Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 7, Issue. 5, May 2018, pg.70 – 75

Fraud Resilient Software for Offline Micro-Payments

Syeda Gazala Rizvi[1], Noor E Amreen[2], Kavana L[3], Ranjini M.R[4], H.V. Shashidhara[5]
[1]Department of Computer Science & Engineering VTU, India
[2]Department of Computer Science & Engineering VTU, India
[3]Department of Computer Science & Engineering VTU, India
[4]Department of Computer Science & Engineering VTU, India
[5]Department of Computer Science & Engineering VTU, India
[1] gazalarizvi96@gmail.com; [2] nooreamreen05@gmail.com; [3] lkavana12@gmail.com;
[4] ranjinimourya13@gmail.com; [5] hvs@mcehassan.ac.in

Abstract— ***One fundamental issue with today's Online Payment System is increased Cybercrime. Where Attackers aim at stealing customer confidential data by targeting the Point of Sale (POS) systems, i.e., the point at which a bankers or retailer first acquires customer data. Modern POS systems are powerful computers equipped with a card reader and running specialized software. In this scenario a Malicious Software (MS) can be used by the attacker to steal card data. As such, in case where customer and vendor are persistently disconnected from the network, no secure online payment is possible. To overcome from these attacks, in this paper, we describe Fraud Resilient Software for Offline Micro-Payment that is a Secure Offline Micro-payment solution which is resilient to POS Data Breaches in terms of both flexibility and security. To the best of our knowledge, this is the first solution that can provide secure fully offline payments while being resilient to all currently known POS Breaches.***

Keywords— ***POS, MS***

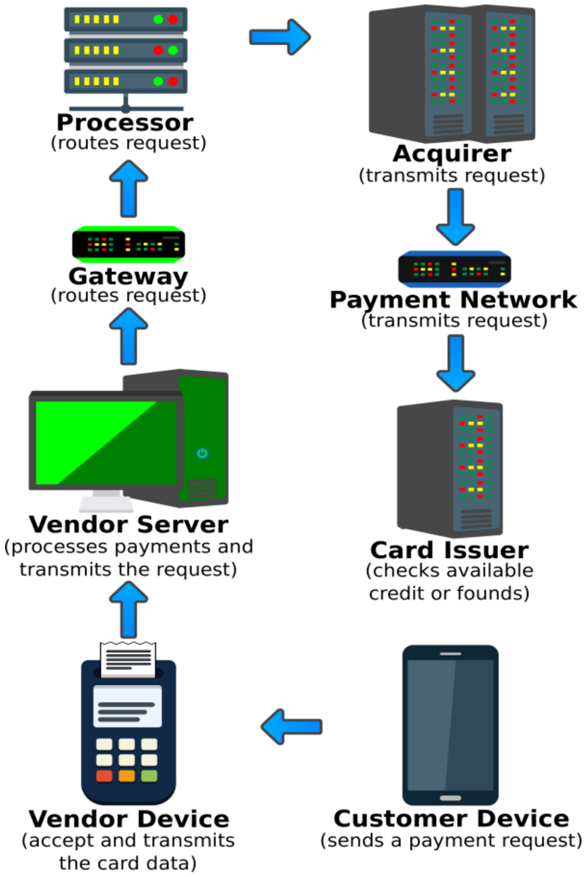
I. Introduction

Market analysts have predicted that mobile payments will overtake the traditional marketplace, thus 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 entrants novel business chances. Widely supported by recent hardware, mobile payment technology is still at its early stages of evolution but it is expected to rise in the near future as demonstrated by the growing interest in crypto-currencies. The first pioneering micro-payment scheme was proposed by Rivets and Shamir (see Pay word [1]) back in 1996. Nowadays, crypto-currencies and decentralized payment systems (e.g. .Bit coin) are increasingly popular, fostering a shift from physical to digital currencies. However, such payment techniques are not yet commonplace, due to several unresolved issues, including a lack of widely-accepted standards, limited interoperability among systems and, most importantly, security.

Over the last years, several retail organizations have been victims of information security breaches and payment data theft targeting consumer payment card data and Personally Identifiable Information (PII).

Although POS breaches are declining, they still remain an extremely lucrative endeavour 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. Regardless of the structure of the electronic payment system, POS systems always handle critical information and, oftentimes, they also require remote management.

Figure 1: Payment Authorization Stages



Usually, as depicted in Figure 1, 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. However, larger businesses that wish to tie their POS 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. However, a network connection might not be available due to either a temporary network service disruption or due to a permanent lack of network coverage. Last, but not least, such on-line solutions are not very efficient since remote communication can introduce delays in the payment process.

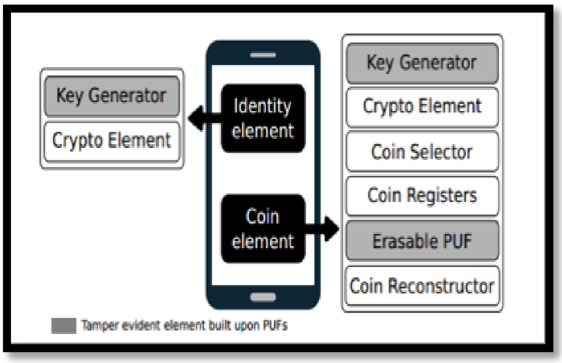
Most POS attacks can be attributed to organized criminal groups. Brute forcing remote access connections and using stolen credentials remain the primary vectors for POS intrusions. However, recent developments show the resurgence of RAM scraping malware. Such attacks, once such malware is installed on a POS terminal, can monitor the system and look for transaction data in plain-text, i.e. before it is encrypted.

II. Literature Survey

In the paper, “Pay word and micro mint: two simple micropayment schemes [2]” the author describes that the goal is to minimize the number of public key operation required per payment, using hash operations instead whenever possible. As a rough guide, hash functions are about 100 times faster than RSA signature verification, and about 10,000 times faster than RSA signature generation: on a typical workstation, one can sign two messages per second, verify 200 signatures per second, and compute 20,000 hash function values per second. To support micropayments exceptional efficiency is required; otherwise the cost of the mechanism will exceed the value of the payments.

In the paper, "2014 data breach investigations report [3]" the author describes about a drive for change is three-fold: first, we realized that the vast majority of incidents could be placed into one of nine patterns: second, we can (and did) draw a correlation between these patterns and industries: and third, we wanted challenge ourselves to look at the data with a fresh perspective. The ultimate goal is to provide actionable information presented in a way that enables you to hash out the findings and recommendations more relevant to your organization.

In the paper "Point-of-Sale system breaches [4]" the author describes about a Point-of-sale (POS) systems have been around in one form or another for decades. Businesses in the retail and hospitality industries use these systems not only to accept payment, but to provide other operational information such as accounting, sales tracking and inventory management. These systems are also used to improve the customer experience through customer loyalty programs and suggestions POS systems require some sort of connection to a network in order to contact external credit card processors. This is necessary in order to validate credit card transactions.



III. System Architecture

The architecture of Fraud Resilient Software for Offline Micro-Payments 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. 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.

IV. Implementation

Fraud Resilient Software for Offline Micro-Payment is the solution that does not requires trusted third parties, bank accounts, trusted devices to provide resiliency against frauds based on data breaches in a fully off-line electronic payment systems. By allowing Fraud Resilient Software customers to be free from having a bank account, makes it also particularly interesting as regards to privacy. The digital coins used in Fraud resilient software 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 tamperproof hardware, Fraud Resilient Software 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. Fraud resilient software can be applied to any scenario composed of a payer/customer device and a payee/vendor device. All involved devices can be tweaked by an attacker and are considered not trustworthy except from a storage device, that we assume is kept physically secure by the vendor. Furthermore, it is important to highlight that Fraud resilient software has been designed to be a secure and reliable encapsulation scheme of digital coins.

MODULES USED

A. Key Generator

The key generator element is used within the identity element and within the coin element. The main purpose 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. PUFs have been used in Fraud resilient software to implement strong challenge-response authentication. In particular, multiple physical unclonable functions are used to authenticate both the identity element and the coin element to allow them to interact in a secure way. In order to compute each private key, a publicly known ID (respectively the identity element ID and the coin element ID) is used as input to the PUF.

B. Erasable Coins

PUF, used to compute on-the-fly each coin, has the property that reading one value destroys the original content by changing the behavior of the PUF that will response with random data in further challenges.

C. The Protocol

This describes the payment protocol that is being used in Fraud Resilient Software. For completeness purpose, the Transaction Dispute and the Redemption phases will be introduced in this section.

D. Pairing Phase

Fraud Resilient Software for Offline Micro-Payment relies on standard pairing protocols such as the Bluetooth passkey entry simple pairing process . At the end of the pairing protocol, both the customer and vendor devices will share their public keys that will be used for message integrity and authenticity.

E. Payment Phase

Fraud Resilient Software's payment protocol is described in two different points of view. First one from messages exchanged between the vendor and the customer device will be described. Then, from the second one customer device internal messages exchanged between the identity element and the coin element will be described.

F. Transaction Dispute

Due to its fully off-line nature, Fraud resilient software does not provide any transaction dispute protocol. To prevent off-line disputes by altering past transaction, direct off-line disputes between vendors and customers are avoided.

V. Result Analysis

The Performance Analysis is generated to check whether the data is transmitted between the Client and Server in an error free manner i.e. between vendor and receiver. It can also avoid the data loss during the transmission. So the client can make use of data in an efficient manner. Fraud Resilient Software for Offline Micro-Payment has been designed to be a secure and reliable encapsulation Scheme of digital coins.

This paper describes Fraud Resilient Software for Offline Micro-Payment a secure off-line micro-payment solution that is resilient to POS data breaches. Our solution improves over up to date approaches in terms of flexibility and security. To the best of our knowledge, Fraud Resilient Software for Offline Micro-Payment is the first solution that can provide secure fully off-line payments while being resilient to all currently known POS breaches.

As we discussed off-line POS are attacked to steal customer data. Device that are belonging to POS system are kept secure. Attacks against POS system in mature environment are multi staged, further as the scenario is fully off-line, there no connection to outside world, therefore the stolen data as to be kept hidden within the POS system.

VI. Conclusion

We have presented Fraud Resilient software for offline that is, to the best of our insight, the primary information rupture strong completely disconnected micropayments approach. The security investigation demonstrates that Fraud Resilient Software for Offline Micro-Payment does not force dependability suppositions. Further, Fraud Resilient Software for Offline Micro-Payment is likewise the principal arrangement in the writing where no client gadget information assaults can be misused to bargain the framework. This has been accomplished fundamentally by utilizing a novel erasable PUF engineering and a novel convention outline. Moreover, our proposition has been altogether talked about and looked at against the cutting edge. Our examination demonstrates that Fraud Resilient Software for Offline Micro-Payment is the main recommendation that appreciates every one of the properties required to a protected miniaturized scale installment arrangement, while likewise presenting adaptability while thinking about the installment medium (sorts of computerized coins). At last, some open issues have been distinguished that are left as future work. Specifically, we are exploring the likelihood to enable computerized change to be spent over various disconnected exchanges while keeping up a similar level of security and convenience.

A. Drawbacks of Existing System

Disconnected situations are harder to secure, client information is kept inside the POS for any longer time, along these lines being more presented to aggressors. Skimmers: in this assault, the client input gadget that has a place with the POS framework is supplanted with a phony one to catch client's card information. The primary issue with a completely disconnected approach is the trouble of checking the reliability of an exchange without a trusted outsider. Indeed, monitoring past exchanges with no accessible association with outer gatherings or shared databases can be very troublesome, as it is troublesome for a merchant to check if some advanced coins have just been spent. This is the fundamental motivation behind why amid most recent couple of years, a wide range of methodologies have been proposed to give a solid disconnected installment plot. Albeit numerous works have been distributed, they all centered around exchange secrecy and coin unforgetability. Nonetheless, past arrangement slack an intensive security investigation. While they center around hypothetical assaults, dialog on certifiable assaults, for example, skimmers, scrubbers and information vulnerabilities is absent.

B. Future Enhancement

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]. Vanesa Daza, Roberto Di Pietro, Flavio Lombardi, And Matteo Signorini “Frodo: Fraud Resilient Device For OffLine micro-Payments”, Dependable And Secure Computing, IEEE Transactions On (Volume: PP , Issue: 99), 12 June 2015.

[2]. R. L. Rivest, “Pay word and micro mint: two simple micropayment schemes,” in CryptoBytes, 1996, pp. 69–87.

[3]. W. Chen,G. Hancke,K. Mayes,Y. Lien, and J.-H. Chiu,“Using 3G network components to enable NFC mobile transactions and authentication,” in IEEE PIC ’10, vol. 1, Dec 2010, pp. 441 –448.

[4]. T. Nishide and K. Sakurai, “Security of offline anonymous electronic cash systems against insider attacks by untrusted authorities revisited,”ser. INCOS’11.Washington, DC, USA: IEEE Comp. Soc., 2011, pp.656–661.

[5]. 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. New York, NY, USA: ACM, 2011, pp. 1–6.

[6]. J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, “FPGA intrinsic PUFs and their use for IP protection,” ser. CHES ’07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 63–80.

[7]. S. Gomzin, Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions, 1st ed. Wiley Publishing, 2014.

[8]. Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” SIAM J.Compute, vol. 38, no. 1, pp. 97–139, mar 2008.

[9]. B. Kori, P. Tuyls, and W. Ophey, “Robust key extraction from physical unclonable functions,” in Applied Cryptography and Network Security, ser. LNCS, J. Ioannidis, A. Keromytis, and M. Yung, Eds. Springer Berlin Heidelberg, 2005, vol. 3531, pp. 407–422.

[10]. M.-D. Yu, D. M. Raihi, R. Sowell, and S. Devadas, “Lightweight and Secure PUF Key Storage Using Limits of Machine Learning,” in CHES 2011, ser. LNCS, B. Preneel and T. Takagi, Eds. Springer Berlin Heidelberg, 2011, vol. 6917, pp. 358–373.