Kartik Padave

A022

70362019039

Experiment 8

Aim

Study of E-Commerce Applications and use of cryptology

Abstract

Many businesses and consumers are wary of conducting business over the Internet due to a perceived lack of security. Electronic business is subject to a variety of threats such as unauthorised access, misappropriation, alteration and destruction of both data and systems.

Introduction

The seminal purpose of e-commerce is to perform Business-to-Business (B2B) as well as Business-to-Consumer (B2C) online transactions, and to exchange goods and services from a distance by any electronic and networked device that can use the Internet, that has now covered all the existing platforms worldwide. E-commerce is all about the exchange of information by Electronic Data Interchange (also known as EDI). The success of eCommerce will continue to be a critical part of business growth & development and enhanced performance only if it can overcome the concerns businesses and consumers have with stolen identity, secure banking, payments, and transactions. One of the finest ways to wipe out these concerns (and secure e-Commerce) is to use the concept of cryptography (briefly - the practice as well as study of techniques for secure communication).

Theory

As our use of E-commerce continues to soar, the need for encryption of customer data (as well as inventories, company financial information, etc.) increases exponentially as well. You must be knowing the fact that whenever

you sign up on a website for a membership, club, or even just for their weekly newsletter, your personal information is stored in a certain database. Once you start to purchase products or services from that retailer or service company, those transactions are stored in your —history‖ for a record of your activity with that company. If you think about it, you now have most of your personal information tied to your purchase history, including your basic personal details and the most secret of all the information and that is none other than your credit card information and more. If it weren't for encryption, if a hacker were to breach the initial security of these websites, they would have access to all your vital information. To try and prevent our system from this unethical approach that generally leads to a serious consequence of mishap, companies have special and dedicated teams within their organization that, not only are responsible for encrypting the data to keep it secure but are also constantly reviewing new technologies to support an even stronger encryption and data security solution. It is a continuing fight and commitment to an increased vigilance that keeps these experts' steps ahead of hackers and thieves to keep your data safe. Here at Unleaded Group, we are committed to keeping our clients and their customers safe with the latest encryption technologies.

The Internet is not known for its secure environment. In fact, the Internet is not safe for e-Commerce that usually involves tremendous number of transactions, unless it involves using cryptography and making its users aware of the concerns with e-Commerce. PC users need to know, how to improve e-Commerce security. Both PGP and SSL encryption provide cryptography; they can form the basis of a secure e-Commerce infrastructure. It is fair to say that, when performing an e-Commerce transaction, people still tend to provide their credit information to just about anyone asking without first knowing for sure, that the person or the Web site is completely safe and can be trusted. Trust in eCommerce is indeed a real concern. Being in e-Commerce involves risks (such as spoofing and eavesdropping) and possible threats (such as privacy). The use of cryptography in e-Commerce provides a safety layer, which is the only way to ensure highly secure e-Commerce transactions and Web applications that contain a customer's personal information. If e-Commerce is allowed to handle by SSL, server security and digital certificates, then it will be completely in safer hands, and this will provide the authentication, privacy and data integrity through encryption that is needed to overcome threats associated with Internet based transactions. The importance of cryptography is that it can protect e-Commerce and reassure businesses and consumers that they are safe and

secure from prying eyes (hackers who utilize the Web to steal information). The use of cryptography allows the integrity of e-Commerce transactions and can safeguard information. Thinking practically, providing cryptography is the only way to secure an e-Commerce environment for banking; and SSL encryption is necessary to handle payments–to establish a secure channel, that can guarantee a customer's financial data remains secure.

Simply said, e-Commerce is the way of the future. It changes how people will conduct business, buy, and sell things, and provide goods and services right from a PC. Knowing this, e-Commerce must have a secure environment so that people and business alike, need not to worry about unethical access (like hackers) stealing their identity and data to gain access to their credit cards or banking related information. If e-Commerce is going to continue to be a significant part of conducting business online, then it will require security and trust. And the use of cryptography and encryption is a must to protect the customers who provide their personal information online.

Conclusion

With all the above realizations, that some encryption techniques can be cracked if the right resources are channelled and synched towards the process, this paper recommends that those loopholes should be perused, and they are supposed to be solved amicably. This could be done by, investing the right kind of resources or more, that maybe needed to break the code if possible, and exploring the number of bit blocks that are used to break that code. After all this is done, the developers will be in a good way to determine the exact requirements needed to improve the existing algorithm. Such techniques, for example, are the likes of Data Encryption Standard (DES). AES is said to be a direct improvement/replacement to the DES, as it uses transformations on 128bit blocks as compared to the 64bit blocks of DES. Also, research suggests that online customers should be advised to opt for latest encryption enabled software environments like SSL enabled browsers, as their payment information needs to be confidential between them and their retailers and only such environments can guarantee such confidentiality and integrity.

References

1. Gudimetla Sai Dharma Reddy, Varma Buddharaju Shanmukh, Gudimetla Sai Raghukanth Reddy : A Secure Protocol for M-commerce Secure SMS Mobile Payment, International Journal of Science Engineering and Advance Technology, IJSEAT, Vol. 4, Issue 4, April–2016, pp. 200-205.
2. MurphyAnn, MurphyDavid: The Role of Cryptography in Security for Electronic Commerce, The ITB Journal, Volume 2, Issue 1, Article 3, May-2001, pp. 21-50.
3. RanePradnyaB., Meshram B.B.: Application-Level and Database Security for E-Commerce Application, International Journal of Computer Applications (0975– 8887), Volume 41– No.18, March 2012, pp. 1-5.
4. RathiNikita A., Gupta S.R.: Analysis of Security mechanism in E-commerce transaction, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 5 Issue 1, January 2016, pp. 131-135.
5. Ritu: Cryptography Based E-Commerce Security, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 7, July 2016, pp. 359-363.
6. VishvalingamK., Sandanayake T.C.: An Overview of Online Transaction Technologies in E-Commerce, International Journal of Engineering Development and Research, Volume 5, Issue 2, 2017 IJEDR, pp. 993- 998.