International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

Fraud Resilient Tool for Offline Micro Payments

Yashas. B.R[1] , Dr. Prabha. R[2]

[1]*PG Scholar, Department of ISE, Dr.AIT, Bangalore, Karnataka, India*
[2]*Associate Professor, Department of ISE, Dr.AIT, Bangalore, Karnataka, India*

Abstract— *Credit and debit card data theft is one of the latest forms of cybercrime. Still, it is one of the most common currently. Attackers often aim at stealing such customer data by aiming the Point of Sale system, i.e. the point at which a retailer first obtains customer data. Modern point of sale systems are powerful computers furnished with a card reader and running specialized software. Regularly user devices are leveraged as input to the Point of sale. In these situations, malware that can steal card data as soon as they are read by the device has flourished. As per, in cases where customer and vendor are persistently or intermittently disconnected from the network, no secure on-line payment is probable. This paper describes Frodo, a secure off-line micro-payment solution that is resistant to Point of sale 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 resolution that can provide secure fully off-line payments while being resistant to all presently known Point of sale breaches. In particular, we detail Frodo architecture, components, and protocols. Further, a detailed analysis of Frodo functional and security properties is provided, showing its efficiency and viability.*

1 INTRODUCTION

Market analysts have predicted that mobile payments will overtake the traditional marketplace, thus providing greater convenience to consumers and new sources of revenue to many companies. This scenario produces a shift in purchase methods from classic credit cards to new approaches such as mobile-based payments, giving new market entrants novel business chances.

Broadly supported by current hardware, mobile payment equipment is still at its initial stages of advancement but it is likely to increase in the close future as demonstrated by the growing interest in crypto-currencies. The first pioneering micro-payment system, was proposed by Rivest back in 1996. Currently, crypto-currencies and decentralized payment systems are gradually popular, fostering a shift from physical to digital currencies. However, such payment methods are not yet commonplace, due to numerous unresolved issues, including a lack of widely-accepted standards, limited interoperability between systems and, most prominently, security.

1.1 Problem and Objectives

Over the last years, several retail organization have victim's data theft targeting consumer payment card data and personally identifiable information.

Although Point of sale breaches are declining, 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, Point of sale systems always handle critical information and, oftentimes, they also require remote management [7].

Usually, as depicted in Fig. 1, Point of sale 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 Point of sale with other back-end systems may connect the former to their own internal networks. In addition, to reduce cost and simplify administration and maintenance, Point of sale devices may be remotely managed over these internal networks. However, a network connection might not be available due to whichever a transitory network service disruption or due to a stable lack of network coverage. Last, but not least, such on-line results are not actual efficient since remote communication can introduce delays in the payment process.

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

1.2 Contribution

This paper introduces and discusses Frodo, a secure off-line micro-payment approach using multiple physical unclonable functions (PUFs). Frodo features an identity element to authenticate the customer, and a coin element where coins are not locally stored, but are computed on-

thefly 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 (see Section 2). 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 Point of sale breaches.

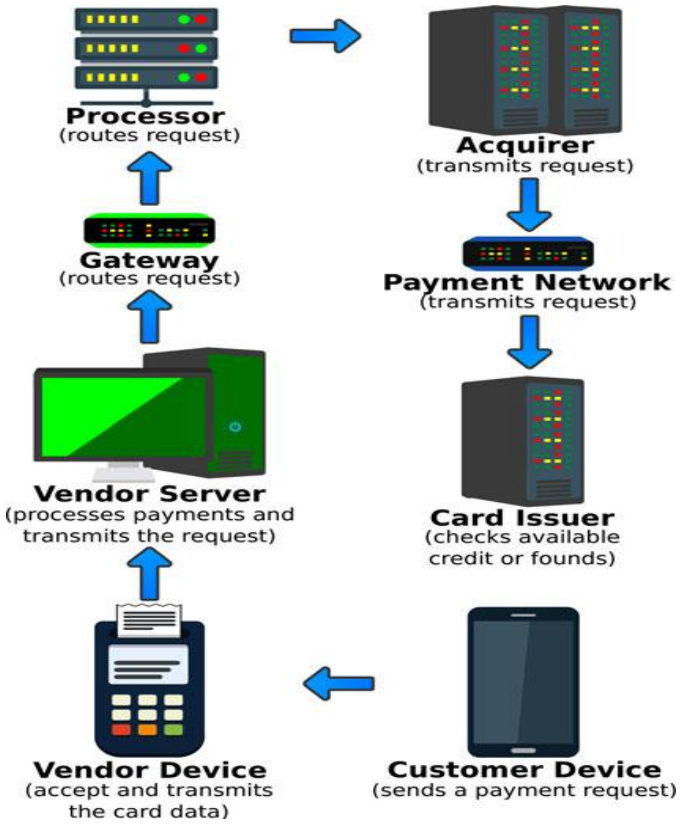

Fig-1: Payment authorization stages.

2 RELATED WORK

Mobile payment solutions proposed so far can be classified as fully on-line [8], [9], [10], [11], semi off-line [12], [13], weak off-line [14], [15] or fully off-line [16], [17], [18]. 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. This is the main reason why during last few years, many different approaches have been proposed to provide a reliable off-line payment scheme. Although many works have been published, they all focused on transaction anonymity and coin unforgeability. However, previous solutions lack a thorough security analysis. While they focus on theoretical attacks, discussion on real world attacks such as skimmers, scrapers and data vulnerabilities is missing.

As regards physical unclonable functions [19], a key component of our solution, other applications on banking scenarios have already been proposed in the past [20]. However such strong functions are generally used for authentication purposes only. As such, they only guarantee that data has been computed on the right device but they cannot provide any proof about the trustworthiness of the data itself.

It is worth mentioning here our previous work called FORCE [8] that, similarly to Frodo, was built using a PUF based architecture. FORCE provided a weak prevention strategy based on data obfuscation and did not address the most relevant attacks aimed at threatening customer sensitive data, thus vulnerable to many advanced attack techniques.

3 PROPOSED MODEL

The proposed system deals with introducing, Frodo, is depend totally on the physical unclonable functions [13] whereas that does not needed any pre-determined computed challenge-response pair mechanism [29]. Physical Unclonable Functions, it referred as (PUFs) was proposed by [14]. They demonstrated about the working process and their flows as well as the process variations, in each and every transistor in an integrated circuit considered in the physical properties. It may meager variation and various physical properties that causes to identifiable differences in relation to electronic properties. As these process variations are not measurable while it is manufacturing so therefore device the physical properties cannot be cloned or copied. Since, it is very important to have authentication process in the device. As such, they are unique to that device and can be used for authentication purposes.

As an solution that neither it needs the trusted devices nor bank accounts or requires trusted third parties to obtain the privacy re-siliency scheme against frauds depend on the on data breaches which is totally depend on the off-line payment systems in the banking sector. By utilizing Frodo customers can be visible from having account in the bank, it also makes attractive features in regards to the customer's privacy. In despite, Frodo utilizes two important element they are coin and identity element. The coins are utilized in Frodo as an digital version of using the real cash, that they are not associated to anyone else expect the holder of both

the coin and the element. It is presented in the Fig . Frodo can be utilized to any conditions which is applicable to payee/vendor and payer/customer device. All the considered devices can be affected by an attacker and are taken in the untrusted pasties without taking any storage device, it is assumed that vendor is secure physically.

3.1 Point of sale System of Breaches

Any assaulters against Point of sale (architecture) systems are referred as infiltration in the multi networks. The vendor improve the access level immediately to card-holder who has the confidentially data. It is very important to install antivirus software to prevent the data from the attackers who tries to steal data from the system. Point of sale system can provide the additional support to the network access, in order to stolen data waiting assaulters which is referred as exfiltration. Point of sale system would easily have shared connections with any networks especially open network for getting or cracking the password of the merchant's network. Hence, networks should be protected and supervised against assaulters performances. Infiltration is one of the common attack in the network. The proposed comprises of two important stages, they are authorization and the settlement. The authorization is process where the payment is accessed when the purchase is confirmed and verified as well as finalized. The settlement is consists of all stages occurring once after the authorization process. Therefore, it is processed at the first stage during the authorization process, it still contains the information regarding the money transactions to the customers in terms of security and the privacy and therefore it has to be secured.

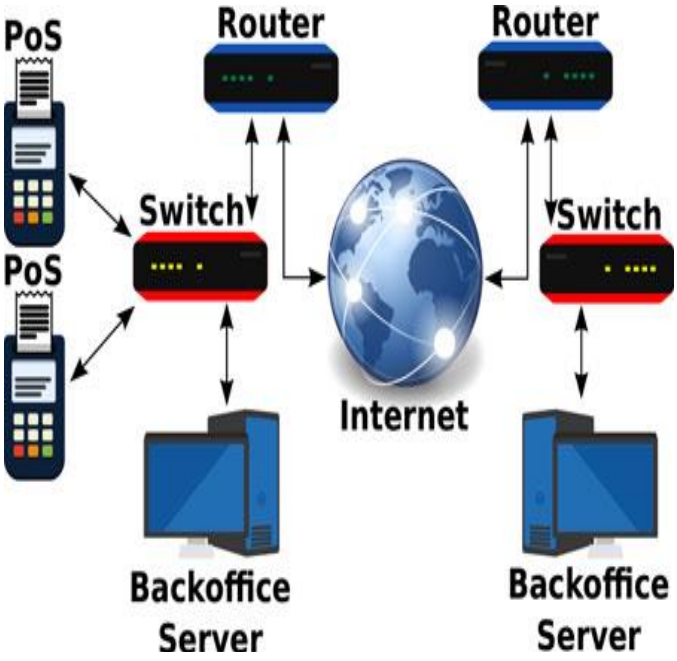

Fig -2: Point of sale architecture.

3.2 Threat Models

Depend on the capabilities and on the transactions of the money in terms of devices that can performed during the attackers are listed below;

• Ubiquitous: It is an internal assaulter they can permission to perform in any devices.

• Collector: It is an external assaulter that exchange data between vendor device and customer.

• Malicious Customer: This is an internal assaulter can neither it can include misbehavior node or physically customer device inside the customer device to crack the data of the customer.

• Ubiquitous It is also an internal assaulter with full access to perform in any devices.

3.3 System Model

It needs the trusted devices nor bank accounts or requires trusted third parties to obtain the privacy resiliency scheme against frauds depend on the on data breaches which is totally depend on the off-line payment systems in the banking sector. By utilizing Frodo customers can be visible from having account in the bank, it also makes attractive features in regards to the customer's privacy. In despite, Frodo utilizes two important element they are coin and identity element. The coins are utilized in Frodo as an digital version of using the real cash, that they are not associated to anyone else expect the holder of both the coin and the element. Apart from the various other payment solutions, it depend on the tamperproof hardware, Frodo considers that not only the PUFs but also on chips to consume the benefits of the tamper evidence feature. As a correlations, our consideration are very much limited than other techniques. As depicted in Figure 3, it can be utilized to any conditions which is applicable to payee/vendor and payer/customer device. All the considered devices can be affected by an attacker and are taken in the untrusted pasties without taking any storage device, it is assumed that vendor is secure physically.

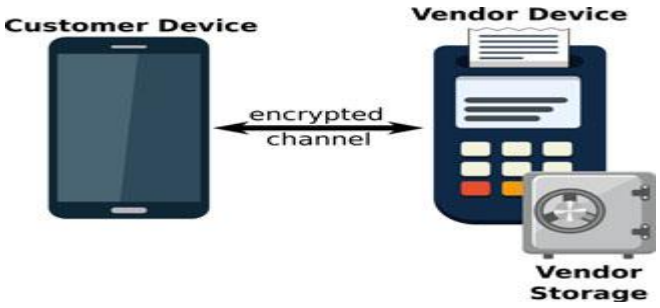

Fig-3: Frodo model

However, it is very urgent to indicate that Frodo has been proposed to be a reliable and secure encapsulation technique in terms of digital coins. This makes Frodo also applicable to various bank scenarios. Despite, as for debit and credit cards where trusted third parties (TTPs) such as card issuers includes the support the cards which is in validity, some common standard protocol can be utilized in Frodo to ensure banks capable to generate and market their own coin element. In such bank has the capacity of asserting digital coins delivered by some other banks by needing vendors and banks to accept on the same standard protocol.

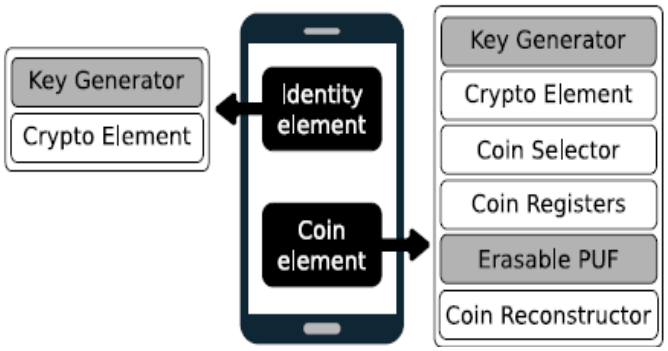

Fig-4: Frodo main architecture

3.4 Frodo Protocol

This Frodo protocol analysis about the payment protocol which is utilized in this section. It is completely depend on the Pairing and Payment phases.

3.4.1 Pairing Phase

It depend upon standard pairing protocols like as the Bluetooth passkey which is very normal pairing process. At the last stage of the pairing protocol requires both the vendor and customer devices will share their own public keys that will be applied for authenticity and data integrity.

3.4.2 Payment Phase

For providing the complete clarity in the Frodo payment protocol, it is analyzed from different points of views to in order to make the secure transactions. At the first, it is encrypted by using the private key values and then data will be exchanged between the customer and the vendor which is described in the above section. Then, from the next point of view, customer device contains the specific data which can be exchanged between the coin element and identity element. Thus proposed standard protocol is only suitable for the generation and verification of payment transactions. Once after the success transaction and all the coins elements related with the process are asserted in such way that all coins will be later on spent/redeemed by the vendor to advance the goal of the proposed protocol.

4 CONCLUSION

In this paper we have propose Frodo, to make secure and privacy transactions off-line micropayment scheme in against of Point of sale such as fraud resiliency attackers. The Frodo utilizes multiple physical unclonable functions. Frodo special features analysis coin element and the identity element to make secure authenticate for the customer, and a coin element where digital coins are not locally stored in the devices. The Frodo protocol utilized for the making the secure transaction payment which not only examine the clients coins but also authenticate the identity of the user using identify element. Our investigation proves that Frodo enhances elasticity and security and increases the effectiveness of the system by providing the secure micro-payment among the customers and vendors.

REFERENCES

[1]J.Lewandowska.(2013).[Online].Available:http://www.frost.Com/prod/servlet/press release.pag?docid=274238535

[2] R. L. Rivest, "Payword and micromint: Two simple micropayment schemes," in Proc. Int. Workshop Security Protocols, 1996, pp. 69–87.

[3] S. Martins and Y. Yang, "Introduction to bitcoins: A pseudoanonymous electronic currency system," in Proc. Conf. Center Adv. Stud. Collaborative Res., 2011, pp. 349–350.

[4] Verizon, "2014 data breach investigations report," Verizon,Tech.Rep.,2014.

[5] T. Micro, "Point-of-sale system breaches, threats to the retail and hospitality industries," University of Zurich, Department of Informatics, 2010.

[6] Mandiant, "Beyond the breach," Mandiant, 2014, https://dl.mandiant.Com/EE/library/WP_MTrends2014_140409.pdf

[7] Bogmar, "Secure POS & kiosk support," Bogmar, 2014, http://www.bomgar.com/assets/documents/Bomgar_Remote_Support_pos_systems.pdf

[8] V. Daza, R. Di Pietro, F. Lombardi, and M. Signorini, "FORCEFully off-line secure credits for mobile micro payments," in Proc. 11th Int. Conf. Security Cryptography, 2014, pp. 125–136.

[9] W. Chen, G. Hancke, K. Mayes, Y. Lien, and J.-H. Chiu, "Using 3G network components to enable NFC mobile transactions and authentication," in Proc. IEEE Int. Conf. Progress Informat. Comput., Dec. 2010, vol. 1, pp. 441–448.

[10] S. Golovashych, "The technology of identification and authentication of financial transactions. from smart cards to

NFC-terminals," in Proc. IEEE Intell. Data Acquisition Adv. Comput. Syst., Sep. 2005, pp. 407–412.

[11] G. Vasco, Maribel, S. Heidarvand, and J. Villar, "Anonymous subscription schemes: A flexible construction for on-line services access," in Proc. Int. Conf. Security Cryptography, Jul. 2010, pp. 1–12.

[12] K. S. Kadambi, J. Li, and A. H. Karp, "Near-field communicationbased secure mobile payment service," in Proc. 11th Int. Conf. Electron. Commerce, 2009, pp. 142–151.

[13] V. C. Sekhar and S. Mrudula, "A complete secure customer centric anonymous payment in a digital ecosystem," in Proc. Int. Conf. Comput., Electron. Elect. Technol., 2012, pp. 1049–1054.

[14] S. Dominikus and M. Aigner, "mCoupons: An application for near field communication (NFC)," in Proc. 21st Int. Conf. Adv. Inf. Netw. Appl. Workshops, 2007, pp. 421–428.

[15] T. Nishide and K. Sakurai, "Security of offline anonymous electronic cash systems against insider attacks by untrusted authorities revisited," in Proc. 3rd Int. Conf. Intell. Netw. Collaborative Syst., 2011, pp. 656–661.

[16] W.-S. Juang, "An efficient and practical fair buyer-anonymity exchange scheme using bilinear pairings," in Proc. 8th Asia Joint Conf. Inf. Security, Jul. 2013, pp. 19–26.

[17] M. A. Salama, N. El-Bendary, and A. E. Hassanien, "Towards secure mobile agent based e-cash system," in Proc. Int. Workshop Security Privacy Preserving e-Soc., 2011, pp. 1–6.

[18] C. Wang, H. Sun, H. Zhang, and Z. Jin, "An improved off-line electronic cash scheme," in Proc. 5th Int. Conf. Comput. Inf. Sci., Jun. 2013, pp. 438–441.

[19] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in Proc. 9th Int. Workshop Cryptographic Hardware Embedded Syst., 2007, pp. 63–80.

[20] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical oneway functions," Science, vol. 297, no. 5589, pp. 2026–2030, 2002.