SECURE MICROPAYMENTS USING PHYSICAL UNCLONABLE FUNCTION

Mareeswari.R[1], Gayathri.D[2], Assistant Professor Vanitha.D[3] and Project Coordinator Kapilavani R.K[4]

[1,2] Department of Computer Science and Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India
[3]Assistant Professor, Department of Computer Science and Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India
[4]Assistant Professor, Department of Computer Science and Engineering, Prince DR.K Vasudevan college of Engineering and technology,Chennai,India.

ABSTRACT

EMV card data theft is one of the earliest forms of cybercrime. Attackers often aim at stealing such customer data by targeting point of sale(POS) system. PoS is a combination of software and hardware that allows merchants to take transactions. Modern PoS systems are well equipped with the card reader and running specialized software. Customer and vendor are persistently or intermittently disconnected from the network, no secure online payment is possible. This paper describes PUF, a secure offline micropayments solution that is resilient to PoS breaches. This solution improves the flexibility and security.

Keywords: micropayments, protocols, cybercrime, fraud-resilience.

1 INTRODUCTION

Market industries uses the card processing, Now a days is increasingly popular, It will be overtake the traditional marketplace. This process providing the greater convenience to the customer. Widely supported recent hardware, it is expected to rise in the near future as demonstrated by growing interest in crypto currencies. The first pioneering micropayments scheme, was proposed by Rivest and Shamir back in 1996. Nowadays, crypto currencies and decentralized payment systems(e.g Bitcoin[3]).Fostering a shift from physical to digital currencies.

1.1 PROBLEM AND OBJECTIVES

Several retail industries have been victims of information security breaches. Payment data theft is targeting consumer payment card data and Personally Identifiable Information[4],[5].

Structure of the electronic payment system, PoS systems always handle critical information and also require remote management[7].
PoS system act as gateways and require some sort of network connection in order to contact external credit card processors. Larger business that wish to tie their PoSes with other back end systems may connect the former to their own internal networks. In addition, to reduce cost and simplify administration and

maintenance, PoS devices may be remotely managed over these internal networks. RAM scraping malware [5][6].

Payment card industry security standards council to establish data security standards for all those organizations that handle credit, debit, and ATM card holder information.

Fig:1.1 Resilient device or Vendor device or swiping machine

In payment processing can be classified as fully online, semi offline, weak offline, fully offline [8][9]. Fully oofline approach is the difficulty of checking the trustworthiness of a transaction without a trusted third party. Communication protocol used for payment transaction. The main benefir is simpler, faster and secure interaction between involved actors/entities.

2 RELATED WORK

Solutions can be proposed the payment schemes classified as following:
Fully On-line: solutions such as that require the customers mobile device to be connected to a network in order to communicate with a bank, a bank, a payment gateway or a trusted third party.
Semi Off-line: solutions such as that require an active connection only on the vendor side.
Weak Off-line: Weak off-line category work with digital cash designed to be accepted either by specific vendors (known as digital vouchers).
Fully Off-line: solutions that do not require any external connection but either assume involved devices to be trusted or are limited to transactions tied to a bank account.
Main issue of a fully off-line solution is that keeping track of past transactions can be hard, as it is difficulty for vendors to check if some digital credits have already been spent.

In Exixting System using the private key, the encryption process using the Data Encryption Standard encryption algorithm . In existing we use only one key used for encryption and decryption process. In proposed system we use private key for encryption, and using the RSA algorithm. Bankers public key used for decryption process. The algorithm is Advanced Encryption Standard.

Physical unclonable function [9] is a key component . It is already been proposed in past. It is mainly used for authentication process.

FORCE provide a weak prevention strategy based on data confusion and did not address the most relevant attacks aimed at threatening customer sensitive data. Thus being vulnerable to many advanced attack techniques.

Payment transactions are usually processed by an electronic payment system (EPS).
The EPS is a separate function from the typical point of sale function. EPS performs all payment processing , while the PoS system is the tool used by the cashier or consumer.

3 POS SYSTEM BREACHES

PoS sytems network level hacking can be rendered possible by exploiting shared connections, open networks, or by cracking the password of the merchants network. Network can be monitoted and protected against malicious activities.

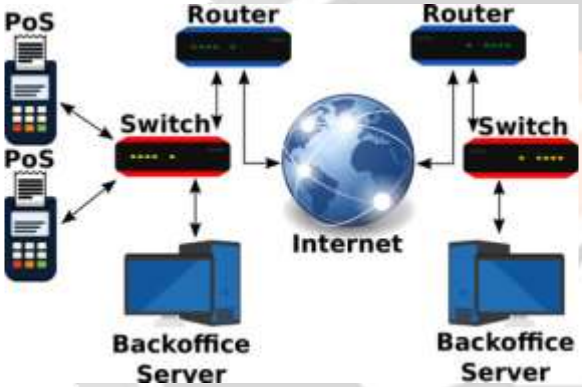


Fig 2: Point of Sale Architecture

Payment process composed of two main processing phases, the authorization and settlement.
Authorization is the state of the payment process where the purchase is verified and finalized. The settlement comprises all actions happening after the authorization stage.

Data processed by the PoS can still be eavesdropped by having physical access to the PoS itself or by exploiting device vulnerabilities.

3.1 ATTACK METHODS:

There are many possible way to attack the PoS system. Following as the Pos Vulnerabilities:
Skimmers: PoS system is replaced with a fake one in order to capture customers card data.
Scrapers: A malware is installed within the PoS system in order to steal customers card data.
e.g RAM scraping malware.
And forced offline authorization ,software vulnerabilities. Three ways to analysed the attacks are
Data in memory , data in transit and data at rest.

Acronym	Meaning
APD	Avalanche photo diode
CRP	Challege response pair
EPS	Electronic Payment System
IC	Integrated system
PUF	Physical Unclonable Function
TTP	Trusted Third Parties

TABLE: Most relevant acronyms used in this paper.

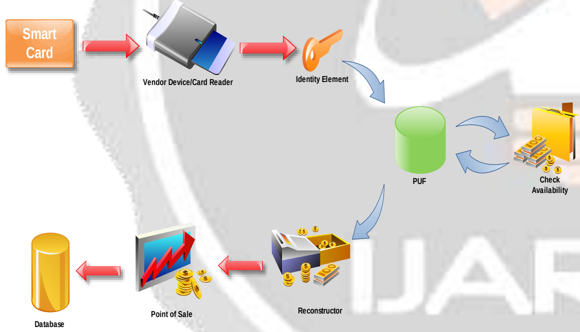
4 PROPOSED MODEL:

Frodo based on strong physical unclonable function. The Physical Unclonable function was introduced by Ravikanth in 2001.

FRoDo is the first solution that neither requires trusted third parties, nor ank accounts, nor trusted devices to provide resiliency against frauds based on data breaches in a fully offline electronic payment systems.

Digital coins used in FRoDo are just digital version of real cash and, as such, they are not linked to anybody else than the holder of both the identity and the coin element.

FRoDo assumes that only the chips built upon PUFs can take advantage from the tamper evidence features. A secure offline micropayment approach using multiple physical unclonable functions.



FRODO features an identity element to authenticate the customer, and a coin element where coins are not locally stored, but are computed on- the fly when needed. The communication protocol used for the payment transaction does not directly read customer coins. Identity element in order to identify the user.

The benefit is simpler, faster, and more secure interaction. It is a two steps protocol allows the coin element issuer to design digital coins to be read only by a certain identity element.

Identity element improve the security of users.

This is the first solution that can provide secure offline payments while being resilient to all known PoS breaches.

Identity Element:

-Key Generator: used to generate the private key.

-Cryptographic Element: used for symmetric and asymmetric cryptographic algorithms applied to data received in input and send as output by the coin element.

Coin Element:

-Coin Selector: selection of the right registers together with the output value computed by the coin element.

Coin Registers:

Used to store PUF input and output values.

-Coin Seed: it is the input to the PUF.

Erasable PUF:

Is a read once PUF.

Even if the same input is used , the ouput will be random.

Coin Reconstructor:

The output of the PUF together with coin helper data then the reconstruction process is performed.

Vendor coin request do not contain the erasable PUF challenge by themselves, but they are used as input to the coin selector. Selecting the coin registers.

Coin seed register is used as input to the erasable PUF coin helper data is combined with the PUF output is used to reconstruct the process.

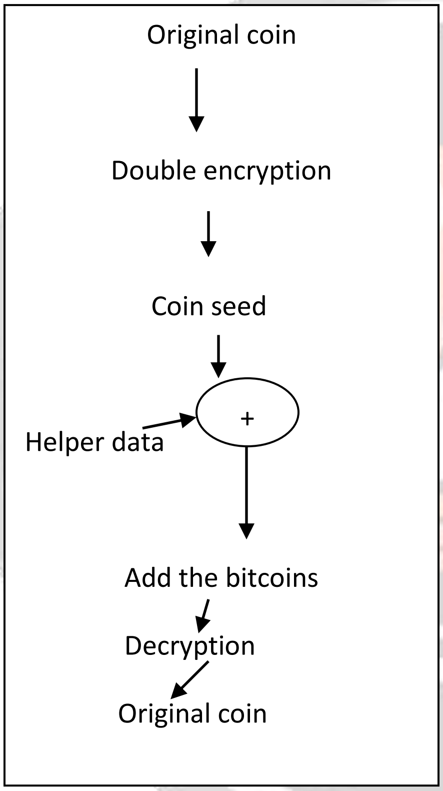


Fig: Coin Reconstruction

This figures depicts the reconstruction process of the payment processing.

Finally the user account will be transferred to the vendor account.

This is a way to perform the payment transaction process.

Each algorithm efficiency represented as the graphical diagram shown in the figure.

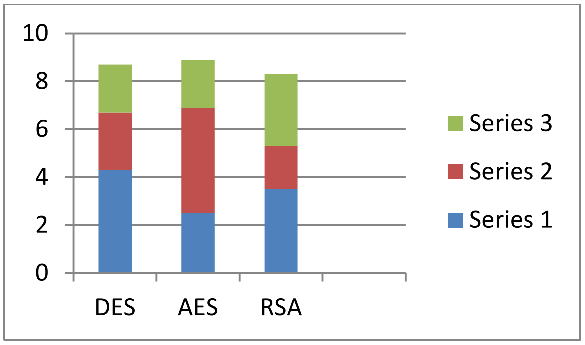


Fig: Algorithm efficiency

5 CONCLUSION:

The first data breach resilient fully offline micropayment approach. The security analysis shows that Frodo does not impose trustworthiness.

This has been achieved mainly by leveraging a novel erasable PUF architecture and a novel protocol design. Multiple off line transactions while maintaining the same level of security and usability.

Reference:

[1] V. Daza, R. Di Pietro, F. Lombardi, and M. Signorini, “FORCE Fully off-line secure credits for mobile micro payments,” in Proc. 11th Int. Conf. Security Cryptography, 2014, pp. 125–136.

[2] S. Gomzin, Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions, 1st ed. New York, NY, USA: Wiley, 2014.

[3] M.-D. Yu and S. Devadas, “Secure and robust error correction for physical unclonable functions,” IEEE Design Test Comput., vol. 27, no. 1, pp. 48–65, Jan. 2010.

[4] G. Hong and J. Bo, “Forensic analysis of skimming devices for credit fraud detection,” in Proc. 2nd IEEE Int. Conf. Inf. Financial Eng., Sep. 2010, pp. 542–546.

[5] W. Chen, G. Hancke, K. Mayes, Y. Lien, and J.-H. Chiu, “Using 3G network components to enable NFC mobile transactions and authentication,” in Proc. IEEE Int. Conf. Progress Informat. Comput., Dec. 2010, vol. 1, pp.

[6] Mandiant, “Beyond and breach,” Mandiant, Technical Report, 2014.

[7] Bogmar, “Secure POS & kiosk support,” Bogmar, Technical Report, 2014.

[8] C.Wang, H.Sun, H.Zhang, and Z.Jin, “An improved off-line electronic cash scheme,” in ICCIS 2013,June 2013,pp.438-441.

[9] M.A. Salama, N. El-Bendary, and A.E. Hassanien,”Towards secure mobile agent based e-cash system,” in Intl.Workshop on security and Privacy Preserving in e-societies. Newyork, NY, USA:ACM,2011, pp.1-6.

Mareeswari is doing B.E degree in computer science and engineering in Prince shri venkateshwara padmavathy Engineering college, Chennai. Her research interest include network security.

Gayathri.D is doing B.E degree in computer science and engineering in Prince shri venkateshwara padmavathy Engineering college, Chennai. Her research interest includes visual cryptography, information security.

Vanitha . D is a M.E. degree holder who is currently working as an assistant professor in computer science department at Prince Shri Venkateshwara padmavathy Engineering college, Chennai. Her research interest includes computer graphics, Data structures etc.

Kapila Vani. R. K. is a M.E graduate currently working as Assistant Professor in computer science department at Prince Dr.K vasudevan College of Engineering and Technology,Chennai. Her research interest includes compiler design, Theory of computation and Software project management.