MIGRATION, AUTHENTICATION AND PROTECTION (MAP) OF CONSUMERS AND CARDS

Basant Kumar*

P Mani Joseph*

Rashmi Dwivedi**

Abstract:

In preceding few years attacks on web services have developed from pretty simple credential stealing attacks to advanced content-manipulation attacks by means of malevolent software scattered on the client end-devices.The right long-term goal is to make data unusable to criminals and therefore reduce the incentive to steal it. We will never be able to keep the track data cloaked in secrecy and out of the hands of criminals.

Modern Internet banking services will be able to survive only if banks strongly care about the reasonableness of their solutions and users strongly care about their responsibility and due diligence to protect credentials and validate transaction data whenever needed. MITB,MITM, DOS and DDOS are in fact Trojan horse programs and capable enough to hack confidential data for future misuse.

We must migrate from static data to dynamic data for authenticating consumers and cards.

Keywords: *Web Services, Malicious Software, End Device, MITB,MITM, Trojan Horse Program ,DOS,DDOS*

[*] Department of Computer Science, Modern College of Business and Science, PO Box 100, PC 133, Bousher, Sultanate of Oman.

[**] Researcher Nanotechnology and NanoScience, Sultanate of Oman

Introduction

The payment industry is caught up in a security quandary. The PCI DSS has provided a set of rules in an attempt to shore up protection of cardholder data and improve the overall security of the payment system. But the new regulations, system changes, documentation, audit requirements, and threat of financial penalties have imposed new burdens on merchants and payment intermediaries prompting some to question whether the gain is worth the pain. Whereas convenience was once the hallmark of credit, debit and ATM card networks, these days regulatory issues, liability concerns, and financial costs that now extend well beyond interchange fees have dampened the mood of card accepting retailers to the point where cash and checks look more appealing. Now merchants and other payment system intermediaries are being asked to invest even greater sums in technology to further secure the cardholder. Will these investments payoff or invite more oversight, regulation and needless cost?

What is the Problem?

Cybercriminals use peer-to-peer (P2P) tools for identity theft.[6] Using P2P tools to share music, software and other digital content is similar to leaving the front door of a house wide open for a burglar to saunter in. A woman's credit card details were found in disparate places such as Troy, Michigan, Tobago and Slovenia because her shared music folder was making her entire "My Documents" folder available to P2P audience for 24 hours a day.[7]

Instead of a regulatory and punitive approach to payment security, we need to examine and discover the underlying problem. Why is cardholder data in need of so much protection? The industry is spen holder data in need of so much protection? The industry is spending small fortunes on PCI compliance and ance and while many advocate that compliance measurement is but a snapshot in time and genuine security should be the goal, few have done a root cause analysis of the problem and laid out options that would truly secure cardholders and their personal data. Thus we can use the mobile phone as software token to generate Digital Signature code.

Understanding Criminal Motivation

Cybercrime is a necessary endeavour to maintain the social and political benefits that accrue from the more visible and high profile criminal areas.[2], [3]

So let us examine the issues. The first question is "Whattakescardholders' data attractive?" Unfortunately, criminals have
given us the answer: It's plentiful, static, easy to acquire and very useful to commit fraud. The next question is "How can we make it unattractive?"
The answer is we must make it harder to acquire the data and make it more difficult to use. To date, PCI mandates h

ave only focused on the first half of the solution – making data acquisition more difficult. To restore confidence and convenience to the payment system, we must make stolen data very difficult to use. The following material describes a range of possible solutions and an explanation and assessment of each.

Possible Solutions

The cardholder data is attractive and insecure. How can the payment industry secure itself? Possible solutions are:

Encryption
Counterfeit Detection
Tamper Recognition
Tokenization
Data Relevance & Integrity
Dynamic Transaction Authentication.

Encryption :

Encryption is very useful. Encryption protects data by scrambling it.

Information such as data or messages that are sent is regarded as plain text until that information is encrypted and then is labelled as Cipher text [1].

It makes the data unreadable unless you know the secret key. To be useful, a strong algorithm must be employed alo ng with sound key management practices. PCI has mandated the encryption of cardholder data transmitted across open, public networks and whenever it's stored. This was an excellent directive. PCI recognized that access by thieves to large, concentrated storage facilities of cardholder data is highly attractive and extremely dangerous because it allows quick and efficient theft of data.

The PCI mandate to encrypt data post authorization closes a big hole, but this encryption offers no protection for the millions of other locales where cardholder data may be obtained. The PCI mandate might be expanded to include the protection of cardholder data in transit over private networks. This should prove valuable because it will further constrict the avenues available for data theft. But once again encryption cannot protect cardholder data that lives outside the network. That data is widely available from other data capture venues: pocket skimmers, false front ATMs, tampered POS terminals, unattended gas pumps, Phishing and pharming sites, and telephone scammers.

At best, requiring the encryption of cardholder data on all "We must move from static data to dynamic data for authenticating consumers and cards."

Networks and in storage protects the intermediaries of the payment system, but does little to protect the cardholder. The criminals can still get the data; they just cannot get it as quickly or efficiently.

The third activity involves the final exploitation of the stolen information obtained through the cyber attack: turning the traded data into cash. When criminals obtain the stolen data (personal information, credit card and bank details), they must use it to steal money. This is not without risk, and this is where the chance of detection and arrest increases significantly.[4]

This activity involves high risk and lower technical capabilities, and can be easily embraced by organised criminal gangs and individual agents looking for money.[5]

Cardholder data is vulnerable at all times when not encrypted. It is un-encrypted on the card itself which puts all parties in the payment world at risk, even if their networks and servers are fully encryption secured. Two and a half billion branded payment cards are in circulation that all contain data in the clear. The magnetic stripe data is not secret. It is used for transaction routing and is nothing more than a magnetic barcode - a series of zeros and ones,decodable by any first year computer science student.

To ask the payment community to protect this data is an impossible task.

This is akin to asking the payment industry to protect consumer personal identification numbers (PINs) with end to end encryption, after they have been written in the clear on a magnetic blackboard for the world to see. The reading method for cardholder data is in the public domain and is well described in both American and International standards documentation. The magnetic stripe cardholder data was never intended to be shrouded in secrecy. The attempt to protect it by encryption is a recent phenomenon, in reaction to large data breaches.

The encryption conundrum is further complicated by the brand rules that require the POS to "to read and transmit the entire unaltered contents of the Magnetic Stripe". Some parties have interpreted this to mean "encryption prior to authorization is not allowed". This ambiguity must be resolved and the language clarified.

Counterfeit Detection

Signature-detection methods are better understood and wildly applied. They are used in both NBIDS [10] and HBIDS [11].

A second option for consideration would be Counterfeit Detection. This can be described as the ability to determine that the data emanated from a legitimate card. If you can successfully identify the token that carries the data and determine that the token itself is authentic, then you can deduce that the data has not been obtained by a breach or a social engineering ruse. In a data breach the criminals take the stolen track data and transfer it to an available magstripe card. This might be an expired financial transaction card or it may be an old hotel door access card or a piece of white (unprinted) plastic. Some data hijackers have access to sophisticated card printing and embossing machines which can turn out cards that look perfectly legitimate. The thieves then use these cards at ATMs, gas pumps or stores to make unlawful purchases. When the card data on the cloned card is identical to the customer's real card, the transaction will be authorized unless the card has been reported stolen or is flagged because it falls outside the cardholder's normal usage pattern. When the token that carries the data can be validated, the counterfeit copies, made with stolen data, can be rejected. How can one tell that the data emanated from a legitimate source? All magnetic stripe cards have unique identifiers buried within the magnetic material. They are like fingerprints that are present at birth and change little as you age. Like snowflakes, no two are alike.

ers" (DIs) which can be used to recognize each individual card. If the card can be identified by its bio tag or its DI, then the accepting or authori-
ing party can have a high degree of certainty that a genuine card was presented at the point of sale, that the us-
age is appropriate, and that the transaction may be safely approved. Conversely, if the card fails the authentication routine, because its bio tag or DI is not recognized, then the transaction may be declined in real time. One such

tine, because its bio tag or DI is not recognized, then the transaction may be declined in real time. One such

DI authentication method is called MagnePrint.

Tamper Recognition

Next, an accepting or authorzing party must be able to determine that the data on a genuine token has not been modified or substituted. This is important because because a genuine card may be used at POS but if cardholder data from another card has been substituted(transferred onto the magstripe) or the original data has been altered, the system needs to be smart enough to recognize this attempt at fraud. In this instance the magnetic fingerprint buried within the magnetic material can be fused to the encoded cardholder data so that a change in the cardholder data with produce a different Magneprint DI than the one stored on the cardholder authorization database, and the transaction can be declined.

Data Relevance & Integrity

It's important to know that the card data is "fresh". This means the authorizing party must be able to determine if the swipe, tap, dip or insertion occurred quite recently. A sound verification method can "time bound" the data to ascertain that it is not from an old swipe that was trapped but not used.

Data of this type should be treated as "stale" or out of date and lead to a decline at the POS. To know that the data is fresh, the reader itself must be capable of mutual authentication, session management, and data integrity verification.

Tokenization

The merchant community has repeatedly voiced their opposition to any obligation to store and safeguard cardholder data. After the data has been transmitted for authorization, there is no need for the merchant to retain cardholder data, provided the POS system can leave behind only masked or tokenized data. With minor infrastructure adjustments, masked PAN data can be used for settlement and chargeback inquiries, liberating the merchant from a burdensome responsibility.

Dynamic Transaction Authentication

However, a strong-password is difficult to memorize. Additionally, the strong-password authentication schemes suffer from stolen verifier attacks and guessing attacks[12]. Several schemes and improvements [13], [14]-[15], [16], have been proposed, but these schemes are based on static login ID. There are numerous applications where static login ID leaks partial information about the user's login message to the adversary. The adversary could intercept the login ID and later try to manipulate it with other intercepted parameters to forge the login ID. Therefore, employing a dynamic ID for each login can avoid the risk of ID-theft. In this paper, we propose a dynamic ID-based remote user authentication scheme using smart cards. The proposed scheme allows the users to choose and change their password freely. The scheme is protected from ID-theft and the security of the scheme is based on a one-way hash function [17].

Data obsolescence or auto-expiration by dynamic authentication is another method to assure that the cardholder track data is genuine – and has not been obtained from a breach or from a counterfeit card. By this method the system is able to observe unique transaction values that are produced by the interaction of the card DI, the swipe, and the reader at POS. Much like a One Time Password (OTP), a one time use dynamic Transaction Authentication Value (TAV) is generated at the reader. This dynamic value will be rejected if it is presented a second time to the authorization system. This method of authentication does not depend on time boundaries. It does rely on the principle of entropy in its validation process.

A stochastic value is produced by unique circumstances – that is the card DI, the swiper, and the reader coalesce to generate dynamic digital output that changes in an unpredictable way but within boundaries that allow it to be correlated and authenticated. The MagnePrint DI provides a unique TAV for each transaction. Once used, the TAV becomes obsolete. If it is presented to the authorization system a second time, the transaction will be declined.

Is there a Best Practice?

The answer lies in understanding what we are trying to accomplish and who and what we are trying to protect. If we are interested only in protecting the merchant or other intermediaries from a claim of breach, and the resulting liability, then encryption may be quite adequate. In the event of a compromise, the parties who cannot decrypt will be able to plausibly deny they had access to the cardholder data because it was encrypted. If the accepting party had no knowledge of the key, they would have no ability to observe cardholder data, and thus theoretically no culpability.

End to End Encryption – Is it enough?

Encryption must not be confused with counterfeit recognition or tamper evidence. A card that has been cloned or altered will be encrypted at the POS just like a genuine card is encrypted. At the point of authorization, both the counterfeit card and the genuine card will appear to be identical, and each will have received equal protection during transmission.

It is useful to note at this point that a merchant who encrypts data from the point of swipe and has no access to the keymay not have any systemic knowledge of cardholder data, but adishonest employee can still methodically steal cardholder data by other means, such as using imprinters, cameras, pocket skimmers, or a pencil and notepad. Encryption cannot protect data that has been - or can be exposed by some other means.

Plausible deniability or Maximum Cardholder Protection

By contrast, 44 US states[8] had enacted legislation by December 2008 which requires notification of any security breaches involving personal information from public and private organisations. Legislation on data breach notification was first passed in California in 2003.[9]

If the objective is to protect the cardholder and his data from fraudulent use, along with the confidence,time and money he stands to lose, then encryption by itself is ineffective.If the intention is to spare the consumer anxiety, aggravation and financial loss, then other authentication methods are required.

The better way to protect the cardholder and his data is a robust combination of cryptographic and authentication techniques. The DI and its generated dynamic TAVs provide an ability to verify that the reader, the card, the card data, the host, and the cardholder are genuine.

This form of confirmation serves and protects every participantin the payment industry: the cardholder, the merchant , the processor, the acquirer, the brand, the issuer and law enforcement.

Making the data useless

Of equal importance, this process (the generation of a dynamic one-time use, DI derived, TAV) renders stolen cardh older data useless to the thieves. It removes the incentive to attack processors and merchants because the thieves can no longer profit from the data theft. The thief must have the genuine card with its original cardholder data intact in order to generate a valid TAV. For criminals, encryption makes theft more complex whereas dynamic authentication takes the profit out of the crime. Authentication protects the cardholder data even if it has been obtained illegally.

Authentication as a forensic tool

An additional benefit of an authentication DI is its ability to leave behind evidence of “card present”. There are times when a cardholder repudiates a legitimate transaction, with a claim that his card was not used and an inference that a counterfeit card was used instead. Because the card itself can be authenticated and determined to be genuine, the cardholder’s disputed transaction may rightfully be resolved in the issuer’s favor.

Set the cardholder data free

Cardholder data theft is not the actual problem. It becomes the problem only because the data can be used so easily to commit fraud. It's more important to stop the payout of dollars (the fraud) than to stop the theft of d ata.This is the only practical approach once we recognize that we will never be able to keep the track data cloaked in secrecy and out of the hands of criminals.

When we face this reality and adopt dynamic authentication, the cardholder data can once again ride in the clear on public communication channels and be used, without fear, for its intended purpose - machine readable data to route transactions and identify the communicating parties.

Once authentication is in place, there is little need to encrypt the cardholder data.

SecureSafe Solution

SecureSafe is multi-layer security architecture, designed to safeguard consumers and their personal data. It leverages strong encryption, secure tokenization, counterfeit detection, tamper recognition, and dynamic transaction authentication. No other security structure offers as much protection. The technology combines MagnePrint card authentication, with triple DES encryption of track data, together with tokenized track elements for local decision making, in a tamper resistant housing. It features DUKPT key cycling, mutual device/host authentication, session management, and data integrity verification.

Conclusion

While End-to-End Encryption has received much attention In the media and industry focus groups, its usefulness to prevent fraud is limited. An investment in hardware and decryption services that doesnot encompass a multi-layer authentication strategy is a poor use of resources.

The payment community must be motivated less by fear of liability and more by a genuine commitment to protect the consumer. It is interesting to note that a morally compelling strategy focused on consumer protection has positive ROI for retailers and an added advantage that it simultaneously protects all the other stakeholders.

References:

1. http://www.essortment.com/encryption-29511.ht- ml [accessed on 2012 Nov 02].

2. Interview with Colin Whittaker, Head of Security, APACS, London, 30th July 2008 and, 14th Octo= ber 2008.

3. Glenny, M., (2008), McMafia: Crime Without Frontiers, (Random House, London), p.426.

4. Kaspersky, (2005), "The changing threat, from prankster to professionals".

5. Russian crime groups, for example, minimize the risk of being caught by selling the credit card in formation ,, 9th December 2008.

6. A peer-to-peer (P2P) computer network uses di verse connectivity between participants in a net work. Such networks are useful for sharing content files containing audio, video, data or anything in digital format.

7. Chris Preimerberger, (2006), "Cyber-criminals use P2P tools for Identity Theft, Security analyst Warns." www.eweek.com/c/a/Security/Cybercriminals-Use-P2P-Tools-for-Identity-Theft-Security-Analyst-Warns/,

8. Plus the District of Columbia, Puerto Rico and the Virgin Islands.

9 Data breach disclosure law, SB 1386.

10. Caswell B, Beale J, Foster J, Faircloth J. Snort 2.0 intrusion detection. Syngress, ISBN 1931836744; 2002.

11. Price KE. Host-based misuse detection and con ventional operating systems' audit data collection. Master's thesis, Purdue University. <http://www.purdue.edu/>; 1997.

12. A. K. Awasthi, and S. Lal, "A remote user authentication scheme using smart cards with Forward

Secrecy," IEEE Transactions on Consumer Electronics, vol.49, no.4, pp.1246-1248, Nov. 2003.

13. C. K. Chan, and L. M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," IEEE Trans. on Consumer Electron., vol. 46, no. 4, pp. 992-993, Nov. 2000.

14. M. S. Hwang, C. C. Chang, and K. F. Hwang, "An E1Gamal-like cryptosystem for enciphering large messages," IEEE Trans .on Knowledge and Data Engineering, vol.14, no.2, pp.445-446, 2002.

15. J. J. Shen, C. W. Lin, and M. S. Hwang, "A modified remote user authentication scheme using smart cards," IEEE Trans. on Consumer Electron., vol.49, no.2, pp.414-416, May 2003.

16. H. M. Sun, "An Efficient remote user authentication scheme using smart cards," IEEE Trans. on Consumer Electron., vol. 46, no. 4, pp. 958-961, Nov. 2000.

17. B. Schneier, "Applied Cryptography," John Wiley & Sons Inc., 1996.