International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 03 | Mar -2017 www.irjet.net p-ISSN: 2395-0072

Survey Paper on

FRoDO: Fraud Resilient Device for Off-Line Micro-Payments

Ms. Rakshitha K S[1], Priya J[2], Sandhya S[3], Thushara Kurup K R[4]

[1]*Assistant Professor,Dept of CS&E,SKIT,Karnataka,India*
[2] *Student, Dept of CS&E,SKIT,Karnataka,India*
[3] *Student, Dept of CS&E,SKIT,Karnataka,India*
[4] *Student, Dept of CS&E,SKIT,Karnataka,India*

Abstract - *Credit and debit card data thefts though were the earliest forms of cybercrime they are the most common cybercrimes. Attackers steal customer data by targeting the Point of Sale (for short PoS) system, i.e. the point at which a retailer first gets customer data. Modern PoS systems are computers equipped with a card reader and running specialized software to read the data. Increasingly user devices are being used as input to the PoS. In these scenarios, malware that can steal card data as soon as they are read by the device has been developed. In the cases where customer and vendor are persistently disconnected from the network, there is no secure on-line payment. The paper describes FRoDO, a secure off-line micro-payment solution that is resistant to PoS data breaches. This improves over up to date approaches in terms of flexibility and security. FRoDO is probably the first solution that can provide secure fully off-line payments while being resistant to all currently known PoS breaches. We have made a survey on the previous solutions that existed before FRoDO discovering their advantages and disadvantages. Later we detail FRoDO architecture and components.*

Key Words: **micro-payment**, **PUF**, **hash-chaining**, **genetic algorithm**, **fraud-resilience**.

1.INTRODUCTION

Market analysts have predicted that mobile payments will over-take the traditional market, in providing greater convenience to consumers and new sources of revenue to many companies. This scenario produces a shift in purchase methods from classic credit cards to new approaches such as mobile-based payments, giving new market players novel business chances. Broadly supported by recent hardware, mobile payment technology is still at its early stages of development but it is expected to rise in the near future as demonstrated by the growing interest in crypto-currencies. At the present time, crypto-currencies and decentralized payment systems (e.g. Bitcoin) are increasingly popular, nurturing a shift from physical to digital currencies. However, payment techniques are not yet commonplace, due to several unsolved issues, including a lack of widely-accepted standards, limited interoperability among systems and, most importantly, security.

Several retail organizations have been victims of information security breaches and payment data theft targeting consumer payment card data and Personally Identifiable Information

Although PoS ruptures are declining, they still remain an extremely fulfilling endeavor for criminals. Customer data can be used by cybercriminals for fraudulent operations, and this led the payment card industry security standards council to establish data security standards for all those organizations that handle credit, debit and ATM cardholder information. Irrespective of the structure of the electronic payment system, PoS systems always handle acute information and, often times, they also need remote management. PoS systems act as gateways and require some sort of network connection in order to contact external credit card processors. This is mandatory to authenticate transactions. However, larger businesses that wish to tie their PoS's with other back-end systems may connect the former to their own internal networks. In addition, to reduce the amount of cost and simplify administration and maintenance; PoS devices may be remotely managed over these internal networks. However, a network connection might not be available due to either a momentary network service interruption or due to a permanent lack of network coverage. Such on-line solutions are not very efficient since remote communication can introduce interruptions in the payment process. In this article, we propose FRoDO, a secure off-line **micro-payment** approach using multiple physical unclonable functions.

The main contributions of this article are:

- FRoDO features an identity element to validate the customer, and a coin element where coins which are computed on-the-fly when needed.
- The vendor only converses with the identity element in order to identify the user.
- The main advantage is a simpler, faster, and more secure interface between the involved actors/entities.
- The two-steps protocol allows the bank or the coin element issuer to design digital coins to be read only by a definite identity element, i.e. by a specific user.
- The identity element used to improve the security of
the users can also be used to impede malicious users.
- This is the first solution that can provide secure fully off-line payments while being robust to all currently known PoS breaches.

[1]: Towards an Internet of Trust Issues and Solutions for Identification and Authentication in the Internet of Things.

For online scenarios this paper proposed a solution based on the context and another one based on meta-data synchronization. However both can be improved as:

CONNECT: Context-aware approach makes it possible to detect sybil attackers when the majority of the network is not malevolent. However, when the majority of the surrounding things is malicious or when a device needs to be moved within a new network for which it does not have any information, context-aware approach might not work. Last but not least, CONNECT is now based on a two-step authentication protocol where the first step is manual whilst the second is self-directed. Using of a single step authentication protocol that completely removes the human factor should be included.

SUF: Our Software-based Unclonable Functions indicated to be able to bring hardware intrinsic security properties such as unclonability, tamper evidence and unpredictability to a software-based authentication protocol. However, it relies on a standard client-server model and assumes a universal and persistent attacker as practically unfeasible. The design of a distributed model where multiple clients and server can work together and where each client is assumed to be malicious should be considered for this. The identification and authentication solutions provided in this thesis improve over the state of the art and show how an Internet of Trust is possible. However, these solutions are not perfect and, since attackers get more powerful over time as their knowledge increase, the solutions still need some enhancements and other approaches have to be examined.

[2]: Offline Micropayments without Trusted Hardware.

The paper demonstrated a simple and, for some applications, practical scheme for offline micropayments without the overhead of either secure hardware or online transaction authorization. It represents a departure from the usual approach to designing such systems. This paper describes a platform that makes it possible to encode risk management rules for offline micropayment. However the paper does not throws light on the area of systems that generate and adapt these rules to actual operational conditions. Use of a **Genetic algorithm** to meet this short coming could have improved the effectiveness of the paper. The most important mechanism for limiting fraud and abuse is the transaction limit encoded in the credentials. The kinds of transactions permitted are determined according to the risk management strategy of the account issuer, and are designed to limit the usefulness to a thief of a compromised user's credentials and secrets. For example, an encoded strategy might permit the offline purchase of newspapers, but only a few copies from any given vendor. If a user's device is stolen, the thief would be able to buy only newspapers, and only as many as he can and vendors.

[3]: Implication of Secure Micropayment System Using Process Oriented Structural Design by Hash chaining in Mobile Network .

This paper describes using extra chains, it is able to initiate payments to the new node in the new network. The paper does not include in view of the trust and reputation management for providing more safe and more consistent operation in micropayments in wireless adhoc network.

The proposed system highlights a secure application for e-payment system in offline via wireless mobile adhoc network. The security of the application is governed by Simple Public Key Infrastructure. The development of chains of certificate allows a distribution of the payment system by delegates. The designed model prevents dual expenditure in offline communication. The proposed system shows a

flexible and robust solution for serviceability, security, and effectiveness in e-payment systems over wireless mobile adhoc network. The paper lacks design of security system based on specific attack on mobile adhoc network like DDoS or Wormhole attack, which is very common issue on pure mobile network deployment in larger scale.

[4]: PayWord, MicroMint and Micropayment two simple micropayment schemes.

PayWord's is based on credit based system foremost goals is to minimize communication with the broker. As an "off-line" structure, PayWord does not require the vendors to interact with Broker for every payment. The Vendor only needs to "clear" the payment once a day. The MicroMint based on debit based system in their security on the notion in which makes use of coin element ,the broker produces the coins then sells to user .the user uses these coins to pay to vendor for the purchases made by them. In this a hacker cannot break the hash function in a short period of time and the fact that they can trace the users who use these coins. As a result, the MicroMint scheme can prevent from counterfeit and double spending effectively.

[5]: The Hardware Intrinsic Security from Physically Unclonable Functions.

PUF consists of a physical object that is rigid to clone due to its exclusive micro-scale properties or nano-scale properties that originate from the manufacture process variations. It resists physical attacks by causing loss to structure when attempted to find the performance of structure. The concept of a physical unclonable function (**PUF**) forms the basic idea on which the proposal of our new key storage approach is built. Unclonability: **PUF**s are by definition very tough to clone. This means that it takes a lot of resources and a lot of time to make either a hardware clone, a mathematical model of the behavior of the structure, or a software program that can compute the response to a challenge in a sensible quantity of time. In summary, a radically new approach, hardware intrinsic security, is available today to prevent cloning of semiconductor products and preserve the returns of those companies. **PUF**s are used to spawn the intrinsic fingerprint intrinsic in each device which is combined with a inimitable activation code to produce the furtive key. No key is actually stored in hardware thus significantly raising the level of security available beyond unconventional methods.

2. SYSTEM DESIGN

Our system design follows the FRoDO chief architecture is composed of two main elements: an identity element and a coin element. The coin element can be any hardware constructed upon a physical unclonable function and it is used to read digital coins in a reliable way. The identity element has to be embedded into the customer device and it is used to tie a specific coin element to a specific device. This new design provides a two factor authentication to the customer. In fact, the relationship between a coin element and identity element prevents an attacker from stealing coin elements that belong to other users.

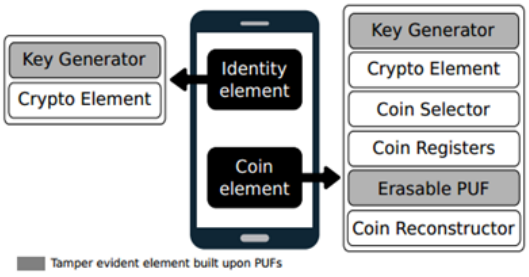

Fig -1: **FRoDO main architecture.**

Identity Element:

Identity element consists of Key Generator which is used to compute on-the-fly the private key of the identity element. It is Cryptographic Element used for symmetric and asymmetric cryptographic algorithms applied to data received in input and sent as output by the identity element.

Coin Element:

Coin element uses the Key Generator in which it is used to compute on-the-fly the private key of the coin element. It is also a Cryptographic Element which is used for symmetric and asymmetric cryptographic algorithms applied to data received in input and send as output by the coin element it consist of Coin Selector which is liable for the selection of the right registers used together with the output value computed by the coin element **PUF** in order to acquire the final coin value .It consists of Coin Registers: used to store both **PUF** input and output values required to recreate original coin values. Coin registers consists of coin seed and coin helper data. Coin seeds are used as input to the **PUF** whereas coin helpers are used in order to reconstruct stable coin values

when the **PUF** is challenged. The figure also contains of Erasable **PUF** is a read-once PUF After the first challenge, even if the same input is used, the output will be arbitrary, Coin Re-constructor is accountable to use the output imminent from the **PUF** together with a coin helper in order to reconstruct the actual value of the coin. The re-constructor uses helper data stored into coin registers to excerpt the original output from the **PUF**.

Key Generator:

The Key Generator element is used both within the identity element and within the coin element. The main concern of such an element is to compute on-the-fly the private key. Such keys are used by the cryptographic elements to decrypt the requests and encrypt the replies.

Erasable Coin:

At the core of FRoDO proposal lies a read-once strong physical unclonable function. Such **PUF**, used to compute on-the-fly each coin, has the property that reading one value terminates the original content by changing the behavior of the PUF that will respond with haphazard data in further challenges. Vendor's coin requests do not contain the erasable-PUF challenge by themselves, but they are used as input to the coin selector. This latter one has information about available funds for each register and it has the liability of selecting the coin registers (one or more) that will be involved in the transaction. The definite coin seed register is then used as input to the erasable PUF, while the coin helper register is united to the PUF output in order to recreate the absolute value of the coin.

3. CONCLUSIONS

In this paper we have presented FRoDO that is, the first data-breach-resilient fully off-line micropayment approach. The security analysis shows that FRoDO does not levy trustworthiness assumptions. Further, FRoDO is also the first solution in the literature where no customer device data outbreaks can be abused to compromise the system. This has been achieved mainly by leveraging a unique erasable PUF architecture and a novel protocol design. Additionally, our proposal has been systematically discussed and compared against the state of the art. Our analysis displays that FRoDO is the only proposal that enjoys all the properties essential to a secure **micro-payment** solution, while also introducing flexibility when allowing for the payment medium (types of digital coins). To conclude, some open concerns have been recognized that are left as future work. In particular, we are inspecting the probability to allow digital change to be spent over multiple off-line transactions while maintaining the same level of security and usability.

REFERENCES

[1] Daza, Vanesa; Di Pietro, Roberto "Towards an Internet of Trust Issues and Solutions for Identification and Authentication in the Internet of Things".

[2] M.Blaze, J.Feigenbaum, J.Ioannidis, and A.D.Keromytis. "Offline Micropayments without Trusted Hardware" *The Key Note Trust Management System Version 2.Internet RFC 2704, September 1999.*

[3] Zygmunt J. Haas, Jing Deng, Ben Liang, PanagiotisPapadimitratos, S. Sajama,"Wireless ad hoc Networks", "Implication of Secure Micropayment System Using Process Oriented Structural Design by Hash chaining in Mobile Network" *John Wiley & Sons, Inc, 2003*

[4] R.Rivest and A. Shamir. PayWord and MicroMint: Two simple Micropayment schemes. *May 7, 1996* "PayWord, MicroMint and Micropayment: two simple micropayment schemes

[5] C.Bssch, J. Guajardo, A.-R. Sadeghi, J. Shokrollahi, P.Tuyls, *in Efficient Helper Data Key Extractor on FPGAs. Proceedings of CHES 2008.*"Hardware Intrinsic Security from Physically Unclonable Functions"

BIOGRAPHIES

Assistant Professor,Dept of CS&E,SKIT,Karnataka,India

Student, Dept of CS&E,SKIT,Karnataka,India

Student, Dept of CS&E,SKIT,Karnataka,India

Student, Dept of CS&E,SKIT,Karnataka,India