Proceedings of National Conference on Computing & Information Technology (NCCIT-2017)

International Journal for Modern Trends in Science and Technology
Volume: 03, Special Issue No: 02, March 2017
ISSN: 2455-3778
http://www.ijmtst.com

Fraud Resilient Mechanism for Micro Payments at Point of Sales

Priyusha.B[1] | Bharani.Y[2] | Durga Bhavani.Ch[3] | B.Venu Gopal[4]

[1,2,3,4]Department of IT, Andhra Loyola Institute of Engineering & Technology, Vijayawada, Andhra Pradesh, India.

To Cite this Article
Priyusha.B, Bharani.Y, Durga Bhavani.Ch and B.Venu Gopal, "Fraud Resilient Mechanism for Micro Payments at Point of Sales ", *International Journal for Modern Trends in Science and Technology*, Vol. 03, Special Issue 02, 2017, pp. 32-38.

ABSTRACT

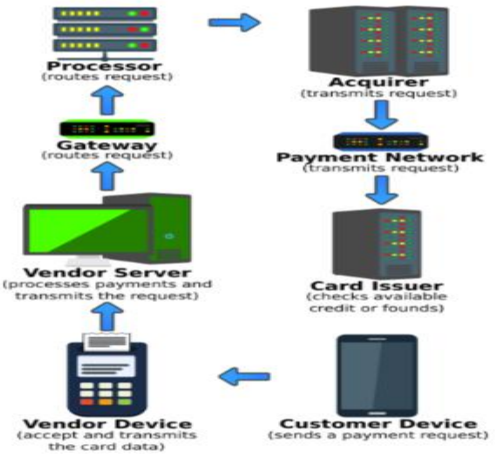
Cybercrimes which are most common nowadays which includes earliest forms of credit card and debit card theft. Point of sale (PoS) is the place where the attackers often aim at steal such customer data by targeting it. This scenario produces a shift in purchase method from classic credit cards to new approches such as device-based payments. Nowadays, crypto-currencies and decentralized payment system are increasingly popular, fostering a shift from physical to digital currencies. However, such payment techniques are not common place, due to several unresolved issues, including a lack of widely accepted standards, limited interoperability among systems and, most importantly, security. To the best of our knowledge, Fraud Resilient Mechanism For Micro-Payments at Point of sale is the first solution that can provide secure fully off-line payments while being resilient to all currently known PoS breaches. Our solution improves over up to date approaches in terms of flexibility and security.

KEYWORDS: *interoperability, micropayments, crypto-currencies, architecture, Fraud resilient, point of sales(pos).*

I. Introduction

PoS systems are acting like a gateways, in order to contact external credit card processors they require some sort of network connection. This is mandatory to validate transactions. To reduce cost of administration and maintenance, PoS devices are managed remotely 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.

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 Rivest and Shamir back in 1996. Nowadays, crypto-currencies and decentralized payment systems are increasingly popular, fostering a shift from physical to digital currencies.



1.1 Contribution

This paper introduces and discusses Fraud Resilient Mechanism for Micro-payments at point of sales, a secure off-line micro-payment approach using multiple physical unclonable functions. This features an identity element to authenticate the customer, and a coin element where coins are not locally stored, which are only 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 user identification. This simplification is to communication burden with the coin element that affected our previous approach. The main benefit is a simpler, faster, and more secure interaction will be seen between the involved actors/entities. Among properties, this two-steps protocol allows the bank or the coin element issuer to design digital coins to be read only by a certain specific user. Furthermore, the identity element used to improve the security of the users can also be used to malicious users. To the best of our knowledge, this is the most accurate solution that can provide secure fully off-line payments while being resilient to all currently known PoS breaches.

1.2 Fraud Resilient Mechanism for micro-payments at Point of sales

"Here we propose the 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. Nowadays, crypto-currencies and decentralized payment systems 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".

1.3 Secure Payment Solutions Fully Off-Line Functions on Fraud Resilient Mechanism

In this survey says nowadays online payments are one of the most popular, when the customer or buyer makes his payment transactions for the goods purchased with the use of the online money payment. In that the purchase methods from classic credit or debit cards to new approaches like mobile- based payments, giving new market entrant's novel business probabilities.

However, many of us still resist the attractiveness and ease of revolving credit transactions because of security issues. So far there are a high risk for taken cards fraud so the purchasers worry debit-card fraud by merchants and different third parties. Payment transactions are usually processed by an electronic payment system (for short, EPS). The EPS is a separate function from the typical point of sale function, although the EPS and PoS system may be co-located on constant machine.

1.4 Offline Micropayments without Trusted Hardware

Current electronic payment systems are not well matched to occasional, low-valued transactions. (For the purposes of this discussion, we use the term "electronic payment system" broadly, to encompass conventional credit cards, stored-value cards, online and offline digital cash, etc.) A central requirement for any electronic payment system is that a single compromise or failure should not have catastrophic consequences. For example, it should not be possible to double spend in a digital cash system, nor should the compromise of a client's authorization secret entail unlimited client liability or uncollectible transactions. Traditional payment systems are designed to prevent such failures. Unfortunately, the prevention mechanisms are generally too expensive to support occasional, low-valued transactions. Typically, such systems require online transactions, trusted client hardware such as smartcards, or must assume conditions that are not always true, such as that payers can be held responsible for any and all fraud or misuse of their authorization secrets. In this paper, however, we present a new approach that focuses instead on risk management. Our central observation is that in some applications we can relax many of the expensive requirements associated with electronic payment systems while still keeping fraud or uncollectible transactions within acceptable levels.

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. 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.

II. THREAT MODELS

Table 1 depicts the most relevant attacks and attacker models that have been analyzed in this work. As such, it shows both the attacks that can be unleashed against the customer device or the transaction protocol, and the attacks aimed at threaten customer sensitive data. Based on the capabilities and on the amount of devices that can be accessed during the attack, a taxonomy of the attackers is first introduced as follows:

- **Collector:** This is an external attacker able to eavesdrop and alter messages being exchanged between the customer and the vendor device.
- **Malicious Customer:** (M. Customer) this is an internal attacker that can either physically open the customer device to eavesdrop sensitive information or inject malicious code within the customer device in order to alter its behavior.
- **Malicious Vendor:** (M. Vendor) It is an internal attacker that can either eavesdrop information from the vendor device or inject malicious code in it in order to alter its behavior.
- **Ubiquitous:** This is an internal attacker with complete access to all the involved devices.

In Fraud Resilient Mechanism for Micro-payments at point of sale has no restrictions made on the capabilities of the attacker that is always considered as ubiquitous.

Keywords: Collectors, Malicious Customer, Malicious Vendor, Ubiquitous, Eavesdrop.

III. ATTACK METHODS

Only a subset of the attacks listed in Table 1 represents real dangers in a fully off-line scenario. In fact, in such a scenario only vendor and customer devices are involved in the transaction and no connection to the external world is provided. In Figure 3 a general picture of all possible PoS system threats is given. It is clear from the picture that, no matter what the environment and the architectural design of the EPS are (boxes 1, 2 and 3), customer data needs at some point to be sent back to the bank or to the coin element issuer. This means that the data read from the customer's card can be stolen within the card reader (label A), within the cash register or back office server (label D), while in transit between the devices (label B) or while in transit to the bank (label C).

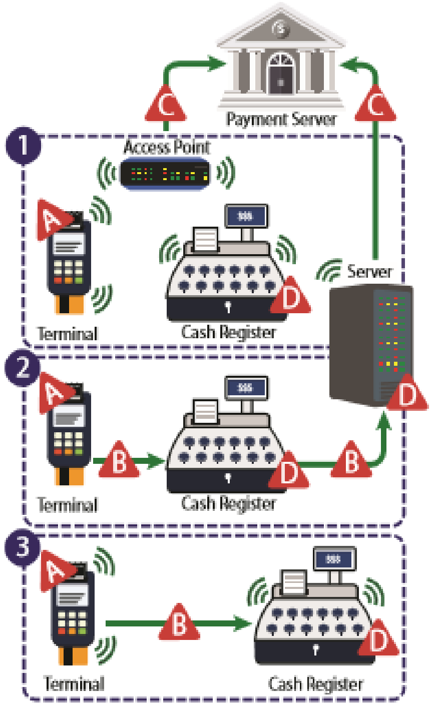


Fig. 3: PoS system threats. Red triangles, labeled *A*, *B*, *C*, and *D*, identify where customer card data can be stolen. Numbers (1,2,3) represent a fully on-line, on-line and off-line payment architectures, respectively.

In fact, many different ways to exploit PoS vulnerabilities and steal customer's data exist:

- **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. As an example, input devices can be either physically replaced or directly purchased with vulnerable or misconfigured software .
- **Scrapers:** In this attacker, a malware is installed within the PoS system in order to steal customer's card data. As an example, cybercriminals can infect the system using phishing attacks. However, in some other cases, the malware is installed with

the help of an insider or via a backdoor. RAM scrapers work by examining the list of processes that are running on the PoS system and by inspecting the memory for customer's card data such as account numbers and expiration dates.

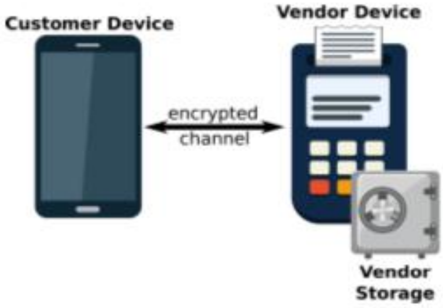
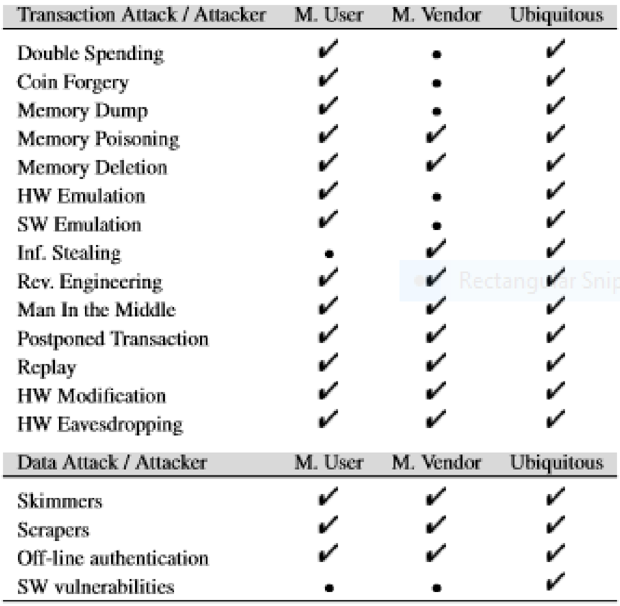


Fig. 4: FRoDO model

• **Forced off-line authorization**: In this scenario, the attacker exploits a DoS attack to force the PoS system to go off-line. By doing so, the attacker will force the payment card data to be locally processed. This means that any data read from the card will be locally decrypted and verified, thus creating an opportunity for the attacker to easily collect all the required information.



Transaction Attack / Attacker	M. User	M. Vendor	Ubiquitous
Double Spending	✓	•	✓
Coin Forgery	✓	•	✓
Memory Dump	✓	•	✓
Memory Poisoning	✓	✓	✓
Memory Deletion	✓	✓	✓
HW Emulation	✓	•	✓
SW Emulation	✓	•	✓
Inf. Stealing	•	✓	✓
Rev. Engineering	✓	✓	✓
Man In the Middle	✓	✓	✓
Postponed Transaction	✓	✓	✓
Replay	✓	✓	✓
HW Modification	✓	✓	✓
HW Eavesdropping	✓	✓	✓
Data Attack / Attacker	**M. User**	**M. Vendor**	**Ubiquitous**
Skimmers	✓	✓	✓
Scrapers	✓	✓	✓
Off-line authentication	✓	✓	✓
SW vulnerabilities	•	•	✓

TABLE 1: Transaction and data attacks that can be unleashed by each attacker model.

• **Software vulnerabilities**: payment applications themselves are also vulnerable to several attacks I attackers and each one of them exploits some payment software vulnerabilities.

With respect to PoS data vulnerabilities, there are three specific attacks that have to be analyzed.

• **Data in memory**: the target of this attack is card data that is feed into the PoS system by some input device. One way to avoid such attack is by encrypting the card data as soon as possible and by keeping it encrypted as long as possible through its life within the system.

• **Data in transit:** the target of this attack is the data that is exchanged between all the entities of the system that processes customer's data. Even in fully off-line electronic payment systems, this attack is still available. In fact, a payment system is usually composed by two or more elements and card data is exchanged between all of them. The technologies that are normally used for addressing the data in transit vulnerability include SSL, TLS and, IPsec .

• **Data at rest:** the target of this attack is the card data stored in non-volatile memories within the system. The only way to avoid such kind of attack is to avoid any data storage at all. Now that all the data breaches and attacks models have been described, it is possible to introduce our solution. After the description of both the architecture and the protocol being used, it will be shown how our proposed system is the first solution able to provide a fraud resilient off-line micro-payment scheme.

IV. SECURITY ANALYSIS

In this section the robustness of proposed system is discussed. Fraud Resilient Mechanism for Micropayments at point of sales uses both symmetric and asymmetric cryptographic primitives in order to guarantee the following security principles:

• **Authenticity:** It is guaranteed in proposed system by the on-the-fly computation of private keys. In fact, both the identity and the coin element use the key generator to compute their private key needed to encrypt and decrypt all the messages exchanged in the protocol. Furthermore, each public key used by both the vendor and the identity/coin element is signed by the bank. As such, its authenticity can always be verified by the vendor.

• **Non-Repudiation:** The storage device that is kept physically safe by the vendor prevents the adversary from being able to delete past transactions, thus protecting against malicious repudiation requests. Furthermore, the content of the storage device can be backed up and exported to a secondary equipment, such as pen drives, in order to make it even harder for an adversary to tamper with the transaction history.

Integrity: it is ensured with the encryption of each digital coin by the bank or identity/coin element issuer. Coin seeds and coin helpers are written into the coin element registers by either the bank or coin element issuer such that the final coin value given as output corresponds to an encrypted version of the real digital coin. As such, by using the public key of the bank or identity/coin element issuer, it is always possible to verify the integrity of each coin. Furthermore, the integrity of each message exchanged in the protocol is provided as well. In fact, both the identity and the coin element use their private/public keys. The private key is not stored anywhere within the identity/coin element but it is computed each time as needed.

- **Confidentiality**: Both the communications between the customer and the vendor and those between the identity element and the coin element leverage asymmetric encryption primitives to achieve message confidentiality.
- **Availability**: The availability of the proposed solution is guaranteed mainly by the fully off-line scenario that completely removes any type of external communication requirement and makes it possible to use off-line digital coins also in extreme situations with no network coverage. Furthermore, the lack of any registration withdrawal phase, makes proposed system able to be used by different devices.

Fraud Resilient Mechanism for offline Micropayments at point of sales uses two different elements an identity element and a coin element, in order to improve the security of the whole payment system In fact, the vendor device does not directly communicate with the coin element but has to go through the identity element. On the other hand this allows either the bank or the coin element issuer to design all the digital coins belong to a specific coin element to be read only by a certain identity element, i.e. by a specific user. This means that even though the coin element is lost or it is stolen by an attacker, such element will not work without the associated identity element. As such, the identity element can be considered as a second factor aimed at improving the security of customer coins. On the other hand, the identity element can be used to fight against attackers as well. In fact, as depicted in if an identity element is considered malicious and is blacklisted, no matter what is the device used by the user, any coin will not be accepted and processed by the vendor.

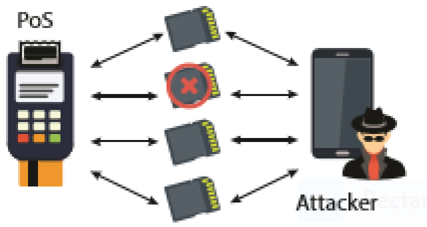
4.1 Attack Mitigation

In this section, the resiliency of Fraud Resilient Mechanism for Offline Micropayments at point of sales to the attacks listed is discussed before

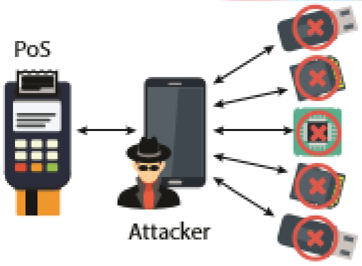
- **Double Spending**: The read-once property of the erasable PUF used in this solution prevents an attacker from computing the same coin twice. Even if a malicious customer creates a fake vendor device and reads all the coins, it will not be able to spend any of these coins due to the inability to decrypt the request of other vendors. Indeed, as the private keys of both the identity and coin elements are needed to decrypt the request of the vendor and can be computed only within the customer device. The fake vendor could then try to forge a new emulated identity/coin element with private/public key pair. However, identity/coin element public keys are valid only if signed by the bank. As such, any message received by an unconfirmed identity/coin element will be immediately rejected.
- **Coin Forgery:** Each coin is encrypted by either the bank or the coin element issuer and thus it is not possible for an attacker to forge new coins.
- **Emulation**: Physical unclonable functions, by design, can be neither dumped nor forged, either in hardware or software. Responses computed by emulated/fake PUFs will be different from the original ones.
- **Postponed Transaction**: The only way to understand data obtained as output from the identity/coin element is by having access to their private key. However, physically opening these elements will alter their PUFs behavior thus invalidating the elements itself. However, no information is kept within the elements, either in plain-text or in the encrypted form. As such, an attacker will not be able to steal any information.
- **Information Stealing**: The private key of each element is computed on-the-fly as needed. No sensitive information is kept in either the identity or the coin element. Coin seeds and coin helpers do not provide by themselves any information about coins and physical access to the hardware will cause the PUFs to change their behavior.
- **Replay**: Each transaction, even if related to the same coin, is different due to the random salt generated each time by the vendor.
- **Man In the Middle:** Digital coins are encrypted by either the bank or the coin element issuer and contain, among all other things, the ID of the coin element. Furthermore, as in proposed system digital coins are computed at run-time rather than being written in to the memory, an attacker cannot

dump coins from another customers. Last but not least, an attacker cannot pretend to be another customer with a different ID because it will not be able to compute his private key.

- **Reverse Engineering:** By design, any attempt to tweak and steal any useful information from either the identity or the coin element will alter the behavior of the PUFs thus rendering the elements no longer usable.
- **Denial of Services:** Fraud Resilient Mechanism for offline micropayments at point of sales uses an initial pairing process. Such step cannot be accomplished by an attacker as it requires a security code to be manually type do the customer's device. As such, DoS attacks are mitigated. Even



(a) The lack of an identity element allows an attacker to play with scratch cards as much as he wants since malicious operations only affect the single scratch card.



(b) The identity element in FRoDO allows attackers or malicious users to be blacklisted, rendering their coin element unavailable for future transactions.

Attacks over the coin element

if the attacker is a malicious vendor, each transaction has to be confirmed by the customer thus preventing batch attacks where either the identity or the coin element are repeatedly challenged.

- **HW Modification**: Again, by design, it is not possible for an attacker to either add or modify or remove any element belonging to either the identity or the coin element without changing its behavior.
- **HW Eavesdropping:** Solutions have been proposed in the literature that use photon counting APD modules and photon emission microscope with In GaAs image sensors together with Focused Ion Beam (for short, FIB) systems in order to locate faults within integrated circuits. However, as explained in we consider this kind of attack an overkill.
- **Repudiation:** Fraud Resilient Mechanism for offline Micropayments at point of sales does not provide a transaction dispute protocol phase. However, while the payment transaction is accomplished in a fully off-line scenario, any additional operation is accomplished on-line. In this way, the customer cannot repudiate a valid transaction (the log entry for that transaction will be notified on-line by the vendor) and the same applies for the vendor (a repudiated valid transaction cannot be spent). So far, resiliency to the attacks has been shown. Next, other considerations are shared based on the different attacker models.
- **Malicious Customer:** As shown at the beginning of this section, forgery, dump, and reply attacks are mitigated by design.
- **Malicious Vendor:** The only feasible attack for a malicious vendor is the deletion of past transaction entries from the storage device. However, this is not possible as the storage device is assumed to be kept physically secure by the vendor.
- **Ubiquitous:** The smarter attack that can be unleashed by such an attacker is the stealing of information from each device involved in the transaction. However, as described later in this section, Fraud Resilient Mechanism for Micropayments at point of sales proved to be resilient to data breaches.

V. CONCLUSION

In this paper we have introduced Fraud Resilient Mechanism for Micropayments at point of sale is, to the best of our knowledg, this is first data-breach-resilient fully off-line micropayment approach. The security analysis shows that Fraud Resilient Mechanism for Micropayments at point of sale does not impose trustworthiness assumptions. Further, Fraud Resilient Mechanism for Micropayments at point of sales is only the first solution in the literature where no customer device data attacks can be exploited to compromise the system. This has been achieved mainly by PUF'S architecture and protocol design. Our analysis shows that Fraud Resilient Mechanism for Micropayments at point of sales is the only proposal that enjoys all the secure micro-payment solution require properties, which gives flexibility when considering the payment medium (types of digital coins). Finally, some issues which are open are identified which are left for future process. In particular, we are researching the possibility to allow digital change which help to spent micro off-line payments while maintaining the same level of security and usability.

Future Enhancement

We present basic idea of Micropayment by introducing two typical Micropayment schemas here. People should keep in mind that Micropayment technology is still not mature yet. It still remains as an attractive but hard challenge.

REFERENCES

[1] J.Lewandowska,http://www.frost.com/prod/servlet/pressrelease.page?docid=274238535, 2013.

[2] R. L. Rivest, "Payword and micromint: two simple micropayment schemes," in CryptoBytes, 1996, pp. 69–87.

[3] S. Martins and Y. Yang, "Introduction to bitcoins: a pseudo-anonymous electronic currency system," ser. CASCON '11. Riverton, NJ, USA: IBM Corp., 2011, pp. 349–350.

[4] Verizon, "2014 data breach investigations report," Verizon, Technical Report, 2014.

[5] T. M. Incorporated, "Point-of-sale system breaches," Trend Micro Incorporated, Technical Report, 2014.

[6] Mandiant, "Beyond the breach," Mandiant, Technical Report, 2014.

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

[8] https://www.deepdyve.com/lp/institute-of-electrical-and-electronics-engineers/frodo-fraud-resilient-device-for-off-line-micro-payments-LvyAOyhGqq.

[9] http://frontl.in/projects/ftj1666-frodo-fraud-resilient-device-for-off-line-micro-payments-ieee-java-project-2016-2017/.

[10] http://www.crypto.com/papers/knpay.pdf.