International Journal for Modern Trends in Science and Technology
Volume: 03, Issue No: 07, July 2017
ISSN: 2455-3778
http://www.ijmtst.com

A Review and Comparative Analysis on Fake Electronic Data Capture Device for Off-Line E-Commerce

Jayaprakash P[1] | Dr.E.Ramaraj[2]

[1]M.Phil., Scholar in Department of Computer Applications, Alagappa University, Karaikudi, Tamilnadu, India.
[2]Professor, Departmentof Computer Science, Alagappa University, Karaikudi, Tamilnadu, India.

To Cite this Article
Jayaprakash P and Dr. E.Ramaraj, "A Review and Comparative Analysis on Fake Electronic Data Capture Device for Off-Line E-Commerce", *International Journal for Modern Trends in Science and Technology*, Vol. 03, Issue 07, July2017, pp. 67-71.

ABSTRACT

Among the new innovations, credit and debit card is an essential part of the trade. When purchase is happening on online and offline, card can aid to buy the things easily. Even everything has done through those cards in particular place, information of cards which is to be in securely by the card holder. Around the more number of merchants have Point of Sale (PoS) System; it detects money from debit card holder account whereas credit card also to make the basic transaction but the company charges some interest on a purchase if the account hasn't sufficient money. Modern PoS systems are integrated with the computers as well as it has a data readers to read the data from cards, which is used as an input to the PoS system. In this scenario, the device has malware which may steal card information and there is no security on the online payment. On how to do overcomes from the conventions of PoS System. This paper is given the preeminent concept for the extreme security.

KEYWORDS:*Unclonable PUF, Resilient Device, protocols, Secure Micro Payments*

I. INTRODUCTION

Several interacting threats, like globalization, demanding consumers, increasing administrative burden and a financial recession force the retailers into action. A specific type of retail Information and communication technology (ICT) that can be working to complete operative store management is a 'Point-of-Sale' (PoS) system.PoS systems act as gateways and require some sort of network connection in order to contact external credit card processors. This is mandatory to validate transactions. To reduce cost and simplify administration and maintenance, PoS devices may be remotely managed over these internal networks.PoS systems are defined in many different methods.

A point-of-sale system tracks sales and identifies inventory levels in real time. There are many different kinds and products of PoS systems available. When a transaction happens it will combine with the server for authentication in each and every process. There is lots of personal information in user magnetic stripe payment cards. Name, account number, password and some other optional data. Know that some information used by airlines when securing reservations with credit card and also some information contains card's account, encrypted PIN may use by ATM to ensure the security. However, thieves also want this information.

Maximum malicious procedures and packages can gather these data and may emulation cards to make purchases or take out cash from ATMs. That will cause great losses for credit card customers. PoS systems are not widely used by these retailers. However, since those superstore 'Target' installment units were assaulted Also over 40 million client's credit cards information unmistakable on attackers, there need aid stacks of PoS malware discovered over later a long time. There are two kinds of essential data information of credit cards Track1 and Track2.

II. RELATED WORK

In [1] author "Anitha, et al."has described, FRODO recognitions for a safe disconnected small scale installment is pliant to PoS information ruptures. It uses the components and protocols to secure transactions while transaction is happening. Result of the paper which provides the convenience interface and extreme secure transaction. The current off-line elucidation implement a withdrawal-phase producing tokens which are pre-computed and pre-cached within a device.

In [2] author "S. von Sohns"sayspresent the various point of sale terminals system. After a transaction PoS device has printed the relevant information about the merchant and consumer receipts, which is enough to perform the succession of online transaction. While the transaction is progress cvv number also obtained to complete transaction without knowledge of authorized card holder.

In [3] author "Tan Soo Fun, Leau Yu Beng"This paper has summarized Mobile payment protocols of the mobile. In every communication has to optimize technique. Which is also having protocol schemes to reduce the computational process of the transaction. It is achieved by the self-certified signature and Symmetric key approach. Macro payment has four major schemes such as KSL protocol, Anonymous protocol, Private Protocol and Secure Agent-based Protocol.

In "Ram Kumar Garg, NK Garg",who has presented[4]about the Biometric payments instead of PoS system. While thecards are used for purchasing online products through the either debit or credit card, this could be read and stored the data on pos system. Bio metric payment has used the integrating Tokenization which could eliminate the risk and make it a highly secure payment instrument. In future biometric system provides the safe and comfortable payment.

In [5] author "Marian Margraf, Steffen Lange"Security Evaluation of Apple Pay at Point-of-Sale Terminals is definedabout the security evaluation of Apple pay. Unlike the traditional credit card payment, to verify the cardholder details using the TouchID mechanism, this can read the data. Additionally the privacy evaluation has to be conducted for the security purpose.

In [6] author "OussamaTahan, Farah Barake" My vWallet-A smartphone application for assisting people with math difficulties at point of sale is defined the v wallet. It's a smart phone application for improving the efficiency of the money handling. Mathematical computation difficulties are there among the peoples who haven't required knowledge to calculate the bill payments. But this application provides the easy manner and achieves the transaction as soon as possible.

III. PERFORMANCE ANALYSIS

S No	Name of the paper	Search Techniques	Authors	Result of the method
1	Preserving Micro-Payments in Deception of Resilient Devices	Electronic Payment System, Digital Coins	A.Anitha, R.Jagatheeswari and L.Lavanya	1. Software developed to confine copy or clone. 2. Highly secure micropayment Elucidation, flexibility in payment medium.
2	An investigation into credit card information disclosure through Point of Sale purchases	card-absent transaction	Von Solms, Sune	1. Wireless technologies for merchants seeking to receive payments remotely. 2. Convenience and eliminates the risk of carrying large cash amounts.
3	Developing secured biometric payments model using Tokenization	Biometric Payments, Payment Card System, Tokenization	Garg, Ram Kumar, and N. K. Garg	1. Integrate with the tokenization and Biometric Payments could eliminate the risk and make it a highly secure payment instrument.

4	PayWord and MicroMint:Two Simple Micropayment Schemes	Public key operation and hash function.	Ronald L.Rivest and Adi Shamir	1. Signature verification 100 times fast 2. Signature generation 10,000 times fast.
5	Anonymous Subscription Schemes A Flexible Construction for On-line Services Access	Subscription Scheme.	H. Li, D. Liu, K. Jia, and X. Lin	1. Multiple anonymous may allow to the transaction and if the same token used more one time the anonymous can be identified through the service provider.
6	FORCE Fully Off-line secuReCrEdits for Mobile Micro Payments	State-Of-the art approach	VanesaDaza1, RobertoDiPietro and FlavioLombardi.	1. Micropayment approach all involved parties can be fully offline 2. Security and flexibility.
7	A Complete Secure Customer Centric Anonymous Payment in a Digital EcoSystem.	Symmetric key	Vorugunti Chandra Sekhar	1. SET, iKP, Kungpisdan et al and Tellez et al protocols are used by security purpose.
8	A Rotary PIN Entry Scheme Resilient to Shoulder-Surfing	Spin wheel	Peipeishi, Bo Zhu and AmrYouseef	1.Need not to memorize the PIN
9	An Investigation into Credit Card Information Disclosure through Point of Sale Purchases	Medium wireless technologies	Von Solms	1. Relevant information printed on the merchant and customer Transaction receipts after a transaction.
10	A Secure Wireless Point of Sale System	Short range wireless technologies	David Busuttil	1. The PoS system has achieved by the infra-red technology. 2. Hash function also applied to care the sensitive data of cardholder.
11	KerNeeS A protocol for mutual authentication between NFC phones and POS terminals for secure payment transactions	Mutual authentication	UgoBiaderCeipidor, Carlo Maria Medaglia, Antonella Marino, Serena Sposato, Alice Moroni	1.To perform the mutual authentication 2. integrated with EMV protocol for payments.

IV. Resilient Device Mechanisms

4.1 Protocols

A. Pairing Phase

A pairing protocol is a Bluetooth Passkey pairing process. The customer and vendor device will share the public key used for message integrity and authenticity.

B. Payment Phase

Payment Protocol will be described in two different points of view. The encrypted message exchanged between vendor and customer using Identity Element and Coin Element.

4.2 Attackers

A. Skimmers

In this attack, the client input device that belongs to the POS system is exchanged with a fake one in order to capture customer's card data. As an example, input system can be each really replaced or straight purchased with in danger or misconfigured software.

B. Scrapers

A malware is connected within the PoS system in order to theft customer's card data. As an example, cybercriminals can infect the system using phishing attacks. However, in some other cases, the malware is installed with the help of an insider or via a backdoor. RAM scrapers toil by inspecting the list of procedures that are organization on the

POS system and by checking the storage for user's card data such as account numbers and expiration dates. Then, they usually encrypt and store the stolen data somewhere on the POS network until they can be ex filtrated. Just like standard viruses, POS malwares do not have a single, well-defined, taxonomy. In any case, a few POS malware individuals have been depicted and acknowledged so far, for example, Alina, Dexter, vSkimmer, FYSNA, Decebel and BlackPOS.

C. Forced Off-line authorization

In this scenario, the attacker exploits a DoS attack to force the POS system to go off-line. By doing so, the attacker will force the payment card data to be locally processed. This funds that any records read from the card will be locally decrypted and verified, thus generating an occurrence for the aggressor to easily collect all the required data.

D. Software Vulnerabilities

Payment applications themselves are also vulnerable to numerous attacks. In application programming interface (for short, API) attacks, lack of access control systems is exploited to retrieve sensitive card data. Disassembling techniques are also used either to alter firm wares / software's or to replace them with malicious functionalities. Many other attacks such as spoofing, sniffing and input attaching are also used by attackers and each one of them exploits some payment software vulnerabilities.

4.3 Security Analysis

A. Authenticity

For authentication process, FEDC used computation of private keys. The coin element and key element use key generator to compute private key needed to encrypt and decrypt all messages exchanged in the protocol.

B. Non – Denial

Deleting past transactions and keep the storage device physically safe. The content of storage device is backed up and exported to secondary devices.

C. Confidentiality

To achieve confidentiality, communication between customer and vendor message is encrypted.

V. CONCLUSION

Point of sale is used in all the trade marks to purchase the goods. After the every transaction, the PoS system has been holding the sensitive data of a cardholder still now. All the proposed techniques are classified as advantage and disadvantage separately in this review. If the Following features would use in the future, which will help to protect the sensitive information's Such as printing the data of particular transaction without stored information in database.

References

[1] Anitha, A., et al. "Preserving Micro-Payments in Deception of Resilient Devices."

[2] Von Solms, Suné. "An investigation into credit card information disclosure through Point of Sale purchases." Information Security for South Africa (ISSA), 2015. IEEE, 2015.

[3] Garg, Ram Kumar, and N. K. Garg. "Developing secured biometric payments model using Tokenization." (ICSCTI), 2015 International Conference on. IEEE, 2015.

[4] Margraf, Marian, Steffen Lange, and Florian Otterbein. "Security Evaluation of Apple Pay at Point-of-Sale Terminals." (NGMAST), 2016 10th International Conference on. IEEE, 2016.

[5] Tahan, Oussama, et al. "My vWallet-A smartphone application for assisting people with math difficulties at point of sale." (ICTA), 2015 5th International Conference on. IEEE, 2015.

[6] Ronald L. Rivest and Adi Shamir [2009], "PayWord and MicroMint:Two Simple Micropayment Schemes" MIT Laboratory for Computer Science, 545 Technology Square, Cambridge, Mass.02139, rivest @theory.lcs.mit.edu.

[7] H. Li, D. Liu, K. Jia, and X. Lin [2010],"ANONYMOUS SUBSCRIPTION SCHEMES A Flexible Construction for On-line Services Access**"**Mar´ıa Isabel Gonz´alez Vasco Dep. Matem´aticaAplicada, Univ. Rey Juan Carlos, Madrid, Spain.

[8] VanesaDaza1, RobertoDiPietro and FlavioLombardi [2014],"FORCE Fully Off-line secuReCrEdits for Mobile Micro Payments" Department of Information and Communication Technologies- Universitat Pompeu Fabra, Barcelona, Spain.

[9] Voruguntі Chandra Sekhar [2012],"A Complete Secure Customer Centric Anonymous Payment in a Digital EcoSystem", [ICCEET].

[10] Peipeishi, Bo Zhu and AmrYouseef[2009], "A Rotary PIN Entry Scheme Resilient to Shoulder-Surfing", Concordia Institute for Information Systems Engineering Concordia University,Montreal, Quebec, Canada pesh, zhubo, Youssef@ciise.concordia.ca.

[11] Von Solms[2015], "An Investigation into Credit Card Information Disclosure through Point of Sale Purchases", (CSTR) School of Electrical, Electronic and Computer Engineering North West University svsolms@csir.co.za.

[12] David Busuttil[2011], "A Secure Wireless Point of Sale System", Technology Department ,Vodafone Malta Ltd, Naxxar, Malta, david.busuttil.vodafone.

[13] UgoBiaderCeipidor, Carlo Maria Medaglia, Antonella Marino, Serena Sposato, Alice Moroni [2012]," KerNeeS A protocol for mutual authentication between NFC phones and POS terminals for secure payment transactions", CATTID, Sapienza University of Rome ScuolaIaD – University of Rome Tor Vergata Rome, Italy