RESEARCH ARTICLE OPEN ACCESS

Offline Micro Payments through Resilient Networks

Ms. Guddeti Divya Rani [1], A.Ravi [2]
M.Tech (CSE) [1], Professor [2]
Department of Computer Science and Engineering
Priyadarshini College of Engineering and Technology
(Affiliated to JNTUniversity, Ananthapuram) Nellore
Andhra Pradesh –India

ABSTRACT
Credit and debit card data theft is one of the earliest forms of cybercrime. Still, it is one of the most common nowadays. 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. Modern PoS systems are powerful computers equipped with a card reader and running specialized software. Increasingly often, user devices are leveraged as input to the PoS. In these 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. Our solution improves over up to date approaches in terms of flexibility and security. To the best of our knowledge, FRoDO is the first solution that can provide secure fully off-line payments while being resilient to all currently known PoS breaches. In particular, we detail FRoDO architecture, components, and protocols. Further, a thorough analysis of FRoDO functional and security properties is provided, showing its effectiveness and viability.

Keywords:- Mobile Secure Payment, Architecture, Protocols, Cybercrime, Fraud-Resilience.

I. INTRODUCTION

Market analysts have predicted that mobile payments will overtake the traditional marketplace, thus providing greater con-venience to consumers and new sources of revenue to many companies [1]. 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 tech-nology 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 (see Payword [2]) back in 1996. Nowadays, crypto-currencies and decentralized payment systems (e.g. Bitcoin [3]) 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.

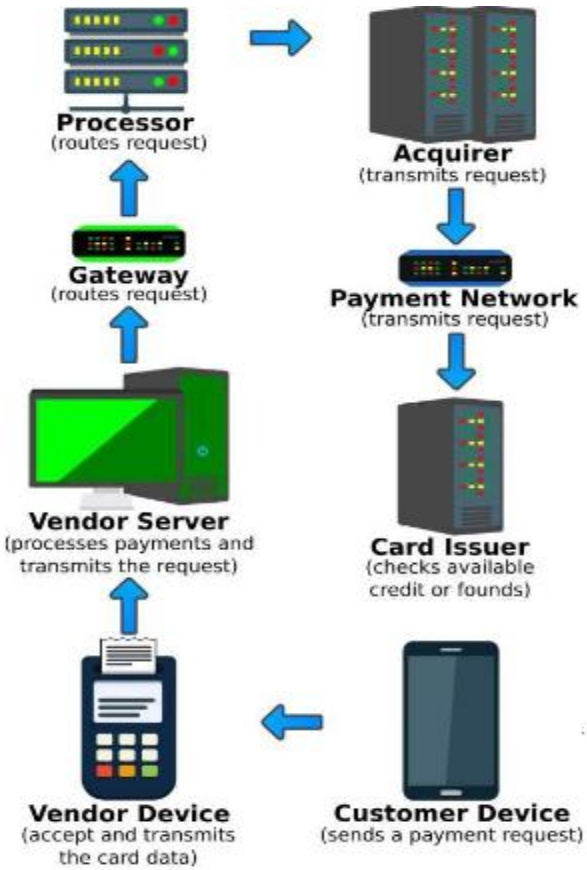
1.1 PROBLEM AND OBJECTIVES

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 Informa-tion (PII) [4], [5].

Although PoS breaches are declining [4], they still remain an extremely lucrative endeavor for criminals [6]. 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 [7].

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 PoSes 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 net-work 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.



II. PROPOSED MODEL

The solution proposed in this work, FRoDO, is based on strong physical unclonable functions [27], [28]

but does not require any pre-computed challenge-response pair [29]. Physical Unclonable Functions (for short, PUFs) were introduced by Ravikanth [29] in 2001. He showed that, due to manufacturing process variations, every transistor in an integrated circuit has slightly different physical properties that lead to measurable differences in terms of electronic properties. Since these process variations are not controllable during manufacturing, the physical properties of a device cannot be copied or cloned. As such, they are unique to that device and can be used for authentication purposes.

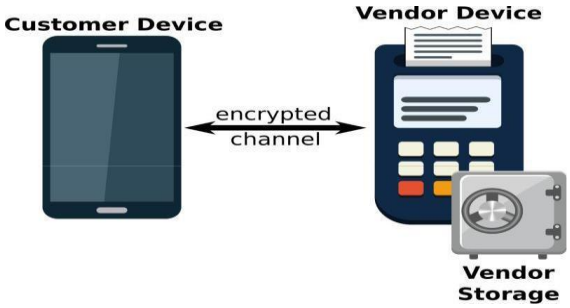
FRoDO is the first solution that neither requires trusted third parties, nor bank accounts, nor trusted devices to provide re-siliency against frauds based on data breaches in a fully off-line electronic payment systems. Furthermore, by allowing FRoDO customers to be free from having a bank account, 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.

As depicted in Figure 4, FRoDO 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 untrusted except from a storage device, that we assume is kept physically secure by the vendor.

Furthermore, it is important to highlight that FRoDO has been designed to be a secure and reliable encapsulation scheme of digital coins. This makes 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. Any bank will then be capable of verifying digital coins issued by other banks by requiring banks and vendors to agree on the same standard formats.



FRoDO does not require any special hardware component apart from the identity and the coin element that can be either plugged into the customer device or directly embedded into the device. Similarly to secure elements, both the identity and the coin element can be considered tamper-proof devices with a secure storage and execution environment for sensitive data. Thus, as defined in the ISO7816-4 standard, both of them can be accessed via some APIs while maintaining the desired security and privacy level. Such software components (i.e. APIs) are not central to the security of our solution and can be easily and constantly updated. This renders infrastructure maintenance easier

III. FRoDO: THE ARCHITECTURE

the architecture of FRoDO is com-posed 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.

Identity Element:

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

– Cryptographic Element: used for symmetric and asymmet-ric 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 asymmet-ric 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 [30]: is a read-once PUF [30]. After the first challenge, even if the same input is used, the output will be random;

– Coin Reconstructor: 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 reconstructor uses helper data stored into coin registers to extract the original output from the PUF.

Both the identity element and the coin element are built upon physically unclonable functions. As such, both of them inherits the following features:

Clone Resiliency: it must be extremely hard to physically clone a strong PUF, i.e. to build another system which has the same challenge-response behavior as the original PUF. This restriction must hold even for the original manufacturer of the PUF;

Emulation Resiliency: due to the very large number of possible challenges and the PUF's finite read-out rate, a complete measurement of all challenge-response pairs (for short, CRPs) within a limited time frame must be extremely hard to achieve;

Unpredictability: it must be difficult to numerically predict be described. Further, in Section 5.2 the transaction protocol will be depicted

KEY GENERATOR

As depicted in Figure 5, the key generator element is used both within the identity element and within the coin element. The main responsibility 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 FRoDO to implement strong challenge-response authentication. In particular, multiple physical unclonable functions are used to authenticate both the identity element and the coin element and last, but not least, to allow them to interact in a secure way (as described in Section 5.2).

ERASABLE COINS

At the heart of FRoDO proposal lies a read-once strong physical unclonable function [30]. Such 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

IV. FRoDO: THE PROTOCOL

This section describes the payment protocol being used in FRoDO. For completeness' sake, the Transaction Dispute and the Redemp-tion phases will be introduced in this section, even though they are not part of the payment procedure (composed of the Pairing and of the Payment phases).

5PAIRING PHASE

FRoDO relies on standard pairing protocols such as the Bluetooth passkey entry simple pairing process (for short, SPP) [38]. 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. Furthermore, in order to avoid brute force pairing attacks during the pairing phase, FRoDO adopts a "fail-to-ban" approach. If fraudsters consecutively fail to perform the pairing,

PAYMENT PHASE

For the sake of clarity and completeness, the FRoDO payment protocol will be described from two different points of view. From the first one (depicted in Figure 10 where by Enc(X,Y 1, ,Yn) we mean that data Y1 Yn is encrypted using key X), messages exchanged between the vendor and the customer device will be described. Then, from the second one (depicted in Figure 11), customer device internal messages exchanged between the identity element and the coin element will be described.

REDEMPTION PHASE

FRoDO digital coins have been designed as containers able to represent and to contain real (digital) money. As such, each vendor can verify them without the help of any TTP as shown in this section. Once the off- line transaction has been completed, the vendor owns one or more digital coins. Such coins are encrypted by the bank/card issuer at manufacturing time and, as such, they can be verified at any time using the public key of the bank/card issuer. If coins prove to be authentic, the vendor can use them either to send them back to the bank/card issuer in exchange for real money or as other digital currencies. In this latter case, the coins will be broadcast over the network depending on the payment scheme being used (a possible example is the Bitcoin network).

It is important to highlight that, as described above, each FRoDO payment transaction just needs the pairing and the pay-ment phases in order to be

accomplished. In fact, as in many other cryptographic currencies, the proposed protocol is only re-sponsible for the creation and validation of payment transactions. Once the transaction and all the coins associated with it have been verified, the way such coins will be further spent/redeemed by the vendor is beyond the scope of the proposed protocol. The same is true for bitcoins where the proof of work algorithm is only used to verify the transaction rather than the way bitcoins are spent. As such, security and reliability aspects of the redemption phase will not be discussed here as their study is beyond the scope of this work.

SECURITY ANALYSIS

In this section the robustness of FRoDO is discussed. FRoDO uses both symmetric and asymmetric cryptographic primitives in order to guarantee the following security principles:

Authenticity: it is guaranteed in FRoDO 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 equip-ment, 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;

1.BLACKLISTS

As detailed in Section 5.1, FRoDO uses two different elements: an identity element and a coin element, in order to improve the security of the whole payment system (see Figure 12). In fact, the vendor device does not directly communicate with the coin element but has to go through the identity element. On the one 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.

2. ATTACK MITIGATION

Double Spending: the read-once property of the erasable PUF [30] 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 (see the payment protocol in Section 5.2). Indeed, as described in Section 5.1, 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. 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

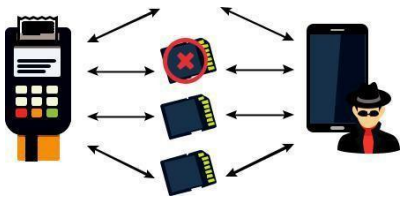
element is by having access to their private key. However, physically opening these elements will alter their PUFs behavior thus invalidating the elements itself. However, no information is kept within the elements, either in plain-text or in the encrypted form. As such, an attacker will not be able 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 as already described in Section 5.1;

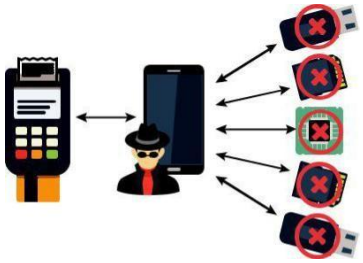
Replay: each transaction, even if related to the same coin, is different due to the random salt generated each time by the vendor;

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 FRoDO digital coins are computed at run-time rather than being written into 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;



(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

3.DATA BREACH RESILIENCY

As already introduced in Section 4, off-line PoS are usually attacked to steal private and sensitive customer's information. However, devices belonging to a PoS system are usually kept physically and digitally secure. As such, attacks against PoS systems in mature environments are typically multi-staged (see also Section 3). Furthermore, as the scenario is off-line, there is no direct connection to the external world. As such, stolen data has to be kept hidden within the PoS system waiting for the attacker to collect them.

The scenario is completely different for mobile payment sys-tems where the customer's device itself is used as input device. Common examples are smartphones used as credit card reader or as digital wallet [3]. In this new scenario, all the attacks that have been introduced in Section 4 are even more dreadful, since customer devices, such as smartphones, are continuously threatened by cyber-attacks. This means that an attacker does not need anymore to infiltrate and traverse the PoS system. He just needs to compromise the device or use forensic tools [49] in order to steal credit card information and keep them hidden within the device itself, ready for an exfiltration. As such, a new approach is required that does not make assumption on the trustworthiness of all the involved devices and that also keeps sensitive data protected against all the attacks listed in Section 4.

4.PHYSICAL ACCESS PROTECTION

As regards physical attacks to PUFs, Integrated Circuits (ICs) and hardware in general, some relevant results are discussed in [50] and [47]. The first one aims at protecting IC integrity as each manufactured IC is rendered inoperative unless a unique per-chip unlocking key is applied. After manufacturing, the response of each chip to specially generated test vectors is used to construct the correct per-chip unlocking key. As concerns [47], Choi and Kim aimed to protect the keys inside TPMs using a PUF. In fact, when the keys are stored in memory and when they are moved through the bus, their value is changed with the PUF, thus rendering eavesdropping out of the PUF IC useless. When the keys are needed for the cryptographic module, they are retrieved from outside the PUF IC and decrypted by the same PUF. However, the values of the keys could be revealed through side-channel attacks, e.g. non-invasive forms of physical attack measuring timings, power consumption, and electromagnetic radiation. Most cryptographic modules are known to be vulnerable to side-channel attacks, and these attacks would be effective against the TPM; thus, countermeasures against side-channel attacks are necessary.

5. KEY ROLLOVER

As for all the real-world payment schemes based on credit, debit and prepaid cards, FRoDO assumes that, in case of bank/coin element issuer private key renewal, a time-window is adequately chosen to let customers decide whether to spend their last coin or to get the current coin element exchanged with a new one. These standard procedures are widely accepted in the real world As such, no custom key rollover protocol has been designed in FRoDO.

V. CONCLUSION

In this paper we have introduced FRoDO that is, to the best of our knowledge, the first data-breach-resilient fully off-line micro-payment approach. The security analysis shows that FRoDO does not impose trustworthiness assumptions. Further, FRoDO is also 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 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 also 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] J. Lewandowska, http://www.frost.com/prod /servlet/press-release.pag? 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] Mandiant, “Beyond the breach,” Mandiant, Technical Report, 2014. Bogmar, “Secure POS & kiosk support,” Bogmar, Technical Report, 2014

ACKNOWLEDGEMENT

First Author: Ms.Guddeti Divya Rani, Pursuing M.Tech in Computer Science and Engineering (CSE) from Priyadarshini College of Engineering and Technoogy (Affiliated to JNTUniversity, Ananthapuram), Nellore, Andhra Pradesh

Second Author: Prof. A.Ravi has received B.Tech review degree in Computer Science and Engineering from Mekapati Rajamohan Reddy Institute of Technology & Science, Udayagiri and M.Tech in Computer Science and Engineering from Gokul Institute of Technology and Sciences, (Affiliated to JNTUniversity, Kakinada), Bobbili, Andhra Pradesh, India. His interesting domain is Web based Domain, he attended 3 International and 2 National Conferences and published 3 papers in various International Journals. He is dedicated to teaching field from last 11 Years, presently working as Assistant Professor in Computer Science and Engineering Department at Priyadarshini College of Engineering and Technology (Affiliated to JNTUniversity, Ananthapuram), Nellore, Andhra Pradesh, India

.