

[16] Cranor, Lorrie, and Joseph Reagle. 1998. The Platform for Privacy Preferences. *Communications*
of the ACM.

[17] Cranor, Lorrie F. 2002. *Web Privacy with P3P*. Cambridge: O'Reilly & Associates.
Cranor, Lorrie Faith, and Paul Resnick. 2000. Protocols for automated negotiations with buyer anonymity and seller reputations. *Netnomics*, 2 : 1-23.

AUTHORS

First Author –
Gnana Sri Moparthy
Electronics & Computers branch of engineering
Koneru Lakshmaiah University
gnanasri.moparthy@gmail.com

Second Author –
Vinni Sheethal Gudipudi
Electronics & Computers branch of engineering
Koneru Lakshmaiah University
vinnisheethal.gudipudi@gmail.com

Third Author –
Venkata Sneha Priya Kotturi, Electronics & Computers branch of engineering, Koneru Lakshmaiah University

snehapriya.kotturi@gmail.com