Inherent Dangers in Database Security

Sartaj Singh
Department of Computer Applications
Lovely Professional University
Punjab (India)
E-mail: Sartaj_2292@yahoo.com

Abstract- With the danger/ risk of data theft looming large over the horizon of the Internet user involved in e-banking, online shopping, transaction etc. it becomes imperative to identify the dangers involved and employ security checks. Usually big stores have secure SSL [1] connections to be used by the owners of credit cards. Use of base64 encoding instead of hexadecimal and similarly using AES-128[2] cipher algorithm certainly heightens database security because these methods ensure high security where as they shorten the length of the encrypted string. Carrying forward these two above stated methods i.e. base64 encoding and AES-128 cipher algorithm, a more secure approach will be to use random number generator in which is required only to store the 8-byte random component instead of full 16 bytes. The existing methods of encryption are also not fool proof for high end professionals. The main thrust of this paper is to identify, pinpoint and find the solutions for the inherent dangers involved in the database storage.

Keywords: ***E-banking (Electronic-Banking), AES (Advanced Encryption Standard)***

I. INTRODUCTION

More than 60% of organisations in India feel that they have taken enough measures to secure their databases. But actually large corporate databases are not as secure as their executives think. The threat is not only for their customers' privacy and safety, but their own corporate secrets also. Corporate database linked security is a two-pronged problem. New threats and vulnerabilities [3] keep surging up making it difficult for database executives and security managers to keep up. The other part is even more important that every company's security problems are different, making it almost impossible to find fool proof solutions.

Use of base64 encoding instead of hexadecimal and similarly using AES-128 cipher algorithm certainly heightens database security because these methods ensure high security where as they shorten the length of the encrypted string. Carrying forward these two above stated methods i.e. base64[4] encoding and AES-128 cipher algorithm, a more secure approach will be to use random number generator in which is required only to store the 8-byte random component instead of full 16 bytes.

Although there have been constant efforts being made to ensure fool proof database/ Credit card transaction security none of the already stated encryption methods[5] can be said to be ultimate. The area of database security keeps offering new problems with every coming new day. As such those involved in creating security measures have to go a step ahead of the shrewd hackers and in this area sky is the limit.

II. CREDIT CARD VULNERABILITIES

The main thrust of this paper is to identify, pinpoint and find the solutions for the inherent dangers involved in the database storage where the buyers are fast taking to the on-line shopping/transactions in the fast changing scenario of sale purchase of various items. Talking about the few possible risks and dangers [6] involved in the possibility of hacking the queries of a prospective buyer, the intruder can twist tamper and change the contents of the query to his/her benefit.

With the danger/ risk of data theft looming over the horizon of the Internet user involved in e-banking, online shopping, transaction etc. it becomes imperatives to identify the dangers involved and employ security checks. Usually big stores have secure SSL [7] connections to be used by the owners of credit cards. It can be safe if this database is solely used by the said store. In case the same is Internet connected database, it will be a welcome cake walk for the clever hackers. Similarly 'password mode' encryption [8] is also open to risks. In the light of the above symmetric encryption Electronic Code Book

978-0-7695-4817-3/12 $26.00 © 2012 IEEE
DOI 10.1109/ICCS.2012.42

(ECB) was put to use considering it to be a better tool. Two modes – Cipher Block[9] Chaining (CBC) or Counter Mode (CTR) have been employed as security measures by a few, however, these methods of encryption[10] are also not fool proof for high end professionals.

According to Ryan Nichols [11] the most common risks involved are: Unauthorized access by insiders, "Brute Force" attacks, incorrect usage, and Personal hardware collection. In addition, some of the hidden dangers that simply leave databases exposed to security threats can cause equal harm and include such vulnerability cases[12] as Data-at-rest (unencrypted information), Sensitive data, Poor application architecture, Password vulnerability, unlocked database, and Vendor bugs.

For example Mr Ramesh presents his credit card. If you press the button you will get a real credit card from the biggest online shop database. The user who clicked on the button in the middle of the screen received detailed information on a randomly chosen card and Ramesh claimed to have stolen more than 50 thousand individual credit card records from the databases of Creditcard.com [13]- a processor of credit cards for hundreds of e-commerce sites. It can be taken as an example of a hacker who exploited the vulnerability in SQL Server database of Microsoft product

III. CREDIT CARD INTERNAL WORKING PROCESS

A credit card [14] is used now a day for purchase online and making its payment also online later. The code on the credit card stands for specific information related to the card holder. The initial digits stand for the financial institution while the succeeding ones tell about the account number. The last one called a 'check digit' is an essential security item. During the reading process of a credit card the sum of odd digits is multiplied by three, and then included to the sum of the even digits, and when added to the check digit the resultant should be a multiple of ten. The black stripe[15] on the backside is the part which reads when the card is swiped. Each stripe has several tracks of minute magnetic particles. These minute particles provide certain required information. The machine reading all this information is known as a magstripe reader.

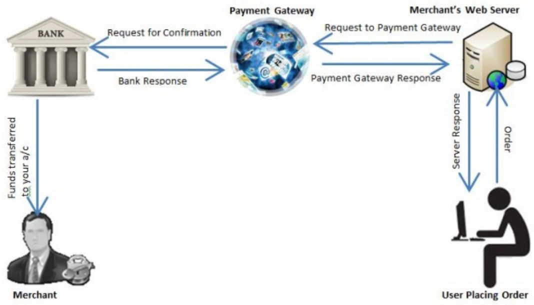

Fig: 01 Steps involved in online transaction

IV. CREDIT CARD HACKING TECHNIQUES

A hacker operates in many ways to acquire credit card number from his soft prey. It is commonly known as phishing. According to this technique [16], the hacker pretends to be an officer having a link within an organization. The hacker sends to email account holders an instruction to alert the receiver to follow the prescribed instructions before the credit card is cancelled.

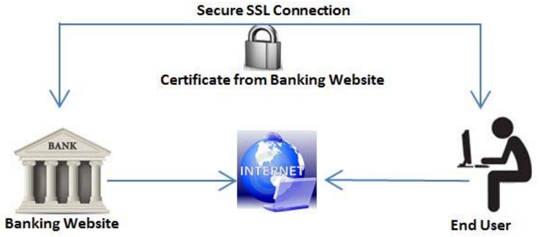

Fig: 02 Transaction using SSL Connection

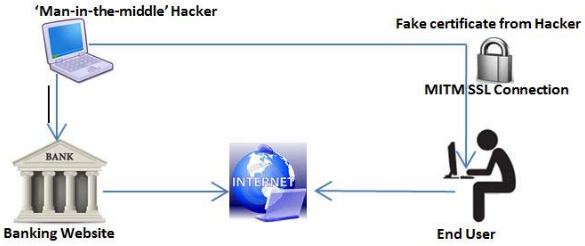

Fig: 03Transaction using MITM SSL Connection

The user unaware of the fraud is likely to insert his credit card, giving number, his name and allied information without being aware that he is going to be a victim of an online hacking. Hackers [17] employ another way for hacking credit card numbers through a website, because these intruders only need hacking the systems of online buyers/sellers. In this way they find out the database where the buyers/sellers store the credentials. Another way of hacking is the use of online process of buying. For example young persons are allured by the website with attractive adult content that they find enticing. It is obvious that the website is only fake, a trap for obtaining information of the credit card.

Radio-frequency identification (RFID) [18] credit cards are easy prey for hackers. Credit cards can be read through clothes and wallets. Kristin Paget [19] says that it is vulnerable to an uber-stealthy form of pickpocketing. Giving demo with a Vivotech RFID credit card reader she bought on eBay for $50. Paget wirelessly read a volunteer's credit card onstage and obtained the number and expiry date of the card, along with the one-time CVV number to authenticate payments [20].

Just a second later, she used a $300 card-magnetizing tool and encoded that data onto a blank card. Thereafter she used a Square attachment for the iPhone that allows anyone to swipe a card and receive payments. She paid herself $15 of the volunteer's money with the counterfeit card she had just created. It showed that these RFID credit cards were also not free from hacking risks [21].

V. CREDIT CARD DATABASE SECURITY TOOLS

With the increase of financial risks and database security hazards as a result of database leaks[22] more and more high end organisations are taking to better security policies in order to protect their information that is considered private and personal, such as credit card, in a better way. This information being highly protected has to be guarded while using it. It has to be securely deleted when it is being used or needed. There have been instances when some credit card databases left behind temporary files containing vital information, or old spread sheets having credit card numbers, buried in sub directory.

There have been new security guards for database protection every other day but the shroud hackers find a key to the latest protections. As such, no security/ discovery tool can be said to be the ultimate one. Among the exciting database protections **Tokenisation** [23] is being used widely. It is the process used in lieu of sensitive data with unique identification symbols. It retains all the necessary information about the data without compromising with its security. Tokenisation seeks to minimize the amount of data required. With a minimum cost, it has become a popular mode for small and mid-sized businesses that helps in the security of credit card and e-commerce transactions. As compared to older systems in which credit card numbers were stored in databases and exchanged freely over heterogeneous networks, the process of tokenisation is much more difficult for hackers to gain unauthorised access to card holder's data.

Another security tool commonly used is **Cornell Spider** [24]. It is available in two versions - Linux and Windows. Although the first one is called the Linux version, it is not Linux-specific. It works with the other operating systems like UNIX, such as Free [25] BSD and Open BSD. The Windows version contains most of the functionality of Linux version with some changes in Windows functionality. Unlike Linux versions it does have a graphic user interface (GUI). But it lacks other features such as the ability to decode more obscure file compression formats. Spider is especially good at weeding out false positives with the use of a 'magic number' style file. Spider has its own limitations the present production version fails in finding credit card numbers which are encoded as 16 unbroken ASCII digits.

It also does not attempt to validate any credit cards numbers against the Luhn algorithm2 [26] to avoid false positives. Currently Windows-beta version of spider is in vogue which attempts to validate credit card numbers with the help of algorithm to find numbers which do not contain dashes or spaces. Spider may have some limitations, however, the tool is being widely used because is supports compressed files searches, and it can feed file data to a central analysis server over a network in an encrypted manner.

It has low false positives and it logs each match and shows the unmatched data before and after each match. Moreover it is free and source code is available. The only limitations are that it is time consuming installation procedure and many dependencies are required for manual installation. It is more prone to false negatives.

SENF [27] is yet another command line tool that is written in Java. The SENF tool does not help in location of matches in a matching file; however, it certainly lets you set a threshold on the number of matches in a single file. It is easy to install and can be run from removable media without a Java virtual machine installed SCNF. It can be run from the command line. However, it is also not free from shortcomings. It has high false positives; no source code is available [28]. It only lists the matches for each file instead of the specific matches and the surrounding data in the file.

Last but not the least EnCase Forensic [29], also referred as Encase is a commercial product floated by Guidance Software. It is mainly a general computer forensics tool. It is used for finding credit card numbers as well as Security numbers. Encase also uses a regular expression engine like most free tools. For credit card numbers, Encase contains a script (EnCase's embedded scripting language) called EnScript. It finds numbers encoded with ASCII digit characters which conform to the Lohn algorithm. Encase is beneficial because it comes with a good script for finding credit card numbers and there is a large user community using it. It has nice graphic user interface (GUI) and commercial support. It has the limitation that it is not free and it does not come with any sophisticated methods [30]. It is somewhat complex; consequently, it is less preferred as compare to other tools.

VI. CONCLUSION

Encrypted data related problems of computing have caused innumerable new attractive techniques. Most of the latest research in cryptography at present is the result of this. A solution to the security problems regarding outsourced databases are likely to be solved if the data are properly encrypted on both ends- front end and back end. At this stage Homomorphic encryption seems to offer a viable and dependable solution to the problem at hand. From the above discussion it is established, without and iota of dough, that so far no hunky-dory protection/security of database information has been achieved. A more effective system comprising really smart credit card with compatible swipe-machine has to be devised which may establish the true identity of a genuine card holder by displaying his/her image and finger print on the interface attached to the swipe machine. If the fresh print and the image are Okayed only then the transaction should further proceed. It will be the first step of forestalling sneaking of database at the back end. Of course it will be imperative that only the owner of the credit card will be able to use it to avoid database leakage. Hence security measures should be adopted at the both ends –front end and back end.

RERERENCES

[1]M. S. Hwang and L. H. Li. 2000 "A new remote user authentication scheme using smart card", In IEEE Transaction on consumer Eleclronic,"vol.40, no 1, pp 28-30,

[2] Dewan Md. Farid, Jerome Darmont, and Mohammad Zahidur Rahman, "Attribute Weighting with Adaptive NBTree for Reducing False Positives in Intrusion Detection," International Journal of Computer Science and Information Security (IJCSIS), Vol. 8, No. 1, April 2010, pp. 19-26.

[3] http://www.zork.org/cwc/draft-irtf-cfrg-cwc-01.txt, Section 2.5.

[4]William Stallings, Cryptography and Network Security Principles and Practices, Pearson, Fourth Edition, pp. 48-49.

[5] McGrew, D. A., Nov 15, 2002, Counter Mode Security: Analysis and Recommendations, pp. 2.

[6]Jesper Andersen,Ebbe Elsborg,Fritz Hengle, Jakob Grue Simonsen and Christian Stefansen, "Compositional specification of commercial contracts", Springer verlag, 2006

[7]Atsa Etoundi Roger and Marel Fouda Ndjodo. "A Generic Abstract Model for Business Processes and Workflows Management", Bieter Gerald and Kirste Thomas, editors, 4th International Workshop on Mobile Computing, pages 62–72. IRB Verlag, Stuttgart Germany, 2003

[8]Amit P. sheth, Will van der Aalst, Ismailcem B. Arpinar. "Processes driving the networked economy". IEEE Concurrency, July-September 1999

[9]Atsa E. Roger and Marcel Fouda. "An Abstract Model For Workflows and Business Processes", CARI 2002, pages 239–247

[10]F. Casati, S. Ceri, B. Pernici, and G. Pozzi. "Conceptual Modeling of Workflows". Springer Verlap, December 1995

[11]Furguson, N., May 20, 2005, Authentication Weakness in GCM. Available online at http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/comments/CWC-CM/Ferguson2.pdf.

[12]Design and Development of a Prosody Generator for Arabic TTS Systems.Available online at http://www.ijais.org/component/zoo/item/ijais-3650

[13]Volume.Available online at 1http://www.ijais.org/component/zoo/item/volume1

[14]Ensemble of Decision Tree Classifiers for Mining Web Data Streams. Available online at http://www.ijais.org/component/zoo/item/ijais12-450112

[15] A Denotational Semantics Methodology (DSM) Approach for Business Processes Modeling. Available online at http://www.ijais.org/component/zoo/item/ijais-3649

[16] Announcing the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication, FIPS 197, Nov 26, 2001.

[17] Sutton, R. 1998. Reinforcement learning, MIT Press, Cambridge, MA, USA.

[18] McGrew, D. A., Viega, J., June 2005, Galois/CTR Mode of Operation. Available online at http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-revised-spec.pdf.

[19] Secured Data Hiding based on Compression Function and Quantization. Available at http://www.ijais.org/component/zoo/item/ijais12-450109

[20]Analysis of Detection and Prevention of Various SQL Injection Attacks on Web Applications. Available at http://www.ijais.org/archives/volume2/number7/176-0372

[21] J. V. William G. J. Halfond and A. Orso, "A classification of sql injection attacks and countermeasures," 2006.

[22] http://en. wikipedia. org/wiki/Social_web.

[23] N.K.Kalantari, Seyed Mohammad Ahadi "A Logarithmic Quantization Index Modulation for Perceptually Better Data Hiding" IEEE Trans on Image Processing, Vol 19, no 6, June 2010.

[24] The Open Web Application Security Project (OWASP), http://www. owasp. org/index. php/Top_10_2007.

[25] Ke Wei, M. Muthuprasanna, S. Kothari, Eliminating SQL Injection Attacks in Stored Procedures,pp. 191-198, IEEE ASWEC, 2006.

[26]William Staling "Cryptography and Network Security" 2nd edition Pearson Education Hall.

[27] Privacy Policy. Available at http://www.ijais.org/privacy-policy

[28]An Efficient and Secure ID-based Remote User Authentication Scheme using Smart Card (Volume 1/Number 6 (ISBN: 978-93-65823-05-7)) Available at http://www.ijais.org/archives/volume1/number6/100-0188

[29] Simar Preet Singh and Raman Maini, "Comparison of Data Encryption Algorithms", International Journal of Computer Science and Communication, Vol. 2, No. 1, pp. 125-127, January-June 2011.

[30]Passwords Management System using Blowfish Cryptographic Algorithm with Cipher Block Chaining Mode (Volume 1/Number 9 (ISBN: 978-93-65823-08-3)). Available at http://www.ijais.org/archives/volume1/number9/114-0226