Analysis on a Payment System Using FRODO

Sheela B.P[1], Sreepathi[2], Shilpa pati[3], Priyanka Deshpande[4]
[1]*Assistant professor, Dept. of ISE, RYMEC/Ballari*
[2]*HOD, Dept. of ISE, RYMEC/Ballari*
[3,4]*Student, Dept. of ISE, RYMEC/Ballari*

Abstract- **A micropayment scheme is designed for providing efficient and secure solution for online payment ecosystems. Micropayment applications have turns to be general usage in electronic payment due to the fasted development of the Internet and the improving sophistication of electronic commerce. It is specifically designed for the customer to make the safe payment. Assaulters commonly aim to stealing the customer data by using the Point of Sale
i.e. the point at which a retail first gathers customer information. During the payment, in cases of network failure, attacker's side to steal the password from the customers so there may be no secure transaction On-line payment is possible. In our paper, we propose secure and privacy off-line micro-payment solution for the resilient attackers due to the PoS data breaches. We utilize the FRoDO protocol to make the secure and safe payment against attackers which not only analyze the customers coins but also verify the identity of the customer using identify element which enhances flexibility and security and improves the effectiveness of the system by providing the secure micro-payment between the customers and vendors.**

Index Terms- **Micropayment Scheme, Point of Sale, resilient attackers, FRoDO protocol, and secure micro-payment.**

1. INTRODUCTION

Credit and debit card data theft is one form of cybercrime. Attackers often aim at stealing such as customer data by targeting the Point of Sale system, where retailer first gets the customer data. Modern POS systems are equipped with a card reader and specialized software. User details are given as input to the POS. In this malware steals card data as soon as they are read by the device. Until the customer and vendor are disconnected from the network, no secure on-line payment is possible. It describes a secure off-line micropayment solution that is resilient to POS data stealing. FRODO Provides secure fully off-line payments.

The main objective of the Frodo system is to encrypt user's sensitive data when users payment processing takes place. This will ensure that the third party pos vendors or merchants can't able to see user's personal data like card no cvv number etc. This will be only visible to bank admin where they either accept or deny the payments.

Computer security (Also known as cyber security or IT Security) is information security as applied to computers and networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters. Otherwise, in the computer industry, the term security or the phrase computer security refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorize at ion. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

2. RELATED RESEARCH

- Payword and micromint: two simple micropayment schemes

Author: r. L. Rivest

The Basic Pepper coin method can be implemented in a variety of ways, to maximize ease of use for the customer in a given situation. While the basic peppercoin method requires that each consumer have digital signature capability, one can easily eliminate this requirement by having a party trusted by the consumer sign payments for him as a proxy, this might be a natural approach in a web services enivornment.

The pepper coin method can also be implemented so that it feels to the consumer as a natural extension of his existing credit-card processing procedure, further increasing consumer acceptance and ease of use.

- SECURE POS & KIOSK

Author: Bomgar

Limited interfaces and location within local networks, supporting kiosks and point of sale (POS) terminals can be challenging. Often they are located on networks that are not connected to the internet, making direct access impossible for most remote support tools. And even when an employee is present at the terminal, access restrictions and/or lack of technical knowledge

makes communicating the solution to a problem difficult. To add complications, hackers are ramping up their efforts to steal payment card data by gaining access to POS systems and kiosks.

- Reliable OSPM schema for secure transaction using mobile agent in micropayment system

Author: Nc Kiran

The paper introduces a novel offline payment system in mobile commerce using the case study of micro-payments. The present paper is an extension version of our prior study addressing on implication of secure micropayment system deploying process oriented structural design in mobile network. The previous system has broad utilization of SPKI and hash chaining to furnish reliable and secure offline transaction in mobile commerce.

However, the current work has attempted to provide much more light weight secure offline payment system in micro-payments by designing a new schema termed as Offline Secure Payment in Mobile Commerce (OSPM). The empirical operation are carried out on three types of transaction process considering maximum scenario of real time offline cases. Therefore, the current idea introduces two new parameters i.e. mobile agent and mobile token that can ensure better security and comparatively less network overhead.

3. ANALYSIS

3.1.1 EXISTING 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.
- ❖ Mobile payment solutions proposed so far can be classified as fully on-line, semi off-line, weak off-line or fully off-line.
- ❖ The previous work called FORCE that, similarly to FRoDO, was built using a PUF based architecture. FORCE provided a weak prevention strategy based on data obfuscation and did not address the most relevant attacks aimed at threatening customer sensitive data, thus being vulnerable to many advanced attack techniques

Disadvantages of Existing System:

- ❖ Off-line scenarios are harder to protect, customer data is kept within the PoS for much longer time, thus being more exposed to attackers.
- ❖ Skimmers: in this attack, the customer input device that belongs to the PoS system is replaced with a fake one in order to capture customer's card data.
- ❖ The main issue with a fully off-line approach is the difficulty of checking the trustworthiness of a transaction without a trusted third party. In fact, keeping track of past transactions with no available connection to external parties or shared databases can be quite difficult, as it is difficult for a vendor to check if some digital coins have already been spent. This is the main reason why during last few years, many different approaches have been proposed to provide a reliable off-line payment scheme.
- ❖ Although many works have been published, they all focused on transaction anonymity and coin unforgeability. However, previous solutions lack a thorough security analysis. While they focus on theoretical attacks, discussion on real world attacks such as skimmers, scrapers and data vulnerabilities is missing.

3.1.2 PROPOSED SYSTEM:

- ❖ In this Frodo system , FRoDO is the first solution that neither requires trusted third parties, nor bank accounts, nor trusted devices to provide resiliency against frauds based on data breaches in a fully off-line electronic payment systems. Furthermore, by allowing FRoDO customers to be free from having a bank account, makes it also particularly interesting as regards to privacy.

- In fact, digital coins used in FRoDO are just a 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.
- Differently from other payment solutions based on tamper-proof hardware, FRoDO assumes that only the chips built upon PUFs can take advantage from the tamper evidence feature. As a consequence, our assumptions are much less restrictive than other approaches.
- This Frodo system introduces and discusses FRoDO, a secure off-line micro-payment approach using multiple physical unclonable functions (PUFs).
- 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. Instead, the vendor only communicates with the identity element in order to identify the user. This simplification alleviates the communication burden with the coin element that affected previous approach.
- The main benefit is a simpler, faster, and more secure interaction between the involved actors/entities. Among other properties, this two-steps protocol allows the bank or the coin element issuer to design digital coins to be read only by a certain identity element, i.e., by a specific user. Furthermore, the identity element used to improve the security of the users can also be used to thwart malicious users.
- To the best of our knowledge, this is the first solution that can provide secure fully off-line payments while being resilient to all currently known PoS breaches.

ADVANTAGES OF PROPOSED SYSTEM:

- FRoDO has been designed to be a secure and reliable encapsulation scheme of digital coins.
- FRoDO also applicable to multiple-bank scenarios. Indeed, as for credit and debit cards where trusted third parties (for short, TTPs) such as card issuers guarantee the validity of the cards, some common standard convention can be used in FRoDO to make banks able to produce and sell their own coin element.
- The identity and the coin element can be considered tamper-proof devices with a secure storage and execution environment for sensitive data.

4. SYSTEM ARCHITECTURE

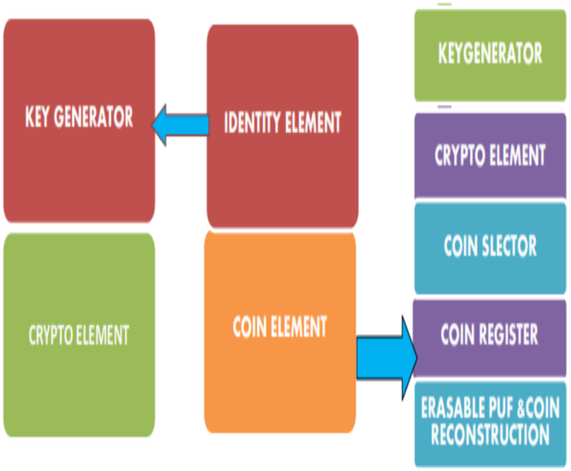

Fig : Frodo System Architechture

The forodo sytem architechture describes following modules:

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 valueswhen 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 reconstructor 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 onthe-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.

3.1 frodo classes

The frodo system has 4 main classes as shown in Fig2 a user class, a vendor class ,Frodo class and a puf class. The fgi2 represents , a class diagram in the Unified Modeling Language (UML) which is a type of static structure diagram that describes the structure of a Frodo system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes.

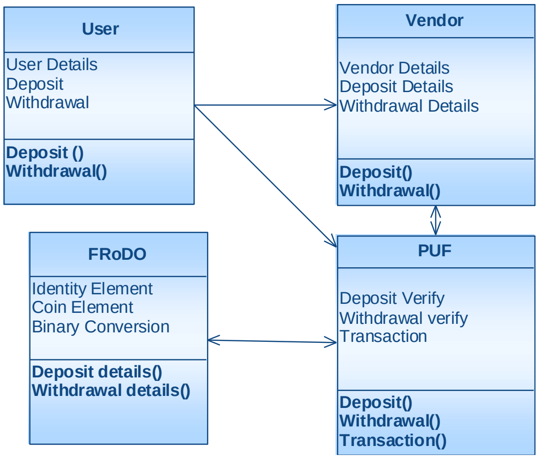

Fig 2: Frodo Classes.

5.CONCLUSIONS

In this project we have introduced FRODO that is, to the best of our knowledge, the firs t data-breach-resilient fully offline micro-payment approach. The security analysis shows that FRODO does not impose trustworthiness assumptions. Further, FRODO is als o the firs t s olution in the literature where no cus tomer device data attacks can be exploited to compromise the system. This has been achieved mainly by leveraging a novel erasable PUF architecture and a novel protocol design. furthermore, our proposal has been thoroughly discussed and compared against the state of the art. Our analysis shows that FRODO is the only proposal that enjoys all the properties required to a secure micro- payment solution, while a ls o introducing flexibility when considering the payment medium (types of digital coins). Finally, some open issues have been identified that are left as future work. In particular, we are investigating the possibility 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"