International Journal of Advanced Trends in Engineering and Technology (IJATET)
Impact Factor: 5.665, ISSN (Online): 2456 - 4664
(www.dvpublication.com) Volume 2, Issue 1, 2017

MICRO PAYMENTS IN OFF-LINE SECURE CREDITS USING RODO RESILIENT DEVICE

P. R. Gowdham Sankar* & K. Mahalakshmi**
** PG Scholar, Department of Computer Science and Engineering, SSM College of Engineering, Tamilnadu
** Assistant Professor, Department of Computer Science and Engineering, SSM College of Engineering, Tamilnadu

Cite This Article: P. R. Gowdham Sankar & K. Mahalakshmi, "Micro Payments in Off-Line Secure Credits Using Rodo Resilient Device", International Journal of Advanced Trends in Engineering and Technology, Page Number 34-38, Volume 2, Issue 1, 2017.

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.

Index Terms: Mobile Secure Payment, Architecture, Protocols, Cybercrime & Fraud-Resilience

Introduction:

Credit-card-based purchases can be categorized into two types: 1) Physical card and 2) Virtual card. In a physical-card based purchase, the cardholder presents his card physically to a merchant for making a payment. To carry out fraudulent transactions in this kind of purchase, an attacker has to steal the credit card. If the cardholder does not realize the loss of card, it can lead to a substantial financial loss to the credit card company. In the second kind of purchase, only some important information about a card (card number, expiration date, secure code) is required to make the payment. Such purchases are normally done on the Internet or over the telephone. To commit fraud in these types of purchases, a fraudster simply needs to know the card details. Most of the time, the genuine cardholder is not aware that someone else has seen or stolen his card information. The only way to detect this kind of fraud is to analyze the spending patterns on every card and to figure out any inconsistency with respect to the "usual" spending patterns. Fraud detection based on the analysis of existing purchase data of cardholder is a promising way to reduce the rate of successful credit card frauds. Since humans tend to exhibit specific behaviorist profiles, every cardholder can be represented by a set of patterns containing information about the typical purchase category, the time since the last purchase, the amount of money spent, etc. Deviation from such patterns is a potential threat to the system. Commercial activities on the Internet have increased in tandem with the fast growth of the Internet itself. With electronic commerce (e-commerce), business transactions have been made easier and faster via the Internet uncertainties and lack of standardized e-commerce procedures. This has slowed down the acceptance of e-commerce activities online. It would thus be beneficial if there can be some way to streamline and standardize e-commerce.

Agents and E-Payment Systems:

Agents are bits of software that help computer users by performing routine tasks, typically in the background on behalf of its user. Information gathering, filtering, and presentation are some well-defined tasks prescribed to agents. Traditional software such as word processors and spreadsheets only respond to human input in a fixed and predictable manner. Intelligent agents are capable of "thinking" and producing intelligent feedback. A key element in any e-commerce system is the method of payment. However, existing monetary and fund-transfer arrangements are difficult to be transplanted directly into the e-commerce marketplace. Currently, a common e-payment method involves the client transmitting to the merchant details of a payment card such as a VISA credit card. The merchant receives the information and proceeds to carry out a payment request with the card issuer via traditional payment card procedures. This system is simple and does not require the development of a new commercial infrastructure.

Problem Issues:

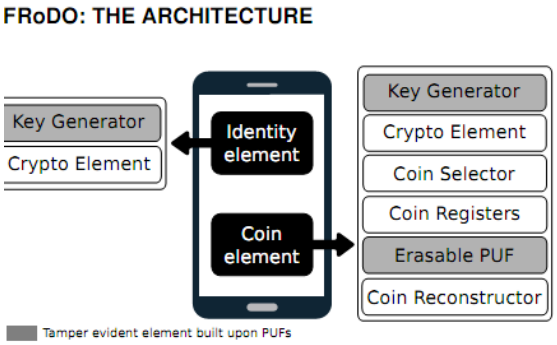
Over the last years, several retail organizations have been victims of information security breaches and payment data theft targetingconsumer payment card data and Personally Identifiable Information Although PoS breaches are declining, they still remain an extremely lucrative endeavor for criminals. 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 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 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 veryefficient 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.

Proposed Method:

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 in2001. 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 resiliency against frauds based on data breaches in a fully off-line electronic payment systems. Furthermore, by allowing FRoDO customers to be free from having a bank account, makes it also particularly interesting as regards to privacy. In fact, digital coins used in FRoDO are just a digital version of real cash and, as such, they are not linked to anybody else than the holder of both the identity and the coin element. Differently from other payment solutions based on tamperproof 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 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 FRoDO model 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, asdefined 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.

FRoDO: The Architecture:t



As depicted the architecture of FRoDO is composed of two main elements: an identity element and a coinelement. 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. The basic 64-sum PUF block firstly introduced in measuresthe difference between two delay terms, each produced bythe sum of 64 PUF values. Then, given a challenge, its ith bit(called Ci) determines, for each of the 64 stages, which PUF isused to compute the top delay term, and which one is used to compute the bottom delay term. The sign bit of the differencebetween the two delay terms determines whether the PUF outputsa 1 or a 0 bit-value for the 64-bit challenge C0 _ _ _C63. Theremaining 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 containsboth 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.

FRoDO: The Protocol:

This section describes the payment protocol being used in FRoDO. For completeness' sake, the Transaction Dispute and the Redemption 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). FRoDO relies on standard pairing protocols such as the Bluetooth passkey entry simple pairing process (for short, SPP) . At the end of the pairing protocol, both the customer and vendor deviceswill 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, their pairing future requests will be automatically banned (i.e.dropped) by the vendor for a given time-frame, usually 20 or 30seconds. If the number of consecutive bans reaches a security threshold value, the vendor can decide to blacklist the customer. To simplify exposition, all the encryption operations involved in the Bluetooth SPP protocol and used in the FRoDO pairing process will be omitted here as they refer to standardized protocols.

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 (Enc(X,Y1,_ _ _ ,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, customer device internal messages exchanged between the identityelement and the coin element will be described.The protocol depicted is composed of the following steps

- ✓ The customer sends a purchase request to the vendor asking for some goods
- ✓ The vendor first creates a random salt value. Then, it encrypts the coin request three times. The first time with the salt itself.The second time with the public key of the identity element (i.e. the public key of the customer device that is going to receive this request), and the last time with the private key of the vendor itself. Thus, operations performed by the vendor are the following:

  EncSalt (Req) =CReq (1)
  EncIePK(CReq;Salt) = EncReq (2)
  EncVSK(EncReq) = PrivateReq (3)
- ✓ Once the private request has been built, it is sent to the customer;
- ✓ When the customer receives such a request, first the private key of the identity element is computed by the identity element key generator. Then, all the encryption layers computed by the vendor are removed. As such, the customer computes three decryption operations. The first one with the public key of the vendor.The second one with the private key of the identity element and the last one with the salt value. Details follow:

  DecVPK(PrivateReq) = EncReq (4)
  DecIeSK(EncReq) = (CReq;Salt) (5)
  DecSalt (CReq) = Req (6)
- ✓ Once the coin request is in plain-text, the value of the coin is retrieved from the coin element. Then, such a value computed by the erasable PUF and the coin reconstructor is first encrypted with the salt, then with the private key of the identity element (in order to prove theauthenticity of the response) and at the end with the publickey of the vendor – to ensure that only the right vendor device can decrypt it. That is:

  EncSalt (CoinValue) =CValue (7)
  EncIeSK(CValue) = EncValue (8)
  EncVPK(EncValue) = PrivateResponse (9)
- ✓ When the vendor finally receives the Private Response, the last step only requires the coin just read to be validated. Then, the whole payment transaction can be authorized and committed. Main steps are as follows: first, the received response is decrypted with the private key of the vendor. Secondly, the

obtained value is decrypted with the public key of the identity element. Then, the salt is used to obtain the value read from the erasable PUF. As a final step, the public key of the bank/coin element issuer is used to decrypt the Coin Valuethat was encrypted (at manufacturing time) by the bank/coin element issuer, with its private key. This way, it is possible to obtain and verify the raw coin data built by the bank/card issuer.

DecVPK(PrivateResponse) = EncValue (10)
DecIePK(EncValue) =CValue (11)
DecSalt (CValue) =CoinValue (12)
DecBPK(CoinValue) = RawValue (13)

- ✓ If the raw value of the just read coin is correct, a new entry is stored in the storage device of the vendor after being encrypted with the vendor's private key. It is important to stress that the Coin Value value is not a raw representation of the coin, but it is encrypted at manufacturing time by the bank with its private key. This means that it is not possible to forge digital coins. Indeed, the whole transaction will be validated if and only if the decryption of the Coin Value with the public key of the bank is successful.

Client Module:

In this module client is going to online website and View Product and select to product models and view product details. Select and purchase their product .and transaction from their account All details are encrypted by using Private Key and public key, Keys are generated during user to purchase the product.

Key Generator:

This module is using cryptographic algorithm, this algorithm used for symmetric and asymmetric cryptographic algorithms applied to received the data input and sent as output by the identity element. Key Generator is by PUFs, which have been used to implement strong challenge-response authentication. Also, multiple physical unclonable functions are used to authenticate both the identity element and the coin element.

Secure Payment:

This module is used to Users are view products, and select products and their details and to be wish to purchase product and give all sensitive data like account details, payment details. All user information is encrypted because hackers do not hacking user information. All Encrypted data are separated by symmetric and Asymmetric cryptographic algorithms this is used to separate private and public keys. Private Key is send to user mail. User is used this key to view their purchase product and transaction their account.

Transaction at Coin Element:

This module is used to admin to work their website and add products like product name, description, warranty period, etc., and admin view all users purchase products but cannot view user account details. and to view which product is delivered or not.

Conclusions:

The first data-breach-resilient fully off-line micropayment 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 beenachieved 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 spentover multiple off-line transactions while maintaining the same level of security and usability.

References:

1. Chen. W, Hancke. G, Mayes. K, Lien. Y, and Chiu. J. H, Dec 2010,"Using 3G network components to enable NFC mobile transactions and authentication," in IEEE PIC '10, vol. 1, , pp. 441 –448
2. Dodis. Y, Ostrovsky. R, Reyzin. L and Smith. A, Mar 2008, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," SIAM J.Compute, vol. 38, no. 1, pp. 97–139,
3. Gomzin. S, 2014, Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions, 1st ed. Wiley Publishing,
4. Guajardo. J, Kumar. S. S, Schrijen. G. J and Tuyls. P, 2007, "FPGA intrinsic PUFs and their use for IP protection," ser. CHES '07. Berlin, Heidelberg: Springer-Verlag, pp. 63–80
5. Kori. B, Tuyls. P, and Ophey. W, 2005, "Robust key extraction from physical uncloneable functions," in Applied Cryptography and Network Security,ser. LNCS, J. Ioannidis, A. Keromytis, and M. Yung, Eds. Springer Berlin Heidelberg, vol. 3531, pp. 407–422
6. Nishide. T and Sakurai. K, 2011, "Security of offline anonymous electronic cash systems against insider attacks by untrusted authorities revisited,"ser. INCOS'11.Washington, DC, USA: IEEE Comp. Soc., pp.656–661

7. Rivest. R. L, in CryptoBytes 1996, "Payword and micromint: two simple micropayment schemes", pp. 69–87
8. Salama. M. A, El-Bendary. N, and Hassanien. A. E, in Intl 2011, "Towards secure mobile agent based e-cash system". Workshop on Security and Privacy Preserving in e-Societies. New York, NY, USA: ACM, pp. 1–6
9. Yu. M.-D, MRaihi. D, Sowell. R, and Devadas. S, in CHES 2011, "Lightweight and Secure PUF Key Storage Using Limits of Machine Learning," ser. LNCS, B. Preneel and T. Takagi, Eds. Springer Berlin Heidelberg, 2011, vol. 6917, pp. 358–373
10. VanesaDaza, Roberto Di Pietro, Flavio Lombardi, And Matteo Signorini, 12 June 2015 "Frodo: Fraud Resilient Device For Off-Line micro-Payments", Dependable And Secure Computing, IEEE Transactions On (Volume: PP , Issue: 99)