VOL 3 (2019) NO 2

e-ISSN : 2549-9904
ISSN : 2549-9610

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

Examining Users' Understanding of Security Failures in EMV Smart Card Payment Systems

Akeem Olowolayemo[#], Nafisat Adewale[*], Akram M. Zeki[**], Zubair Ahmad[**]

[#] *Department of Cognitive Science, Faculty of Cognitive Science & Human Development, University Malaysia Sarawak, Malaysia*

[*] *Independent Researcher*

[**] *Department of Information Systems, Faculty of Information and Communication Technology, International Islamic University Malaysia, Kuala Lumpur, Malaysia*

E-mail: oakeem@unimas.my, umusalman@gmail.com, akramzeki@iium.edu.my

***Abstract*— New credit cards containing Europay, MasterCard and Visa (EMV) chips for enhanced security, and for in-store purchases (rather than online purchases) have been adopted considerably in recent years. EMV supposedly protects the payment cards in such a way that the computer chips in a card referred to as chip-and-pin cards generate a unique one-time code each time the card is used. The one-time code is designed such that if it is copied or stolen from the merchant system or from the system terminal, it cannot be useful for creating a counterfeit copy of that card or counterfeit chip of the transaction. However, in spite of this design, EMV technology is not entirely foolproof from failure. This paper dis-cusses the issues, failures and fraudulent cases associated with EMV Chip-And-Card technology. The work also evaluates people's understanding of these issues and the consequential precautions they take to safeguard their information while using the EMV cards for transactions.**

***Keywords*— Chip and PIN Card Fraud, Card Security, Protocol Failure, Card Authentication, Users' perceptions, Payment Risks, Awareness.**

I. INTRODUCTION

For e-payment applications, the underlying intention is to offer customers a safe and easy way to pay online. The purpose of all payment processors is the same; to ensure secure and convenient payments. With this mindset, it is a good idea to have a detailed understanding of all characteristics and technicalities of how several of the online and offline payment methods function in order to avoid pitfalls and make the most effective choice to grow a business or carry out transactions. The main components in the transaction system between a business organization and customers in the online environment include an internet merchant account and a payment gateway. In order to facilitate payment, an alternative payment method such as PayPal can be included to cater for those customers who may not want to use credit cards. Once these pieces are in place, then customers can make purchases from business checkout page by submitting their payment information. The information presented by the customers is then sent to the payment gateway, which encrypts the payment information and shuttles it through the series of payment processors and networks for authorization where the payment is either accepted or declined. The decision whether the transaction is accepted or rejected is then relayed back to the customer in a short period of time, typically in few seconds.

Another type of payment is carried out by swiping the cards on POS (point of sale) devices of a merchant or retailer. Payment information is taken off from the credit card magnetic strips in order to process the transaction. The magnetic strip often called a magstripe, unfortunately, is not a satisfyingly secured technology as fraudsters can still steal the information from the magstripe and clone a new credit card with the customer information stolen. Subsequently, the fraudsters could use the card for several criminal or fraudulent activities such as shopping. This is why banks and credit card issuers are trying to devise other alternative so-lutions apart from magstripe credit cards. One of such solutions is the chip-and-pin cards. This type of cards are more prevalent in Europe, although not very common in the US (Barisani, Bianco, & Laurie, 2011; EMVCo, 2011, EMVCo, 2011b; EMVCo, 2011c). Most countries still do not have infrastructures to sup-port the chip-and-pin technology.

The primary difference between the chip-and-pin and magnetic stripe technology is that the magstripe credit cards store all information on the magnetic stripe. In the case of

chip-and-pin cards, all personal information and credit card details are embedded in a microchip of the card. When a user checks out at retailer or merchant system, the scanner reads the chip prompting the user to enter the pin to allow or complete the transaction process. It is very likely that many retailers will move away from magnetic stripe type of technology and start accepting chip-and-pin because it does help to minimize the risk of fraud. This is because it is more difficult to clone a chip-and-pin credit card compared to magnetic stripe credit card (Degabriele, Lehmann, Paterson, Smart, & Strefler, 2012; EMVCo, 2011b, 2011d; Ruiter & Poll, 2012).

This work x-rays the uniqueness of the EMV cards, highlighting the protocols that are engrained in the way it is designed which may have made it fool proof against attacks peculiar to the previously adopted magnetic stripe cards. It also evaluates the emerging security challenges to the EMV cards and the need for a review of its protocol, architecture, security and policies to further protect users of the payment methods. The work goes a step further to evaluate users' perception to justify the call for review in its protocol, security and security policies**.**

A. EMV Based Smart Cards

EMV stands for Europay, MasterCard, and Visa which is a widely-used proto-col for smart card payment systems. This protocol provides powerful security to payments compared to magnetic stripe cards. EMV commonly refers to a credit card with a smart chip but its supposedly secure technology used worldwide for all major payment methods, namely Credit, Debit and Prepaid. EMV can be used in three forms, namely; Contact payments, Contactless payments and Mobile Pay-ments (EMVCo, 2011a, 2011b) depicted in figure I below.

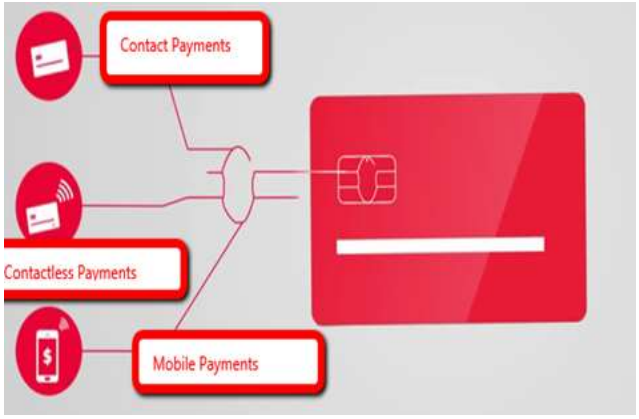

Fig. 1 Types of EMV Cards (EMVCo, 2011d)

The rationale for EMV or chip-and-pin cards is as a result of the issues associated with magnetic stripe cards which are prone to duplication or cloning. Countries using EMV cards have seen a huge decrease in fraudulent cases. This is because it is virtually impossible to clone an EMV card. Most of the other countries that have not adopted the EMV chip-and-pin technology have been incapacitated due to the infrastructure problem. EMV chip uses secret cryptographic keys to generate a unique code for each transaction. Stolen cards cannot be used at EMV terminal without the chip to generate this unique one-time code.

B. Problems and Security Issues with EMV Chip and PIN Systems

EMV is a no-swipe chip technology which is used by simply inserting the card into the terminal and waiting for the transaction to complete. No swipe is needed but some cards require a PIN code from the user while in other cases the user is required to sign after the transaction is completed. Contactless EMV cards are even easier to use and accomplish transactions faster where it is possible to tap the card on the reader and complete the transaction rapidly. EMV is also used for mobile payments mostly referred to as Mobile EMV which one can tap and pay using one's mobile phone after having downloaded the EMV securely on one's smart phone.

EMV emerged with the promise to solve security issues inherent in the magnetic stripe cards previously widely adopted for payments and making payments more convenient to its users. Unfortunately, after introducing EMV based cards in Europe in 2003, different types of fraud cases have risen which are totally different from magnetic Stripe type cards as shown in Figure 2. EMV cards also do offline card verification and transaction approval and since they are smart cards, they can have multiple applications at the same time in one single card such as MasterCard combined with Visa protocols.

C. Relay Attacks

Chip-and-Pin was designed in late 1990 based on some early experiments and it was introduced in Europe in 2003 to 2005. One of the fraud cases is the relay attacks. It is an attack that tries to intercept the transaction between the card and the terminal so that the card is wired up in the false terminal elsewhere. Whenever a user puts his card into the merchant terminal, it tries to transmit it to the doggy card that is remotely connected and thereby assessing user information located on the chip (Barisani, Bianco, & Laurie, 2011; Bond, Choudary, Murdoch, Skorobogatov, & Anderson, 2014; Murdoch, 2015). An illustration is provided in figure 3.

Figure 3 shows how the relay attack is carried out. After introducing chip-and-pin technology, fraudulent activities with respect to attacking the new EMV became drastically reduced initially. However, after some time, the hack-ers/criminals had taken considerable time to study and device approaches to beat the newly introduced technology. A relay attack is executed by an adversary us-ing two devices, namely the token and a reader, connected over any convenient communication channel that is capable of transmitting information over a consid-erable distance.

The token, acting as a proxy, is placed closer to the real reader, while reader, proxy, placed beside the real token in order to effect communication with the real token. The intention is to ensure that information communicated by the reader is read by the proxy-token which is then relayed to the proxy reader. The proxy reader in turn communicates the information to the real token. The real token would generally assume it is the real reader that it is communicating with, thereby responding accordingly. Subsequently, the response

from the token is transmitted back to the proxy-token which that then communicates the information to the reader. The aim here is to make sure that the reader becomes confused about dif-ferentiating information received from the real token and the proxy. Once, this confusion has been achieved the reader, thereby assuming that there is close prox-imity between the token and the right reader, provide the attacker with access (Murdoch, Drimer, Anderson, & Bond, 2013).

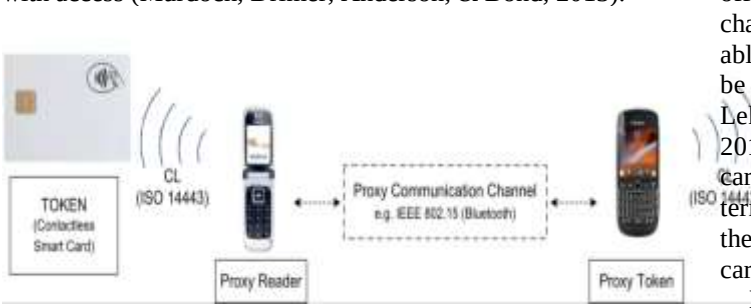

Fig. 2. Relay Attack using NFC Mobile Phones (Murdoch et al., 2013)

D. Skimming, Cloning and PIN Harvesting

A second fraudulent approach used by criminals can be regarded as skimming, cloning and PIN harvesting. Skimmers place hidden electronic devices between card and terminal, thereby enabling them to suck up all available data similar to ATM skimmers and subsequently creating fake pin pad or fake reader. The skim-ming is very difficult to notice unless the reader is opened and checked at regular intervals. As a result, it can go undetected for a long period of time whereas it re-quires minimal effort to install. The users may never know that the reader has been tampered (Anderson, Bond, & Murdoch, 2007; Bond, Choudary, Murdoch, Skorobogatov, & Anderson, 2014; Drimer & Murdoch, 2007; Drimer, Murdoch, & Anderson, 2008; Francis, Hancke, Mayes, & Markantonakis, 2012; Murdoch, Drimer, Anderson, & Bond, 2010). This is a very tiny thin skimmer that can be covertly inserted into the POS device. The device is a reader with two faces that acts like a shim and man in the middle device. When a user inserts his card, the card is intercepted by the device. It is so small that it is not easily noticed and once it's plugged inside, it is not easy to remove (The U K Cards Association, 2012).

E. Liability Shift Issue

A third prominent problem associated with the chip-and-pin cards or EMV cards is the liability shift issue. Using the chip acclaimed as a very "secure tech-nology" basically enables card issuers to shift the liability to the final consumer. The argument is that the chip-and-pin is protected from cloning and if a user ad-heres strictly to the procedure, the process and technology are foolproof. So, it is assumed that if a customer uses PIN for transactions and given that the PIN is to-tally secured it means that either the actual user undertaking the transaction has been negligent in storing PIN and in the case of any fraud, the liability might shift to the consumer if the consumer is not able to prove satisfactorily that he did not do the transaction.

1) Offline Data Authentication

Another issue with EMV cards is the offline data authentication. The chip-and-pin can have three types of authentication, namely;

a) Static Data Authentication (SDA)
b) Dynamic Data Authentication (DDA)
c) Combined Data Authentication (CDA)

Each of these authentication methods is designed to mitigate the flaws in the preceding authentication approach. The offline authentication method was intro-duced to support offline transactions. There are ways in which the offline transac-tions can be forged since there is no challenge response involved. The SDA and DDA are not able to provide security for offline transactions as they can be either cloned (SDA) or tempered with (DDA) (Degabriele, Lehmann, Paterson, Smart, & Strefler, 2012; Ruiter & Poll, 2012). Transaction using EMV begins at the inser-tion of the card by the buyer into the merchant terminal. Thereafter, the terminal authenticates the card by reading the information on the card for risk management as well as to ensure that the card is authentic.

Not all cards support DDA. Those cards that support DDA have signature key pair as well as the procedure to generate signatures.

Many cards manufacturers such as, Target, in attempts to improve security are significantly increasing the number of staffs in their IT security departments, spending several millions on improving security and making painstaking efforts to improve the security protocols & designs in their cards (Gray & Ladig, 2015). However, tackling security on one side should be supported with adequate users' protection and awareness programs. The protocols design issues are discussed in the next section.

F. Protocol Design Issues

EMV is designed into 4 main phases. First of all, there is the initiate applica-tion request processing where the terminal gets to access the card, while at the se-cond stage,(the authentication stage), the card is authenticated and this can hap-pen in several different ways. Then, the third stage is the card holder verification done by entering the PIN or with the signature before the actual transaction is ef-fected.

There are problems with the way this protocol has been designed. Firstly, all of these four steps are separate and not strongly tied together. This is one of the main issues with the design. The second problem is that most of the data exchanged here are completely unencrypted and unauthenticated. And the third problem is that the backend relies on the correct and secure operation of the terminals (Drimer & Murdoch, 2007; EMVCo, 2011a; Francis et al., 2012; Murdoch, 2009).

II. METHODOLOGY

This section is devoted to the method adopted in addressing the research objectives highlighted in the preceding sections. Firstly, the context of the study is discussed as well as the description of the population and the sample. Subsequently, the data collection strategy adopted is explained. An exploratory design approach was adopted. The research explored existing literatures on EMV usage and risks associated with EMV and as well adopts a survey questionnaire for data collection to evaluate users' perceptions of these issues and the efforts taken to protect themselves from the risks associated with using EMV cards.

A. Context of study, population, sample and Instrument

Quantitative approach was adopted in this study. As such, data was gathered using survey questionnaire. The questionnaire was developed in accordance with the issues gathered from the literatures on related works. The questionnaire was designed with the intention to identify the participants' level of awareness of the aforementioned risks associated with in-store payment with EMV Smart Cards. It also examined the extent to which users are concerned about the security to pro-tect their information. The questionnaire was designed using a 5-point Likert scale from "strongly agree" (5) to "strongly disagree" (1). There are three sections in the questionnaire. Firstly, a section contained questions about the users' demographic details. The second section of the questionnaire was devoted to the participants' usage of IT tools while the third section covered the respondents' awareness of likely risks associated with in-store payment with EMV Smart Cards as well as the responsive concerns based on their level of their awareness of how EMV cards safeguard their cards from the risks.

This questionnaire contains 14 variables . Purposive sampling method was adopted.. The population of the study is a group of EMV users. In order to get respondents from EMV users, an online questionnaire was used to elicit their re-sponses.

B. Data collection strategy

The questionnaire for the purpose of this research was created online. Each of the participants was contacted and a brief information about the purpose of the re-search was provided. On gaining approval, the link to access it was sent to partici-pants through WhatsApp, Instant Messages or any other SNSs. The responses were updated as soon as the questionnaire was completed by each respondent and submitted. Frequency analysis and simple percentages were used to analyze the data collected. . The study sample included 400 respondents.

III. Data Analysis

The data analysis is discussed in this section. The analysis of the demographic section is first presented. Subsequently, a discussion of IT tools usage was done. The evaluation of the responses to the Likert scaled questions were discussed in light of the perception of respondents with respect to their awareness of the issues and risks when using EMV cards for transaction on merchants' machines.

From the demographic information presented in Table 1,, it can be observed that 53.1% of the survey respondents are males while females account for 46.9%. Majority of the respondents are staff or employees of different companies and they account for 31.8%. In term of age group, most of the respondents (31.6%) are aged between 23-27years, followed by those in age group 28-32 years (25.6%). The least age group are those below 18 years (3%). The most common level of education among the respondents is bachelor degree (53.9%), followed by college certificate holders (14.8%), while sizeable number are also postgraduate holders such as those with masters, professional degrees or doctorates. Almost all respondents use mobile phones to access the internet. The percentage of those who use laptop is next after those that use mobile devices.

TABLE I
DEMOGRAPHIC INFORMATION

Profile	Items	Percentage (%)
Gender	Male Female	57.9% 42.1%
Age	Below 18 18-22 23-27 28-32 33-37 38-42 Above 42	3% 17.3% 31.6% 25.6% 11.8% 6.3% 4.9%
Level of Education	No School Attended Primary/elementary school Secondary/High School/College Trade/Technical/Vocational Training Bachelor Degree Master's Degree Professional/Diploma Degree Doctorate Degree	- 5.8% 14.8% 5.3% 53.9% 8.5% 10% 1.8%
Area of Specialization	Teacher Medical/Health/Nutritional Worker Lecturer/Academic Private Business/Entrepreneurs Employee/Staff of Company Sport/Fitness IT Professional Other	4.3% 6% 7% 16.3% 37.3% 4.5% 13.3% 13.3%
Tool/Devices for Accessing Internet	Mobile Phone Laptop Desktop Tablet/iPad Other	88.7% 65.2% 21.6% 22.3% -

This section shows how frequently the respondents use EMV cards. The result shows that most of the respondents (37.3%) prominent frequency of use of EMV cards is "Sometimes" use the EMV cards, accounting for 37.3%. Interestingly, the percentage of those who claimed to have "Nnever" used the EMV cards were next, accounting for is second, at 29.8%, while 15.3% claim to "Rarely" use the EMV cards.which is followed by rarely, at 15.3%. These This shows that majority of the users may do not feel particularly excited to use the EMV cards, unless it is out of necessity, such as instances where they fall being short of cash, or could not find ing an ATM machine around to withdraw. and so on.

In terms of security concerns relating to EMV cards, From the above, it can be noticed that majority of the respondents claimed that they are confident using the EMV cards when purchasing items on merchants' machines. Yet, it is surprising at the same time to see that they are subconsciously afraid as they use the technolo-gy. It is likely that the respondents are thinking of technical usage when asked questions about confidence. This points to the fact that majority of the respondents do not consider it safe using EMV cards in transactions.

TABLE II
FREQUENCY OF USE OF EMV CARDS FOR TRANSACTIONS

Frequency	**Percentage(%)**
Never	29.8%
Rarely	15.3%
Sometimes	37.3%
Often	10.8%
Always	6.8%

The respondents generally felt that it is preferable to pay with cash instead of using EMV cards. Furthermore, majority of them responded that they often feel insecure using EMV cards and also felt that someone might misuse their cards. Again, majority of the respondents felt that the security of EMV cards needs to be improved. These concerns may be due to the general uneasiness associated with transactions since money is involved rather than precise information or understanding of the risks that they may incur due to the use of EMV cards.

TABLE III.
CONFIDENCE AND SECURITY CONCERNS

	Gender	N	Mean	Std. Deviation	Sig. (2-tailed) – 95%
EMV Confidence	Male	231	3.6046	1.01890	.016
	Female	168	3.3472	1.08725	
EMV Security Concerns	Male	231	3.6041	.81420	.390
	Female	168	3.5298	.90253	

To further understand whether there are different perceptions of the risks of using EMV cards among male and female respondents, a comparison of means of the two groups about the two variables were carried out. The result is presented in Table III. It can be said that when it comes to fear about risks of using EMV, the male respondents seem to be slightly more concerned. However, there is no statistically significant difference between both genders in term of the security concerns (P-value = 0.39, at 95% level of confidence). For confidence using EMV cards during transactions, ironically, male respondents are seen to be significantly different from their female counterparts (P-value = 0.016, at 95% level of confidence).

TABLE IV.
CONFIDENCE AND SECURITY CONCERNS REGRESSION ANALYSIS

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	F	Sig.
1	.415[a]	.172	.170	.77639	82.511	.000
a. Predictors: (Constant), EMVConfidence						

The relationship between confidence and security concerns was also examined using Pearson correlation analysis. The intention is to find out whether there is a correlation between the respondents' level of confidence in using EMV cards for transactions on merchants' machine and the extent of security concerns. This is to determine whether there is a commensurate concern for security based on the respondents' level of confidence in the use of EMV cards. An inverse correlation is the hypothesis assumed here.

Judging from the results of the test, it is shown that there is no significant correlation between respondents' confidence to use EMV cards and their level of concern for security (R = 0.415, P-value = 0.000, at 95% level of confidence). Again, examining the coefficient of determination, $R^2 = 0.172$, it can be noticed that using level of confidence in using EMV cards to predict the extent of security concerns is not reliable, at only 17.2%.

IV. DISCUSSION AND FINDING

From the responses, it can be concluded that most people believe that EMV smart cards are not completely fool proof and secure. Consequently, the cards still need improvement in terms of security protocols, procedures and policy review.

Conclusively, tThe EMV smart cards can add convenience and safety to transac-tion, but the challenges facing today's systems can be daunting. In EMV systems, security mechanisms are implemented across the entire system to safeguard cus-tomers' data and privacy. The security protocols in EMV card technology provide several security features to be implemented with the EMV payment level. The purpose of these features is to guard the memory contents of the EMV to ensure adequate protection or to counter any form of attacks. Additionally, there are sev-eral countermeasures that are also included in the proprietary variants from differ-ent manufacturers which remain confidential. Several attacks have been designed to target the physical features of the EMV systems, relying on the limitations of physical components. Such attacks include the power analysis attack, simple power analysis (SPA) or differential power analysis (DPA). EMV manufacturers have consequently implemented several diverse features to obscure attackers to prevent critical information from being exploited.

Furthermore, another layer of security can be added to software in the operating system (OS) to further mask the physical operations, thereby strengthening the countermeasures considerably. To improve the security features, a close cooperation between hardware and software developers to provide additional security layers which can strengthen the secure EMV features. This is due to the fact that hardware can be used to strengthen software and the converse is also true. It is also possible to update the security of the system by enabling the OS to download and update secure software to ensure new security features can be added to the EMV security suits when required.

There is no payment and identity system that does not have security as its core component. It is also noteworthy to know that no properly-designed system is de-pendent on a single security component. This is because there is no single security mechanism that can provide a complete security. Again, complete security is never possible. However, the main objective in designing every secure system is to ensure that appropriate security measures are in place to counter the anticipated risks and threats to the system. The EMV smart cards have become an important component of most secure

payment and identity system designs. This enables organizations to provide secure and portable device for consumers and employees. The main objectives of these portable devices are to ensure that users' personal information is protected and provisioning of secure, authenticated transactions. Hence, it might be advisable to include feedback mechanism or procedures to inform users of deductions from their EMV cards to be sure of a complete transaction as well as possible fraudulent deduction from their cards. Furthermore In addition, the technology available in smart card provides several security benefits. For instance, the secure microcontroller allows intelligent interaction between smart card, the reader and the system. The implementation of cryptographic algorithms that are used to authenticate the card and cardholder to the system as well as the reader and system to the card. The advances in smart cards technologies such as flexible interfaces; contact and contactless, increasing processors' powers, different memory options, and symmetric as well as asymmetric cryptographic algorithms that can be implemented in scalable and flexible forms. Consequently, smart card technology has become an indispensable component for a secure system' chain of trust.

V. Conclusions

The objectives of this research are twofold. Firstly, the research sought to re-view the security protocols in using EMV cards for transaction. Specifically, to explore how secured are the EMV cards and what are the risks involved in using EMV cards. Secondly, the research also intends to explore people's perception of the security of EMV smart card payment systems. The findings are analysed from the data elicited from 400 respondents to the survey conducted.

Information security is inarguably one of the most important topics in infor-mation systems in recent years. In this paper, a brief appraisal of the EMV chip-and-pin cards has been carried out. The EMV cards were designed to work around the issues identified with the magnetic stripe cards. However, despite the claims that the EMV cards are foolproof from cloning and interception in a way peculiar to magnetic stripe cards, after a conscientious study by the hackers, ways have been fashioned out to hack or commit frauds based on the design of the EMV cards. This paper described various ways in which fraudsters and skimmers have tried to break the system to commit frauds. Specifically, it demonstrated that the PIN confirmation highlight of the EMV convention is defective which makes it susceptible to various frauds. Again, it can be seen that the EMV design does not necessarily provide additional new layers of security to the online transactions that are done over the web or mobile. Additionally, it can be noticed that there is an absence of verification of the PIN confirmation while the data exchanged here is completely unencrypted and unauthenticated. A survey of the common attacks that have been targeted at the EMV design has been discussed as well as offline authentication flaws associated with the SDA and DDA. Furthermore, as an extension to Ahmad, Zeki, & Olowolayemo (2016), a survey has been conducted to explore users' perspective of the use of EMV cards for transaction. The main objective of the survey is to carry out empirical research on the users' adoption of the EMV technology and their perception of transactions done with the EMV cards. The results from the survey show that users are quite fearful of the transaction and payment system and majority still prefer paying with physical currencies rather than paying with EMV smart cards. They only adopt EMV cards for transactions when other options such as insufficient cash or unavailability of an ATM machine are not obtainable. Therefore, it is recommended that a review of the protocols, design and user protection policy be done to further mitigate credit card frauds.

Acknowledgment

The author would like to acknowledge the Faculty of Cognitive Sciences and Human Development, Univerisiti Malaysia Sarawak as well as the Faculty of In-formation and Communication Technology, International Islamic University Malaysia. The authors also gratefully acknowledge the helpful comments and sug-gestions of the reviewers, which have improved the presentation.

References

[1] Anderson, R., Bond, M., & Murdoch, S. J. (2007). Chip and spin. Infosecurity, 4(8), 38–40. https://doi.org/10.1016/S1754-4548(07)70204-8

[2] Barisani, A., Bianco, D., & Laurie, A. (2011). Chip & PIN is definitely broken - Credit Card skimming and PIN harvesting in an EMV world. In Defcon 2011.

[3] Bond, M., Choudary, O., Murdoch, S. J., Skorobogatov, S., & Anderson, R. (2014). Chip and skim: Cloning EMV cards with the pre-play attack. In Proceedings - IEEE Symposium on Security and Privacy (pp. 49–64). https://doi.org/10.1109/SP.2014.11

[4] Degabriele, J. P., Lehmann, A., Paterson, K. G., Smart, N. P., & Strefler, M. (2012). On the Joint Security of Encryption and Signature in EMV BT - Topics in Cryptology – CT-RSA 2012: The Cryptographers' Track at the RSA Conference 2012, San Francisco, CA, USA, February 27 – March 2, 2012. Proceedings. In O. Dunkelman (Ed.), Lecture Notes in Computer Science (LNCS) (pp. 116–135). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-27954-6_8

[5] Drimer, S., & Murdoch, S. J. (2007). Keep your enemies close: Distance bounding against smartcard relay attacks. USENIX Security Symposium, 7. Retrieved from http://dl.acm.org/citation.cfm?id=1362910

[6] Drimer, S., Murdoch, S. J., & Anderson, R. (2008). Thinking inside the box: System-level failures of tamper proofing. In Proceedings - IEEE Symposium on Security and Privacy (pp. 281–295). https://doi.org/10.1109/SP.2008.16

[7] EMVCo. (2011a). Integrated Circuit Card Specifications for Payment Systems, Book 3: Application Specification. EMV Integrated Circuit Card Specifications for Payment Systems. Retrieved from http://www.emvco.com/specifications.aspx?id=223

[8] EMVCo, L. (2011b). EMV – Integrated Circuit Card Specifications for Payment Systems, Book 4: Cardholder, Attendant, and Acquirer Interface Requirements, Version 4.2 ed. EMV2011, Dec, 4(November). Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Integrated+Circuit+Card+Specifications+for+Payment+Systems#1

[9] Francis, L., Hancke, G., Mayes, K., & Markantonakis, K. (2012). Practical relay attack on contactless transactions by using NFC mobile phones. Cryptology and Information Security Series, 8, 21–32. https://doi.org/10.3233/978-1-61499-143-4-21

[10] Gray, D., & Ladig, J. (2015). The Implementation of EMV Chip Card Technology to Improve Cyber Security Accelerates in the U.S. Following Target Corporation's Data Breach. International Journal of Business Administration, 6(2), 60–67. https://doi.org/10.5430/ijba.v6n2p60

[11] Murdoch, S. J. (2009). Reliability of Chip & PIN evidence in banking disputes. Digital Evidence and Electronic Signature Law Review, 6, 98–115. https://doi.org/10.14296/deeslr.v6i0.1862

[12] Murdoch, S. J. (2015). Banks undermine chip and PIN security because they see profits rise faster than fraud.
[13] Murdoch, S. J., Drimer, S., Anderson, R., & Bond, M. (2010). Chip and PIN is broken. In Proceedings - IEEE Symposium on Security and Privacy (pp. 433–446). https://doi.org/10.1109/SP.2010.33
[14] Murdoch, S. J., Drimer, S., Anderson, R., & Bond, M. (2013). EMV PIN verification " wedge " vulnerability.
[15] Ruiter, J. De, & Poll, E. (2012). Formal Analysis of the EMV Protocol Suite, 113–129.
[16] The U K Cards Association. (2012). Card Expenditure Statistics. January.
[17] The UK Cards Association. (2009). Standard 70, Book 2 – Card Acceptor to Acquirer Interface Standards: Messages, Data Elements and Code Values for Real-time Systems..