ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

STUDY OF POTENTIAL THREATS IN ONLINE BANKING TRANSACTIONS CARRIED BY TWO MAJOR INTERNATIONAL CARRIERS VERI-SIGN & VISA

Shubham Patel*, Madhvi Shelke, Ankit Rakhara, Palak Sharma, Yash Kumar Jain

ABSTRACT

security is concern when wealth & assets are managed in worldwide network. Any transaction between two computers or its network is never one hundred percent safe (Nestek, 1998). In present system of world-wide-web 128 bit SSL is used (Pace, 2009) but based upon the records in Crime Bureau of India 12705677 crimes are related to online robbery and 15% of these cases are direct breach of security layers. Cyber crimes are revolving around wealth theft. US $ British intelligence agencies have successfully cracked much of online encryption relied upon by hundreds of millions of people to protect privacy of online transaction revealed by Edward Snowden (former contractor) (Guardian News and Media Limited, 2015). However for online transaction card processing system adheres to PCI data security standard (PCI-DSS).

Where to overcome the threat the responsible authorities like Veri-Sign & VISA are switching to square network & servers which are monitored around the clock. Here this paper analyses possible planning & best security provided & reason of regular updating in security system by VISA & Veri-Sign which enables secure online transaction.

KEYWORDS: 128 SSL, Veri-Sign, VISA, Encryption, PCI-DSS, Planning, National Records, Cloud Computing, Online Transaction System.

INTRODUCTION

Security basically deals with safeguarding user's private information from unauthorized access. A security risk to database systems includes:

- Unauthorized misuse by users who are authorized for example, database administrators, or access to sensitive data, functions within databases, by the unauthorized authors or hackers.
- Malware practices leading to leakage or disclosure of personal or proprietary data, deletion of or damage to the data or programs, interruption or denial of authorized access to the database, the unanticipated failure of database services.
- Overloads, performance and capacity constraints resulting in the inability to use databases as intended.
- Computer room fires or floods, overheating, static discharge, electronic breakdowns, equipment failures.
- Design flaws and programming bugs in databases and the associated programs and systems, resulting in security vulnerabilities.
- The entry of invalid data or commands, mistakes in system administration processes, criminal damage etc.

Therefore, when it comes to online banking transactions following features are needed to be fulfilled by the security systems-

Confidentiality- Confidentiality is an equivalent term for privacy. Confidentiality insures that sensitive information is prevented from reaching the wrong people, while ensuring that the right people have access to it. In other words, information cannot be accessed by illegal/unauthorized user.

Integrity- Integrity is all about the consistency, accuracy, trustworthiness and completeness of data for entire life cycle. Data changes in transit should not occur, and to ensure that data is not changes by unauthorized people (for example, in a breach of confidentiality). These measures can be file permissions and user access controls. Some data is added with checksums, even cryptographic checksums, for verification of integrity. It deals with maintaining the data completeness and accuracy throughout its lifetime.

Authentication and authorization-Authentication is the process of user identification. It deals with checking and verifying the user identity. Authorization deals with access control. Each user has predefined set of access rights over the resources.

Non-repudiation- It can be represented as one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny receiving a transaction and the other party cannot deny having sent a transaction. It guarantees non-denial of services from either of the party participating in the transaction.

LITERATURE REVIEW

Online banking services started in New York in 1981 when four of the city's major banks (Citibank, Chase Manhattan, Chemical and Manufacturers Hanover) offered home banking services using the videotext system. Various security schemes can be used for a safe transaction.

Security Schemes

Many layers and types of information security control are appropriate to databases, including:

- Access control
- Auditing
- Authentication
- Encryption
- Integrity controls
- Backups
- Application security
- Database Security applying Statistical Method (Wikipedia)

Out of all this, the one which is concerned with the security control of online banking transaction is ENCRYPTION: CRYTOGRAPHY.

Types Of E-Fraud

In Order to assess the risk to do online payment. It becomes very necessary that we understand the electronic frauds and try to provide some way so that the efrauds can not be take place or atleast we can trace the person who has committed online fraud in quick time. There are variety of E-types fraud are actually happening in electronic transaction. Some of the frauds are listed below:

Account Hacking: Account hacking means to take the illegal entry in any person PC. As more than 90% of youth actually connect with internet. Once they one their PC they start the internet. But, most of the user actually not aware with the internet but they only know how to access it. The person actually create it's account through admin. Once it's logged in through admin and connect himself to the internet at that moment of time he actually create an open offer for unauthorised user to access his personal information from their PC and they actually misuse those information..

Phishing : Phishing is another concept of hacking the confidential information or files from the person PC. In phishing technique, it always try to display its original identity to the end user but actually its not the original source. Once the transaction is compeleted all the confidential information is in the illegal peson hand. Suppose for example, I have created one page which actually look like GMAIL but actually it is not original GMAIL account. But when user entered his username and password, it is then hacked and change or it can any illegal things with that. During the next online transaction the malware will activate and steal private and personal financial information, including credit card numbers, PIN number which is used by fraudster to steal money from the account. Malware or „Malicious Software" is software which includes computer viruses, worms, Trojan Horses, spyware and other malicious software.

Spoofing or Website cloning: Spoofing is the way through which we will create the duplicate websites which look like the original website. The frauds actually uses all the original information of the organization like company logo, name, graphics and even the code is actually copied same as that of the organization. The personal information of person is now in the criminals hand. They will do fraud purchases and other things.

Lottery frauds: The end user recieves some scam messages through emails. In that they have provided the details that your name is selected in the lucky draw and you have won the amount of Rs. 1,00,000 and more high range offeres they provide and then he asked to fill the form. In that form they will extract all the personal and bank related information like your name, account number, card number and password.

LIMITATIONS WITH TRADITIONAL KEY CRYPTOGRAPHY

Encryption and decryption is the process through which we can make our data confidential and not easily access by the unauthorized users for any criminal activity to be taking place on the internet. Cryptanalysis is the process to make the data in some other form so that data even access by some other people cannot be understood by them. Encryption is the process taken place at sender end. Here, sender will change the original data in some other form using the public key or private key and then send the data to the recipient. On the other hand the receiver will use the same key to decrypt the data i.e. to generate the original text from the text receive by it. The limitation with such scenario is that the user has to share the key either they need to meet each other or with the help of internet they need to share the key. In both the cases the key will be in hand of the unauthorized person and they are now able to access your confidential data.

METHODOLOGY

THE VERISIGN DIGITAL CERTIFICATE

A digital signature is created by running message text through a hashing algorithm. This yields a message digest. The message digest is then encrypted using the private key of the individual who is sending the message, turning it into a digital signature. The digital signature can only be decrypted by the public key of the same individual. The recipient of the message decrypts the digital signature and then recalculates the message digest. The value of this newly calculated message digest is compared to the value of the message digest found from the signature. If the two match, the message has not been tampered with. Since the public key of the sender was used to verify the signature, the text must have been signed with the private key known only by the sender. This entire authentication process will be incorporated into any security-aware application.

Users of RSA technology typically attach their unique public key to an outgoing document, so the recipient need not look up that public key in a public key repository. But how can the recipient be assured that this public key, or even one in a public directory, really belongs to the person whom it indicates?

As we know that the transaction is now taking place by the internet and we have changed the traditional approach. So that it becomes very necessary that we take digital signatures from the end users in case of any transaction so that the criminal act can be reduced to some extent. Different organizations are actually asking different information's of the end users so that they can maintain the security. To know about the attack is very difficult process. The digital certificate is the user's public key that has itself been "digitally signed" by someone trusted to do so, such as a network security director, MIS help desk, or VeriSign, Inc. Every time someone sends a message, they attach their digital certificate. The receiver first verifies the authenticity of the public key that it actually comes from the sender end or not. Digital certificates have a wide variety of uses ranging from interoffice electronic mail to global electronic funds transfer (EFT). In order to use digital certificates there must be a high degree of trust associated with the binding of a digital certificate to the user or organization linked with the digital certificate. This trust is achieved by building hierarchies of digital certificates, with all members of this hierarchy adhering to the same set of policies. VeriSign operates numerous digital certificate hierarchies.

SECURITY SYSTEM USING VISA

Verified by Visa is a new security system that tells on-line retailers and banks that a user is a genuine cardholder when he/she shops on-line. It allows us to use a personal password to confirm our identity and protect our Visa card when you use your card on the Internet, providing greater reassurance and security then the previous security schemes.
It is easy to enroll, simple to use and works with all Visa cards. It is also free.
Verified by Visa involves two quick steps to authenticate your purchase.

- Firstly the user will see the personal message that he provided when he signed up for Verified by Visa and that only he and his bank know about. This lets him know that the security screen he is seeing is genuine
- Then he'll be asked to enter his Verified by Visa password.

CONCLUSION

In any transaction taking place on internet the authentication is the crucial parameter to be considered. Why should economic services organizations care about strong authentication? The answer brings us—trust. When a strong authentication process in place, the consumer can trust that their E-transactions are secured and can private not access by some other ways and means. With greater customer confidence comes lower customer churn and higher transaction volumes, resulting in increased revenue for the FSP. Online financial transactions, payment settlements, and business-to-business exchanges all depend on establishing participant identity and data integrity. Other time-sensitive operations, such as documentation submission, bill calculation, and stock trading, require an auditable trail. Employing multiple, disparate products creates security gaps and heterogeneous environments, which are costly to manage, create compatibility issues, introduce vulnerabilities, and inhibit future growth. Strong authentication is the most direct and cost-effective way to ensure that any user attempting to access sensitive applications and data is an authorized party with the appropriate permissions to view, copy, and modify that data.

REFERENCES

[1] Mohanad Halaweh, Christine Fidler - " Security Perception in Ecommerce: Conflict between Customer and Organizational Perspectives". Proceedings of the International Multiconference on Computer Science and Information Technology, pp. 443 – 449, ISBN 978-83-60810-14-9- 2008-IEEE
[2] Yuanqiao Wen, Chunhui Zhou "Research on E-Commerce Security Issues". 2008 International Seminar on Business and Information Management.
[3] Rui Wang, Shuo Chen "How to Shop for Free Online Security Analysis of Cashier-as-a-Service Based Web Stores". IEEE S&P'11 proceedings.
[4] V.SRIKANTH "ECOMMERCE ONLINE SECURITY AND TRUST MARKS". IJCET ISSN 0976 – 6375, Volume 3, Issue 2, July- September (2012),
[5] Shazia Yasin, Khalid Haseeb. "Cryptography Based E-Commerce Security: A Review". IJCSI-Vol. 9, Issue 2, No 1, March 2012
[6] Randy C. Marchany, Joseph G. Tront, "E-Commerce Security Issues"Proceedings of the 35th Hawaii International Conference on System Sciences – 2002
[7] Rashad Yazdanifard, Noor Al-Huda Edres "Security and Privacy Issues as a Potential Risk for Further Ecommerce Development"International Conference on Information Communication and Management - IPCSIT vol.16 (2011)
[8] Seyyed Mohammad Reza Farshchi "Study of Security Issues on Traditional and New Generation of E-commerce Model" International Conference on Software and Computer Applications-IPCSIT vol.9 (2011)
[9] RAJU BARSKAR, ANJANA JAYANT DEEN"The Algorithm Analysis of E-Commerce Security Issues for Online Payment Transaction System in Banking Technology"(IJCSIS)-Vol. 8, No. 1, April 2010
[10] Dr. Nada M. A. Al-Slamy, "E-Commerce security" IJCSNS - VOL.8 No.5, May 2008
[11] W. Jeberson, Prof. (Col.). Gurmit Singh. "Analysis of Security Measures Implemented on G2C Online Payment Systems in India" MIT International Journal of Computer Science & Information Technology Vol. 1 No. 1 Jan. 2011