Al-Rafidain Journal of Computer Sciences and Mathematics (RJCM)

www.csmj.mosuljournals.com

EMV Electronic Payment System and its Attacks: A Review

Ahmed O. Ibrahim[1],* Yaseen Hikmat Ismael [2]

Department of Computer sciences, University of Mosul, Mosul, Iraq[1] , Department of Computer sciences, University of Mosul, Mosul, Iraq [2]

**Corresponding author. Email: Ahmed.csp34@student.uomosul.edu.iq [1]*

Article information

Article history:
Received : 26/5/2021
Accepted : 29/7/2021
Available online :

Abstract

Recently,The Automated Teller Machines (ATM) and Point of Sale (POS) are based on the Europay, MasterCard and VisaCard (EMV) protocol. The goal of the EMV protocol is to enhance and improve the level of transaction security at both ATMs and Points of Sale. Despite the high performance of electronic payment systems, they suffer from attacks that can lead to unauthorized disclosure of cardholder data. This paper describes the EMV protocol and its features, and common attacks that threaten EMV card users in transactions at both ATMs and Points of Sale. The study will document the vulnerabilities that threaten EMV card holders and provide countermeasures against various potential attacks. It also describes the proposed methods that have been introduced in recent years to overcome these attacks and enhance the security level of the EMV protocol. The results of the comparison showed that biometrics has the highest performance in card security based on the EMV protocol with additional improvements in the encryption phase against all types of attacks.

Keywords:
EMV, ATM, POS, E-payment system, Smart Card, PIN, Attack.

Correspondence:
Author : Ahmed O. Ibrahim
Email:
Ahmed.csp34@student.uomosul.edu.iq

1. INTRODUCTION

The electronic payment system had great attention during the last decade because of its roles in commercial operations. It is an efficient and secured money transaction between the merchants and the consumer. Many methods had been proposed to improve the security level of transactions such as Credit card ,Debit card , E-money, E-wallet and Europay Master card and Visa card (EMV). They are widely used in all over the world to facilitate money transaction in secured manner[1].

The electronic payment systems are rather based on EMV protocol that is one of the preferred by consumers in most countries. They are rather represented by an Automated Teller Machine ATM or by Point of Sale that are based on the EMV protocol that are connected to the Card Issuing Bank CIB[2]. As another type, the transaction may occur between the consumer and the merchant via websites. These facilities made the EMV protocol more popular in the markets[3].

Although the reputation of EMV protocol had been attacked by intruders to fraud people or steal their money by using deferent methods such as algorithms or communication shims. Sometimes the card is stolen to be used in fake or unauthorized transactions. These attacks lead to improve the security level of EMV transactions by proposing several method to enhanced the security of EMV by additional options and procedures[4].

The study would document the vulnerabilities that threaten EMV Card holders and provide the countermeasures against the various possible attacks. It also shows the proposed methods that are presented in the recent years to overcome these attacks and enhance the security level of EMV protocol.

2. Electronic payment system

E-Payment is a system that provides the tools for payment as reward of services or goods via the internet by an authenticated terminals in on/offline state[5]. The efficiency and reliability of the e-payment system enables fast transactions in enhanced tracking capabilities. In addition to time reduction, They also reduce cost, increase trust between Merchants and Consumers. The implementation of improved technologies in the e-payment system is related to pecuniary transactions, in which consumers are interested in quality of e-payment. This technology had gained a shape of their own perceptions and expectations[3].

2.1 The General Definition:

The electronic payment system is the benefits of technology in modern services of banks. It enhances performance of banks and implement many activities in quick and accurate manner with high productivity [6]. Electronic payments is a mechanism of payment that implements digital media that has no real cash [7].

According to the Federal Financial Institutions Examination Council (2010) it has been defined as: electronic payment is a new payment practice for retail where a merchant retrieves payment information for goods and services and places this information in an electronic template that creates electronic files for processing over the network. In general, e-payment refers to electronic payment in the context of e-commerce online transactions conducted over the Internet. Electronic payments can also be defined as a paperless payment process [8].

2.2 Types of Electronic Payment:

The common types of e-payment can be classified as:

1- Prepaid cards: that consumers use prepaid cards for a predetermined amount via entering of a unique card numbers at the merchant sites[9].

2- Electronic cash: transactions are settled via electronic currency exchange[10].

3- Credit cards: are servers that authenticate cardholder and verify his/her account to ensure availability of sufficient funds before buying something[11].

4- Electronic check: is an electronic institution completing the transaction between the buyer's and the seller's bank in the form of an electronic check[12].

5- The debit card: is the customer maintains a positive balance in the bank account and the money deducted by the account when the debit transaction is made[13].

There are other types of e payment systems that are based in different protocols, methods materials and transactions[14].

3. EMV protocol

EMV is the security payment standard managed by a consortium EMV with shared control between payment schemes: Master Card, Visa, JCB (Japan Credit Bureau), American Express, Discover and China Union Pay. It allows to secure the communication between actors of NFC deposit/withdrawal and purchase transaction, via exchanging a set of security rules and messages [15].

To operate a secure EMV transaction such as deposit/withdrawal or purchase, the secured messages of EMV are exchanged between actors (terminals and consumes and Issuing Bank) in four steps [16][17][18]:

A. Initialization:

Primarily, ATM/POS gets basic data needed for the next steps, such as the Personal Account Number (PAN), the expiration date, and other information about the security and configuration features. The Card may optionally requests from the ATM/POS some information pre-sending its own data[16].

Optionally, the card may request some information from the terminal devices as specified in the first response and as follows: [16].

T → C: SELECT APPLICATION
C → T: [PDOL]
T → C: GET PROCESSING OPTIONS [(data specified by the PDOL)]
C → T: (AIP, AFL) Repeat for all records in the AFL:
T → C: READ RECORD (i)
C → T: (Contents of record i)

The protocol starts by selecting the payment application. In response to the selection, the card optionally provides a Processing Options Data Object List (PDOL).

The PDOL specifies which data, if any, the card wants from the terminal; this could for instance include the Terminal Country Code or the amount.

The card then provides its Application Interchange Profile (AIP) and the Application File Locator (AFL).

The AIP consists of two bytes indicating the supported features (SDA, DDA, or CDA, offline PIN, and if so encrypted or plaintext, etc.) and whether terminal risk management should be performed. The AFL is a list identifying the files to be used in the transaction [18].

1- Static Data Authentication (SDA): this method is based on the authenticated pre-stored data in the card. Online connection is not required.

2- Dynamic Data Authentication (DDA): this method is based on pre-stored nonce in card to generate the public key to authenticate card and perform the transaction. It needs to connect to authenticate card and another time to accomplish transaction.

3- Combined Data Authentication (CDA): It is a combination of the previous methods. In which, card authentication is performed by SDA with the pre-stored data at offline state, while the DDA implement the nonce to generate the public key during the transaction. It is obvious that it needs less connection times.

It is an optional step in which the client's payment device determines the ATM/POS. The ATM/POS executes most secure method if ATM/POS and the client's payment device support more than common methods. If none, this step will not be executed [17].

T → C: AUTHENTICATE (data specified by DDOL)

C → T: signSIC (ICC Dynamic Data,

H (ICC Dynamic Data, data specified by DDOL))

H stands for hash function and sign for signature

B. Authentication of the client:

This step provides security in case of lost and stolen card. The latter must support at least one Cardholder Verification Method (CVM), that can encounter one of the following CVMs: [16][17].

- Entering PIN: the client enters the PIN code into the pad on the ATM/POS. The entered PIN can be validated and verified in two ways:

- Online: by sending encrypted PIN using asymmetric key to the issuing bank.

- Offline: by sending encrypted PIN using asymmetric key to the Card to be compared with the PIN reference stored in its memory.

- Client's signature: A client presents a hard copy of his signature.

- PIN and signature: A combination of entered PIN and a hard copy signature are both depended.

- No CVM: It is only in contactless-NFC. PIN or signature is not required, because fast execution with limited amounts. The executing of CVM is controlled by the capabilities of the card to perform the transaction. First, the Card sends a CVM list of capabilities to the ATM/POS. The CVM list also indicates the CVMs priority order. The ATM/POS will execute each CVM according to that list .If one CVM fails, the ATM/POS continues with the next CVM until at least or successful one[17].

C. The actual transaction:

Finally, an optional step (as step2) if there is no common method, it can be executed either in the online mode (with the issuing bank) or in the offline mode (with card). The ATM/POS determines the mode that would be performed in actual transaction, but the card may refuse that choice of an offline mode and force the online mode. These modes are: [17][18].

- Offline transaction: The card provides a confirmation proof of the transaction via a Transaction Certificate (TC) to the ATM/POS, which sends it later to the issuing bank.

- Online transaction: the client's payment device provides an Authorization Request Cryptogram (ARQC) to the ATM/POS which forwards it to the issuing bank for approval. If the client's payment device receives the approval, then it sends a TC to the ATM/POS as a confirmation proof of the transaction.

- Declined transaction: In both modes, the card can completely reject the transaction if it sends an Application Authentication Cryptogram (AAC) to the ATM/POS instead of a TC or an ARQC. Fig. 1. Shows EMV payment system.

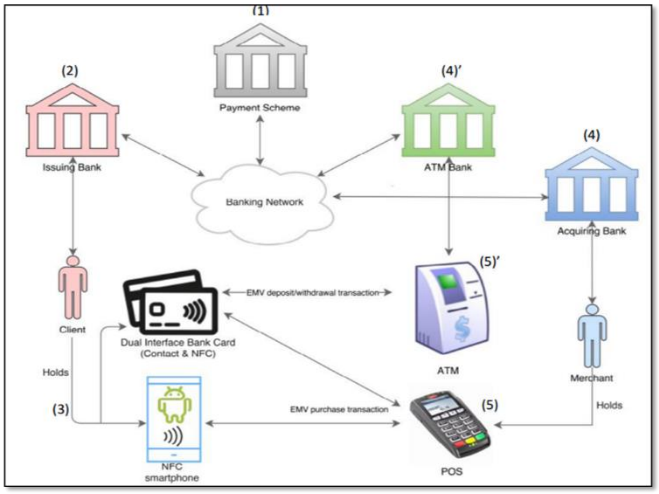

Fig.1 EMV payment system [15].

4. Attacks on EMV System

After the well reputation of EMV based systems, the intruders became more active to attack these systems. Several types of attacks had been invented to overcome the security of the EMV systems. The attackers take interest in the weakness points of the EMV protocol to gain unauthorized access to the consumers' accounts by means of deferent type of software or hardware. The following are some of the common types of attack:

4.1 Man-in-the-middle Attack (MITM)

An attacker is able to perform a MITM attack to intercept the connection between the card and the point-of-sale to trick the terminal by sending a 9000 response, without transferring the PIN to the genuine card and thereby the genuine card assumes that ATM/POS does not have "PIN verification" method and uses the signature method to verify the cardholder [19].

4.2 Pre-play Attack (PPA)

This attack uses an Unpredictable Number (UN) which has a fixed value. The low bits is a counter that is incremented in few milliseconds. It is cycling in 3 minutes. The UN that is generated at the ATM/POS may be predictable, what may provide the required card verification codes (CVC) to withdraw cash from an ATM at other time in which the UN can be predicted. This attack declares that ATMs generated a poor random number after analysis on few more ATMs. The pre-play attack can be used to downgrade the CVM in contactless(offline) Transactions in Magnetic strip based EMV by producing UN in range between 0 to 99,999,999. The main purpose of using the smart card instead of the magnetic stripe card because the magnetic stripe card is not authenticated [20][19].

4.3 NFC-Relay Attack

The Near-Field communication (NFC) is modern technology that allows communication between two devices within a short distance "5-10cm". There are three ways to perform the NFC Attack: [19]

- Card-emulation: The NFC devices emulates in offline mode as a contactless card.
- The peer-to-peer mode: The devices communicate with each other directly to trick both of the victim and the reader terminal.
- The read/write mode: The NFC devices communicate with the NFC tag via NFC-enabled device that acts as a malicious verifier.

This attack considers that the legitimate card has a fake contactless transaction via one of the previous method. While, the fake terminal operates the transaction either in the same time or at later (on/offline) [21].

4.4 Shim-in-the-middle Attack

A shim (flexible circuit and very thin board) is used in this attack by placing the shim between the card and the slot of terminal. This shim transmits a signal by the circuit to the nearest receiver to get the card information. Another shim may be attached to PIN entry Device (PED). The attacker may use the implanted shims after removing the legitimate card. The collected information can be used in a later fake transaction[22].

4.5 Camera and Double Swipe method

In this attack, the merchant is involved as an attacker. He uses a camera to snap the PIN that is taped during Customer enters his/her own PIN onto the PED. The merchant swipes the card into the POS twice to the first in a fake POS and the other into a legitimate POS. PIN intercepting allows the merchant to fraud the EMV card and operate a fake transaction by the taped PIN. This type of attack requires to modify the POS which is indeed a difficult process [23].

4.6 Counterfeit Terminal Attack

This type of attack requires Counterfeit terminal that contains either Software key bloggers or a hardware sensor to capture the PIN of the victim. A counterfeit terminal captures the data to forge the Chip card or use it in web transactions [24].

4.7 Signal Eavesdropping Attack

This attack is used to tap the line of data that is connected the PED. A small thin metal materials or wires can be attached to the data line of the terminal and they ae connected to a special purpose device that transfers the signals to a computer. The computer analysis the unencrypted information that are required to perform a fake transactions in different ways such as web transactions or by using stalled fake cards [19].

4.8 Active Relay Attack

This attack is a fraud method in which, a victim starts an EMV transaction with an installed reader by attacker without the victim's knowledge. In this case, the victim pays a small amount of money at the malicious reader. This reader relays the response of the card to a remote legitimate reader to start another legitimate transaction with more expensive items. Several types of this active attack is presented to be defeated. Those types based on different devices and methods. Mostly, these types are difficult to be detected immediately it requires a complex procedures and time [25].

5. Countermeasure of the Attacks on EMV System

The aim of this survey is to analyze the studies that presented solutions against the common attacks and evaluate the performance and its effects on EMV chip cards based systems. This allows to propose a better methods and solutions that faces those attacks. The related studies are:

In [26],the researchers proposed an enhancement for e-pay system based on EMV protocol via the dynamic tokenization and detokenization of the related protocol information. In addition to End-to-End encryption, the token generation is provided online by the Card issuing bank CIB as token service provider TSP. the tokens are used to represent all the transaction information in which the both of terminal and the server are secured and authenticated. No signature authentication is allowed. The result showed aa good performance against Man-in-the-Middle, Pre-lay, NFC-Relay, Eavesdropping and Active Relay attacks. Although of the promising results, the stolen Cads and PINs and other authentication information are still a weakness point.

In [27], the researchers proposed a method based on Readers-Writers Flow Model (RWFM). By which, the messages are labeled between the card and the terminal or between the terminal and the CIB. Each transaction is labeled according to a labeling dictionary that is used to generate the messages. If the labels do not match a specified label, the model will reject the message, otherwise it will be confirmed. The results showed good performance against MITM, Pre-play, SITM, Counterfeit Terminal, Signal Eavesdropping and Active Relay Attack. The RWFM must be implemented in the POS/ATM to secure transaction in either online or offline states. Another problem of the stolen cards and PIN cannot be overcome.

In [28], authors presented a new security protocol analyzed by the Scyther tool. Their method passed on new Certificate Authority for POS CAp that are trusted to the CIB. Additionally, a RSA2048 is used to generate a secret and public keys of CAp. Those keys are used to encrypt/decrypt data between the Card and terminal.

Actually, this method prevents MITM and Relay attacks, but it still faced the same problem of the stolen cards and captured PIN.

In [29], the authors proposed an enhancement of EMV based on offline tokenization. A Token service provider TSP generates tokens based on nonce of transaction in the POS that are encrypted by end-to-end cryptosystem. During transaction, the method prevents eavesdrop attacks and active relay attack with considering trusted TSB in CIB.

In [30], the authors a management authentication to provide mutual authentication between the POS and the NFC device. In which both of the POS and NFC device are authenticated by implementing a management authentication server MAS. The method prevents NFC-relay, replay and MITM attacks.

In [31], the authors presented an EMV system based on dual authentication stages and biometrics implementation. An Authentication Server AS is used to authenticate both of the terminals and the Management Server MS. The AS controls all users communication including registration and key generation. Where the MS controls the AS and the other

procedures such as re-registration and change password. The method is robust against several types of attacks, but it needs another enhancement.

In [32], the authors presented EMV system based on iris authentication in NFC smart phone. The NFC smart phone transmits Application Protocol Data Unit (APDU) command to the NFC reader, and smart phone receives from latest APDU response. The IRIS image used as a key in encryption/decryption process between the phone and terminal. It is obvious that the method overcome authentication of NFC—relay attack.

6. Comparison

The previous studies have been analyzed to evaluate their proposals and its capabilities against various attacks. Some of these methods still have weak points against some attacks, specially, in authentication steps. Others had tried to solve authentication problems as in the type of devices and terminals. Generally, (Table .1) illustrates the main evaluation parameters of the previous analyzed methods.

Table .1: Analyzed Methods.

Name of Attack	***Ref No.***	***Connection status***	***Needed Equip.***	***Cost***	***Success***	***Proposal***
Man-in-the-middle Attack (MITM)	26	Offline	Fake terminal	High	Possible	-No signature Authorization
	27	On/offline			Possible in RWFM terminals	-RWFM implementation
	28	On/offline			Possible with CAp	-implement a CAp -Encryption system for CAp
	29	Offline			Possible with Offline token authorization	-Implement Trusted Offline tokenization -End-to-end Encryption
	30	On/offline			Possible if MAS provided	-management Authentication
	31	Online			Possible if implementation of two servers	-Dual stage Authentication based on Biometrics and PIN
	32	Online			Possible with IRIS Authentication	-IRIS biometric implementation -IRIS is key of encryption system -Mutual authentication between the phone and the terminal
Pre-play Attack (PPA)	26	Offline	Fake terminal	High	Possible with proposed procedures	-Mutual authentication -End-to-end encryption -Dynamic Transaction Token -Passcode for payment app
	27	On/offline			Possible in RWFM terminals	-RWFM implementation - Using Nonce
	30	On/offline			Possible if MAS provided	-management Authentication
	31	Online			Possible if implementation of two servers	-Dual stage Authentication based on Biometrics and PIN
	32	Online			Possible with IRIS Authentication	-IRIS biometric implementation -IRIS is key of encryption system -Mutual authentication between the phone and the terminal
Name of Attack	Ref No.	Connection status	Needed Equip.	Cost	Success	Proposal
NFC-Relay Attack	26	Online	Fake terminal	High	Possible with proposed procedures	-Mutual authentication -End-to-end encryption -Dynamic Transaction Token -Passcode for payment app
	27				Possible in RWFM terminals	-RWFM implementation
	30				Possible if MAS provided	-management Authentication
	32				Possible with IRIS Authentication	-IRIS biometric implementation -IRIS is key of encryption system -Mutual authentication between the phone and the terminal

Shim-in-the-middle Attack	26	Offline	Shim	Low	Possible in RWFM terminals	-RWFM implementation
Camera and Double Swipe method	26	Offline	Camera+ sensors or software	Medium	Possible in RWFM terminals	-RWFM implementation
	29	Offline			Possible with Offline token authorization	-Implement Trusted Offline tokenization -End-to-end Encryption
Counterfeit Terminal Attack	26	Offline	Fake terminal	High	Possible in RWFM terminals	-RWFM implementation
	29	Offline			Possible with Offline token authorization	-Implement Trusted Offline tokenization -End-to-end Encryption
Signal Eavesdrop Attack	26	Online/offline	Special purpose device	Medium	Possible with available software and hardware	-Authorized Amount by user -Dynamic Transaction Token -Secure channel
	29	Online/offline			Possible with Offline token authorization	-Implement Trusted Offline tokenization -End-to-end Encryption
	31	Online			Possible if implementation of two servers	-Dual stage Authentication based on Biometrics and PIN
Active Relay Attack	26	Online	Special purpose device	High	Possible with available software and hardware	-Authorized Amount by user -Dynamic Transaction Token -Secure channel
	27				Possible in RWFM terminals	-RWFM implementation
	28				Possible with CAp	-implement a CAp -Encryption system for CAp
	29				Possible with Offline token authorization	-Implement Trusted Offline tokenization -End-to-end Encryption
	31				Possible if implementation of two servers	-Dual stage Authentication based on Biometrics and PIN

7. Discussion Conclusion

As mentioned before, the previous methods had overcome some weak points of EMV security. All the methods are capable to overcome the MITM attack. Researchers in [26-27-30-31-32] are capable to overcome Pre-play attack. While researchers in [26-27-30-32] are capable to overcome NFC-relay attack. [26] is capable to overcome Shim-in-the-Middle attack. In [26-29], the researchers are capable to overcome camera and double swap attack and Counterfeit Terminal Attack. In [26-29-31] the researchers are capable to overcome Signal eavesdrop attack. In [26, 27, 28, 29, 31] the researchers are capable to overcome Active relay attack.

It is obvious that there is a lack in some of the previous methods that allow intruders to access the consumers transactions. Although the IRIS authentication are used in [32] but it has to be re-designed to obtain more robustness.

This study has analyzed some previous methods that tried to enhance the security level of EMV payment system. These methods are based in varied techniques to overcome unauthorized access to the consumers' accounts. Most of these methods are not able to authenticate the person that provide a Card and PIN. Most recent methods use the biometrics to authenticate the cardholder. But they still have a lack on eavesdropping or high technical attacks that might provide one or more of biometrics in deferent levels of complexity.

This study suggests that the biometrics are very robust against most types of attacks. They have to be implemented with nonce and high-performance cryptosystem like (Bio-Hashing). It is reasonable to use a special technique to manipulate with the parameters of EMV protocol.

NOTES: In Table No. 1, it should be noted that the cost means the cost of what the attacker needs in terms of peripheral devices to carry out his attack. As for the success, it was found that the author succeeded in blocking a certain possible attack by the attacker. With regard to the proposal, the author suggested another improvement of the EMV protocol as a proposal to block more than one attack of the protocols.

References

[1] A. Premchand and A. Choudhry, “Future of Payments - ePayments,” Jun. 2015.

[2] S. A. Effiong and P. O. Nwanagu, “E-Commerce Transactions and Tax Revenue : A Commensal-Symbiotic Evaluation,” Eng. Manag. ·, no. August, 2020.

[3] N. R. Ab Hamid and A. Y. Cheng, “A risk perception analysis on the use of electronic payment systems by young adult,” WSEAS Trans. Inf. Sci. Appl., vol. 10, no. 1, pp. 26–35, 2013.

[4] A. R. Peša and A. Brajković, “Testing The ‘Black Swan Effect’ on Croatian Stock Market Between 2000 and 2013,” EMAJ Emerg. Mark. J., vol. 6, no. 1, pp. 1–16, 2016, doi: 10.5195/emaj.2016.92.

[5] Z. Bezhovski, “The Future of the Mobile Payment as Electronic Payment System,” Eur. J. Bus. Manag., vol. 8, no. 8, pp. 127–132, 2016.

[6] Shilpa and P. Sharma, “Advance Technique for Online Payment Security in E-Commerce : ‘ Double Verification ,’” Int. J. Comput. Sci. Eng., vol. 5, no. 6, pp. 508–513, 2013.

[7] P. Aigbe and J. Akpojaro, “Analysis of Security Issues in Electronic Payment Systems,” Int. J. Comput. Appl., vol. 108, no. 10, pp. 10–14, 2014, doi: 10.5120/18946-9993.

[8] Junadi and Sfenrianto, “A Model of Factors Influencing Consumer’s Intention to Use E-payment System in Indonesia,” Procedia Comput. Sci., vol. 59, no. Iccsci, pp. 214–220, 2015, doi: 10.1016/j.procs.2015.07.557.

[9] S. Zhou, A. Montgomery, and G. Gordon, “Exploring Customer Spending Behavior and Payday Effect using Prepaid Cards Transaction Data,” Work. Pap., pp. 1–17, 2016.

[10] S. Fatonah, A. Yulandari, and F. W. Wibowo, “A Review of E-Payment System in E-Commerce,” J. Phys. Conf. Ser., vol. 1140, no. 1, 2018, doi: 10.1088/1742-6596/1140/1/012033.

[11] R. J. Rodríguez, “Evolution and characterization of point-of-sale RAM scraping malware,” J. Comput. Virol. Hacking Tech., vol. 13, no. 3, pp. 179–192, 2017, doi: 10.1007/s11416-016-0280-4.

[12] P. Zhang, Y. He, and K. P. Chow, “Fraud track on secure electronic check system,” Int. J. Digit. Crime Forensics, vol. 10, no. 2, pp. 137–144, 2018, doi: 10.4018/IJDCF.2018040108.

[13] E. Payment, S. Use, S. In, and A. N. Arabic, “Electronic Payment Systems Use and Satisfaction in an Arabic Country: Evidence From Kuwait,” Issues Inf. Syst., vol. 16, no. II, pp. 149–160, 2015, doi: 10.48009/2_iis_2015_149-160.

[14] T. Wondwossen and G. Tsegai, “‘E-payment: Challenges and Opportunities in Ethiopia’,” Econ. Comm. Africa, no. October, p. Hal : 1-59, 2005.

[15] N. El Madhoun, E. Bertin, and G. Pujolle, “An overview of the EMV protocol and its security vulnerabilities,” 2018 4th Int. Conf. Mob. Secur. Serv. MOBISECSERV 2018, vol. 2018-Febru, no. February, pp. 1–5, 2018, doi: 10.1109/MOBISECSERV.2018.8311444.

[16] EMV Books - Integrated Circuit Card Specifications for Payment Systems, Book 1: Application Independent ICC to Terminal Interface Requirements, Book 2: Security and Key Management, Book 3: Application Specification, Book 4: Cardholder Attendant and Acquir. , V. 4.3, EMVCo.

[17] J. de Ruiter and E. Poll, “Formal analysis of the emv protocol suite,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6993, pp. 113–129, 2015, doi: 10.1007/978-3-642-27375-9_7.

[18] J. Van Den Breekel, D. A. Ortiz-yepes, E. Poll, and J. De Ruiter, “EMV in a nutshell,” Tech. Rep., pp. 1–37, 2016.

[19] D. Singh, R. Ruhl, and H. Samuel, “Attack Tree for Modelling Unauthorized EMV Card Transactions at POS Terminals,” ICISSP 2018 - Proc. 4th Int. Conf. Inf. Syst. Secur. Priv., vol. 2018-Janua, no. Icissp, pp. 494–502, 2018, doi: 10.5220/0006723304940502.

[20] N. S. Maddi, “EMV Chip and PIN: A Feeble Upgrade,” 2018.

[21] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, “Practical relay attack on contactless transactions by using NFC mobile phones,” Cryptol. Inf. Secur. Ser., vol. 8, pp. 21–32, 2012, doi: 10.3233/978-1-61499-143-4-21.

[22] M. A. Ali, M. A. Azad, M. Parreno Centeno, F. Hao, and A. van Moorsel, “Consumer-facing technology fraud: Economics, attack methods and potential solutions,” Futur. Gener. Comput. Syst., vol. 100, pp. 408–427, 2019, doi: 10.1016/j.future.2019.03.041.

[23] N. Scaife, C. Peeters, and P. Traynor, “Fear the reaper: Characterization and fast detection of card skimmers,” Proc. 27th USENIX Secur. Symp., pp. 1–14, 2018.

[24] Z. Olowolayemo, A., Adewale, N., Zeki, A. M., & Ahmad, “Examining Users’ Understanding of Security Failures in EMV Smart Card Payment Systems.,” Int. J. Informatics Vis., vol. 3(2), 185-.

[25] Y. Zeng and R. Zhang, “Active eavesdropping via spoofing relay attack,” ICASSP, IEEE Int. Conf. Acoust. Speech Signal Process. - Proc., vol. 2016-May, pp. 2159–2163, 2016, doi: 10.1109/ICASSP.2016.7472059.

[26] D. Jayasinghe, K. Markantonakis, R. N. Akram, and K. Mayes, “Enhancing EMV tokenisation with dynamic transaction tokens,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 10155 LNCS, pp. 107–122, 2017, doi: 10.1007/978-3-319-62024-4_8.

[27] K. Shrikrishna, N. V. N. K. B, and R. K. Shyamasundar, “Security Analysis of EMV Protocol,” vol. 2, no. December, pp. 69–85, 2018, doi: 10.1007/978-3-319-72344-0.

[28] N. El Madhoun, E. Bertin, M. Badra, and G. Pujolle, “Towards more secure EMV purchase transactions: A new security protocol formally analyzed by the Scyther tool,” Ann. des Telecommun. Telecommun., vol. 76, no. 3–4, pp. 203–222, 2021, doi: 10.1007/s12243-020-00784-1.

[29] D. Jayasinghe, K. Markantonakis, I. Gurulian, R. N. Akram, and K. Mayes, “Extending EMV tokenised payments to offline-environments,” Proc. - 15th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 10th IEEE Int. Conf. Big Data Sci. Eng. 14th IEEE Int. Symp. Parallel Distrib. Proce, pp. 443–450, 2016, doi: 10.1109/TrustCom.2016.0095.

[30] A. Al-Haj and M. A. Al-Tameemi, “Providing security for NFC-based payment systems using a management authentication server,” 2018 4th Int. Conf. Inf. Manag. ICIM 2018, pp. 184–187, 2018, doi: 10.1109/INFOMAN.2018.8392832.

[31] M. Boopathi and M. Aramudhan, “Dual-Stage Biometrics-Based Password Authentication Scheme Using Smart Cards,” Cybern. Syst., vol. 48, no. 5, pp. 415–435, 2017, doi: 10.1080/01969722.2016.1262703.

[32] S. Chabbi, R. Boudour, and F. Semchedine, “A secure protocol, based on iris technology, for NFC phone applications,” Proc. 2017 Int. Conf. Math. Inf. Technol. ICMIT 2017, vol. 2018-Janua, pp. 78–83, 2017, doi: 10.1109/MATHIT.2017.8259699.

نظام الدفع الإلكتروني EMV وهجماته: ورقة مراجعة

احمد أسامة إبراهيم ياسين حكمت إسماعيل
قسم علوم الحاسوب ، كلية علوم الحاسوب والرياضيات،
جامعة الموصل ، الموصل العراق

تاريخ استلام البحث: 2021/5/26 تاريخ قبول البحث: 2021/7/29

الخلاصة:

في الآونة الأخيرة ، تعتمد أجهزة الصراف الآلي (ATM) ونقاط البيع (POS) على بروتوكول Europay و MasterCard و VisaCard (EMV). الهدف من بروتوكول EMV هو تعزيز وتحسين مستوى أمان المعاملات في كل من أجهزة الصراف الآلي ونقاط البيع. على الرغم من الأداء العالي لأنظمة الدفع الإلكتروني، إلا أنها تعاني من هجمات قد تؤدي إلى الكشف غير المصرح به عن بيانات حامل البطاقة. تصف هذه الورقة بروتوكول EMV وميزاته، والهجمات الشائعة التي تهدد مستخدمي بطاقة EMV في المعاملات في كل من أجهزة الصراف الآلي ونقاط البيع. ستوثق الدراسة نقاط الضعف التي تهدد حاملي بطاقات EMV وتوفر تدابير مضادة ضد مختلف الهجمات المحتملة. كما يصف الطرق المقترحة التي تم تقديمها في السنوات الأخيرة للتغلب على هذه الهجمات وتحسين مستوى الأمان لبروتوكول EMV. أظهرت نتائج المقارنة أن القياسات الحيوية تتمتع بأعلى أداء في أمان البطاقة استنادًا إلى بروتوكول EMV مع تحسينات إضافية في مرحلة التشفير ضد جميع أنواع الهجمات.

الكلمات المفتاحية: EMV، جهاز الصراف الالي ، نقاط بيع ، نظام الدفع الإلكتروني ، البطاقة الذكية ، رقم التعريف الشخصي ، هجوم.