IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

Secure Off-line Micro-payment Solutions on FRoDo

Abhilasha H K[1], Paramesha K[2]

PG Scholar, Department of CSE, Vidya Vardhaka College of Engineering, Mysuru, India[1]

Associate Professor, Department of CSE, Vidya Vardhaka College of Engineering, Mysuru, India[2]

Abstract: Online shopping Payment scheme is one of the popular in recent years. Attackers often aim at stealing such customer data by targeting the Point of Sale (for short, PoS) system, i.e. the point at which a retailer first acquires customer data. In many scenarios malware that can steal card data as soon as they are read by the device has flourished. As such, in cases where customer and vendor are persistently or intermittently disconnected from the network, no secure on-line payment is possible. This paper describes FRoDO, a secure off-line micro-payment solution that is resilient to PoS data breaches. FRoDO is the first solution that can provide secure fully off-line payments while being resilient to all currently known PoS breaches.

Keywords: Fraud resilience, secure payments, PoS system, Architecture.

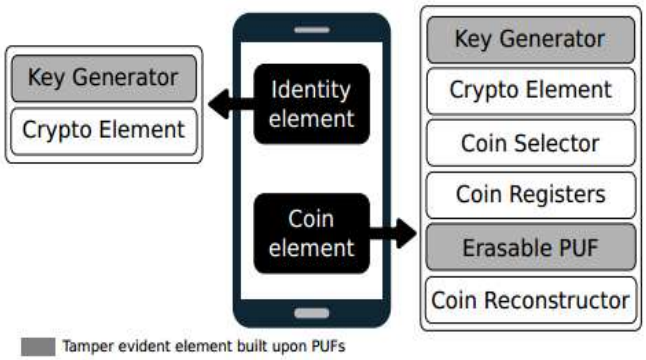
I. INTRODUCTION

Network security consists of the policies and practices adopted to prevent and monitor access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator.
Users choose or assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals.

Mobile micro payments are famous and they are traditional in marketing fields. The classic credit card approaches may be implemented in banking such as mobile-based payments. Even though many technologies developed, many unexpected problems faced in the field for that the crypt-currencies and de-centralized payment systems are used.

The first pioneering micro-payment scheme was proposed by Rivest and Shamir in 1996. Due to several unresolved problems, including a lack of widely-accepted standards, limited interoperability among systems and security the payment schemes are not get successful in the payment system.

II. FRODO: THE ARCHITECTURE



As depicted in Figure, the architecture of FRoDO is composed of two main elements: an identity element and a coin element. The coin element can be any hardware built upon a physical unclonable function (such as an SD card or a USB drive) and it is used to read digital coins in a trusted way. The identity element has to be embedded into the customer device (such as a secure element) and it is used to tie a specific coin element to a specific device.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

This new design provides a two factor authentication to the customer. In fact, the relationship between a coin element and an identity element prevents an attacker from stealing coin elements that belong to other users. A specific coin element can be read only by a specific identity element (i.e. by a specific device).

Furthermore, this approach still provides anonymous transactions as each identity element is tied to a device and not to a user.

The whole FRoDO architecture can be decomposed as follows:

- **Identity Element**:

– Key Generator: used to compute on-the-fly the private key of the identity element;
– 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:**

– Key Generator: used to compute on-the-fly the private key of the coin element;
– Cryptographic Element: used for symmetric and asymmetric cryptographic algorithms applied to data received in input and send as output by the coin element;
– Coin Selector: is responsible for the selection of the right registers used together with the output value computed by the coin element PUF in order to obtain the final coin value;
– Coin Registers: used to store both PUF input and output values required to reconstruct original coin values. Coin registers contain coin seed and coin helper data. Coin seeds are used as input to the PUF whilst coin helpers are used in order to reconstruct stable coin values when the PUF is challenged;
– Erasable PUF: is a read-once PUF. After the first challenge, even if the same input is used, the output will be random;
– Coin Reconstruction: responsible to use the output coming from the PUF together with a coin helper in order to reconstruct the original value of the coin. The reconstruction uses helper data stored into coin registers to extract the original output from the PUF.

III. FRODO PROTOCOL

- **Pairing Phase**

FRoDO relies on pairing protocol such as Bluetooth Passkey pairing process. The customer and vendor device will share the public key used for message integrity and authenticity.

- **Payment Phase**

FRoDO 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.

IV. SECURITY ANALYSIS

• **Authenticity:** For authentication process, FRoDO 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.

• **Non-denial:** By deleting past transactions and keep the storage device physically safe. The content of storage device is backed up and exported to secondary devices.

• **Confidential:** To achieve confidentiality, communication between customer and vendor message is encrypted.

V. ATTACK MITIGATION

To improve the security of whole payment system two different elements will be using by FRoDO. They are coin element and identity element. The vendor device does not directly communicate with the coin element but has to go through the identity element.

On the other hand, the identity element can be used to fight against attackers, if an identity element is considered as malicious and is blacklisted, the device used by user, any coin will not be accepted and processed by the vendor.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

VI. CONCLUSION

FRODO introduces off-line micro payment approach for data-breaches. FRoDO is highly secure micropayment solution and also introducing flexibility in payment medium. To improve the level of security and usability multiple off-line transaction are allowed in the transaction. The current off-line solution adopt a withdrawal-phase producing tokens which are recomputed and pre-cached within a device. Thus FRoDO is secure and flexible for consumer.

REFERENCES

[1] V. Daza and R. Di Pietro, "FORCE -Fully Off-line secuReCrEdits for Mobile Micro Payments," in SCITEPRESS, 2014.
[2] W. Whitteker, "Point of Sale (POS) System and Security," SANS Institute InfoSec Reading Room, 2014.
[3] U. Rhrmair and C. Jaeger,"An attack on PUF-Based Exchange and a Hardware-based Countermeasure:Erasable PUFs," in LNCS 2012.
[4] B. Kori and P. Tuyls, "Robust key extraction from physical uncloneable functions," in Applied Cryptography and Security, 2005.
[5] G. Van Damme and H. Karahan, "Offline NFC Payments with Electronic Vouchers," in MobiHeld, 2009.
[6] Yalin Chen and Jue Sam Chou, "User Efficient Recoverable Off-line E-cash Scheme with Fast Anonymity revoking," in International Journal of Network Security, 2015.
[7] DebasisGiri and ArpitaMazumdar, "A Secure Offline Electronic Payment System Based on Bilinear Pairings and Signcryption,"in IJSCE, 2013.