FRDO: Micro-Payments

[1]Mrs. Shashikala S V, HOD, [2]Likhitha B,

[1]HOD, [2]PG Student, Dept of CSE, BGSIT, BG Nagar, Mandya-571448,

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.

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. 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 back in 1996. 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.

1.1 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) .

Although PoS breaches are declining , they still remain an extremely lucrative endeavor 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 .

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.

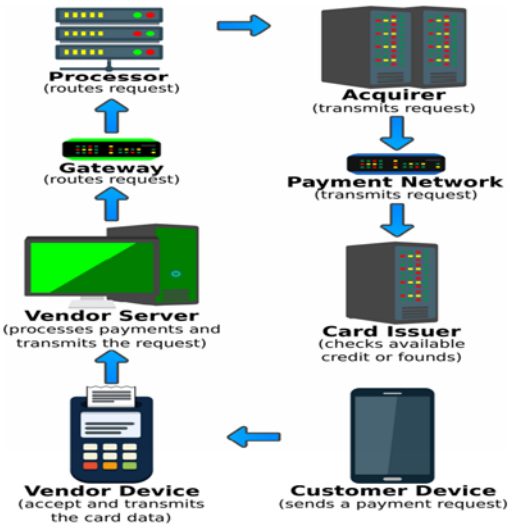

Fig. 1: Payment authorization stages

1.2 Contribution

This paper introduces and discusses FRoDO, a secure off-line micro-payment approach using multiple physical unclonable func-tions. 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 our 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.

II. BACKGROUND

Payment transactions are usually processed by an electronic pay-men system (for short, EPS). The EPS is a separate function from the typical point of sale function, although the EPS and the PoS system could be co-located on the same machine. In general, the EPS performs all payment processing, while the PoS system is the tool used by the cashier or consumer .

2.1 Pos System Breaches

Attacks against PoS systems in mature environments are typically multi-staged . First, the attacker must gain access to the victim's network (this step is called infiltration). Usually, they gain access to an associated network and not directly to the card-holder data environment. They must then traverse the network (this step is called propagation), ultimately gaining access to the PoS systems. Next, they install malicious software in order to steal data from the compromised systems (this step is called aggregation). As the PoS system is unlikely to have external network access, the stolen data is then typically sent to an internal backoffice server (see Figure 2) waiting for the attacker to be back (this step is called exfiltration).

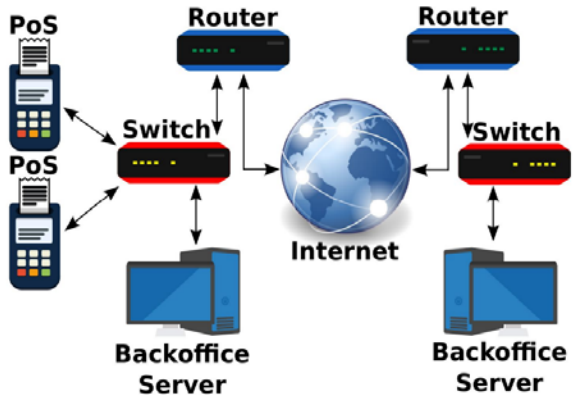

Fig. 2: Point of Sale architecture

PoS system network-level hacking can be rendered possible by exploiting shared connections, open networks, or by cracking the password of the merchant's network. However, networks can be monitored and protected against malicious activities. Network infiltration is just one of the many sophisticated attack methods. In addition, a successful server breach will give attackers access not only to a single PoS system or to a network of PoS systems in a single location but, depending on the architecture, possibly to all PoS systems controlled by the retailer, even in multiple locations.

Regardless of the adopted EPS model, the payment process is composed of two main processing phases, the authorization and the settlement. The authorization is the state of the payment process where the purchase is verified and finalized. The settlement comprises all actions happening after the authorization stage. Even though the data processed at this stage is not as valuable as the data processed during the authorization stage, it still contains sensitive data such as the amount of money spent within the transaction. Such information is relevant to customer privacy and thus it has to be protected.

2.2 Pos Device Breaches

PoS devices can be considered the most important entities in an electronic payment system and are normally "guarded" by employees during operating hours. However, it is still possible for an attacker to inject malware into the PoS or even to replace it with a fake/malicious device. In fact, many all-in-one PoS systems are based on general purpose operating systems. As such, they are susceptible to a wide variety of attack scenarios which could lead to large scale data breaches.

III. 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.

IV. PROPOSED MODEL

The solution proposed in this work, FRoDO, is based on strong physical unclonable functions but does not require any pre-computed challenge-response pair. Physical Unclonable Functions (for short, PUFs) were introduced by Ravikanth 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 3, 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.

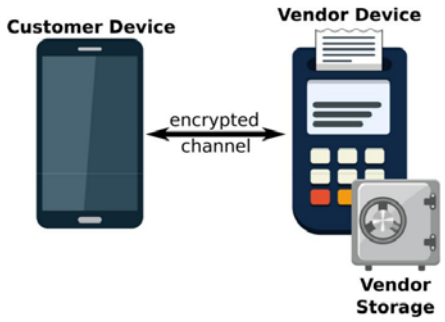

Fig. 3: FRoDO model

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.

4.1 FRoDO: The Architecture

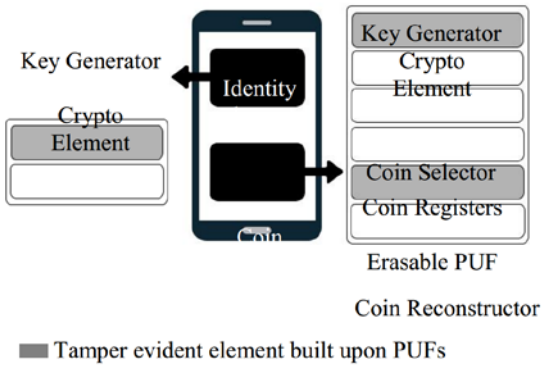

Fig. 4: FRoDO main architecture.

As depicted in Figure 5, 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.

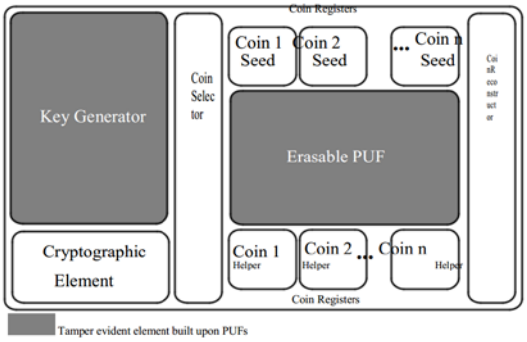

Fig. 5: Coin element architecture.

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 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;

4.2 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 .

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. Thus, both the identity and the coin element are shipped with such a hard-coded ID signed by the element issuer in order to avoid forgery attacks. This allows the customer to broadcast the public key of both the identity and the coin element to vendors that are not required to know all the public keys of all the active identity/coin elements in the world. Furthermore, vendors can encrypt payment requests with public keys of the customer's device identity element, thus ensuring that such requests will be read only by that customer.

However, given a fixed input, PUFs can produce a response that is unique to the manufacturing instance of the PUF circuit but that is not bitwise-identical when reiterated multiple times. As such, in order to use PUFs in algorithms where stable values are required, an intermediate step is needed. This problem is usually faced in cryptographic algorithms (known as "secret key extraction") . It can be solved using a two-steps algorithm. In the first step the PUF is challenged, thus producing an output together with some additional information called helper data. In the second step, the helper data is used to extract the same output as in the first step thus making the PUF able to build stable values. It is also possible to construct a two-steps algorithm guaranteeing that the computed value is perfectly secret, even if the helper data is publicly known. Practical instances of such kind of algorithm have been proposed in and the cost of actual implementations thereof is assessed in .

While this approach is feasible for the coin element that is based upon an erasable PUF, this is not feasible for the

identity element. In fact, storing PUF helper data within the device could allow an attacker to reconstruct the private key of the device. However, a number of solutions have been proposed to correct PUF output on-the-fly thus allowing the generation of stable secret values within the device, without the need of any helper data.

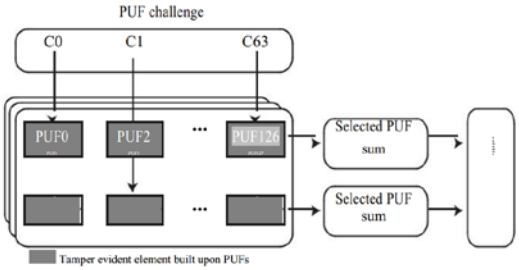

Fig. 6: Stable PUF-based private keys generation.

compute the bottom delay term. The sign bit of the difference between the two delay terms determines whether the PUF outputs a 1 or a 0 bit-value for the 64-bit challenge C0 C63. The remaining bits of the difference determine the confidence level of the 1 or the 0 output bit. The k-sum PUF can be thought of as a k-stage Arbiter PUF with a real-valued output that contains both the output bit as well as its confidence level. This information is then used by the downstream lightweight error correction block that is able to output a stable value.

By using such on-the-fly stable value generation process, the identity/coin element private keys are not stored anywhere within the customer device. Hence, they are much better protected from attackers trying to steal them.

4.3 Erasable Coins

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

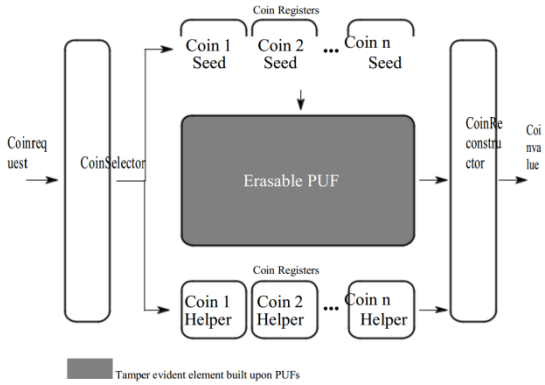

Fig. 7: Coin reconstruction based on an erasable strong PUF.

FRoDO is not tied to any specific digital coin format. Further-more, it does not directly write digital coins within the customer's coin element but uses special hardware to reconstruct them on-the-fly when needed. As depicted in Figure 8, 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 burden of selecting the coin registers (one or more) that will be involved in the transaction. The selected coin seed register is then used as input to the erasable PUF, while the coin helper register is combined to the PUF output in order to reconstruct the final value of the coin. The scheme of a coin reconstruction is given in Figure 9. Coin raw data is first encrypted by the bank with its private key and then modified in order to create a chunk of bytes that are written into the coin seed register. Further, helper data are written in the coin helper register in order to provide stable PUF output . The coin seed register is then used at transaction time to challenge the erasable PUF. The obtained response is combined with the coin helper register data in order to obtain the original encrypted coin again. Finally, as depicted in Figure 9, the original coin data is computed using the public key of the bank.

Last but not least, FRoDO does not rely on any specific number or type of coins. As such, it can work with coin elements of any size and with any number of coins.

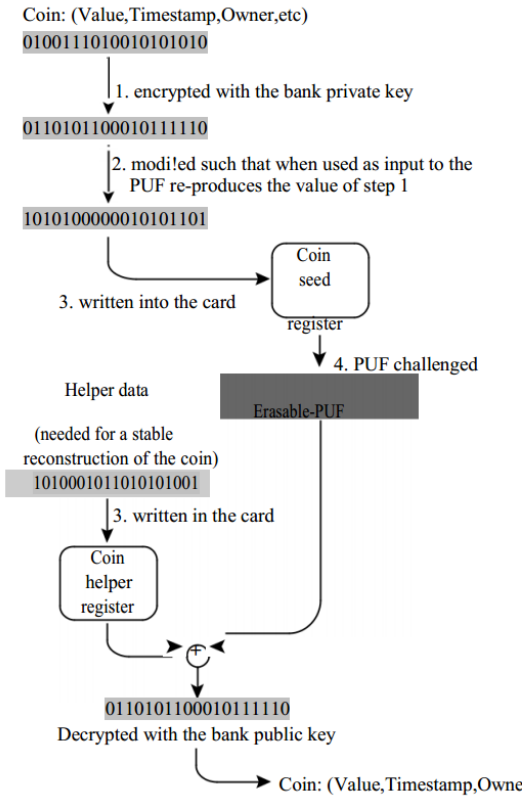

Fig. 8: Coin reconstruction

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.

6

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] Verizon, “2014 data breach investigations report,” Verizon, Technical Report, 2014.

[5] T. M. Incorporated, “Point-of-sale system breaches,” Trend Micro Incor-porated, Technical Report, 2014.

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

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

[8] V. Daza, R. Di Pietro, F. Lombardi, and M. Signorini, “FORCE - Fully Off-line secuRe CrEdits for Mobile Micro Payments,” in 11th Intl. Conf. on Security and Cryptography, SCITEPRESS, Ed., 2014.

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

[10] S. Golovashych, “The technology of identification and authentication of financial transactions. from smart cards to NFC-terminals,” in IEEE IDAACS ’05, Sep 2005, pp. 407–412.