ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

Preserving Micro-Payments in Deception of Resilient Devices

A.Anitha *1, R.Jagatheeswari *1,L.Lavanya *1, K.Pavithra *1,N.Sridivya *2
*1.Bachelor of Computer Science and Engineering,
sprojectmailjpa@gmail.com
*2.Assistant profDept of Computer Science and Engineering, Bharathiyar Institute of Engineering for Women.

Abstract—Credit and debit card data stealing is most popular problem in cybercrime. Slashers aim at stealing the customer data by aiming the Point of Sale systems, i.e. the point at which the vendor handle the customers data. Modern POS systems having specialized software inbuilt in card reader. Often user devices are external input to the POS. In these concepts, malware steal the card data should read by device has proliferated. Like this situation, connection between customer and vendor being intermediately stopped and there secure on-line payment is not possible. This projects providing FRODO concepts for a secure off-line micro-payment is flexible to POS data breaches. Our solution includes flexibility and security. Still, FRODO is the first solution that can provide fully secure off-line payments while being flexible to all currently known POS failures. In certain, it include FRODO architecture, components, and protocols. Thereby, a complete details of FRODO functional, security properties are provided, showing its effectiveness and viability.

Index Terms—mobile secure payment, architecture, protocols, cybercrime, fraud-resilience

1.INTRODUCTION

Mobile micro payments are famous and they are traditional in marketing fields. The classic credit card approaches may be implemented in banking such as mobile-based payments. Even though many technologies developed, many unexpected problems faced in the field for that the crypt-currencies and de-centralized payment systems are used. The first pioneering micro-payment scheme was proposed by Rivest and Shamir in 1996. Due to several unresolved problems, including a lack of widely-accepted standards, limited interoperability among systems and security the payment schemes are not get successful in the payment system.

1.1 PROBLEM ANDOBJECTIVES

The vendor have been victims of information security breaches and payment data theft targeting consumer payment card data and Personally Identifiable Information(PII).The user data can be used by the criminals for fraud operations. For improving security, the credit card and debit card holders use Payment card industry Security Standard Council. PoS system always handle critical information and requires remote management.

PoS System acts as gateways and require network connection to work with external credit card processors. However, a network connection not be available due to either a

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

temporary network service or due to permanent lack of network coverage. on-line solutions are not very efficient since remote communication can introduce delays in the payment process. Brute forcing remote access connections and stolen credentials involved in PoS intrusions.

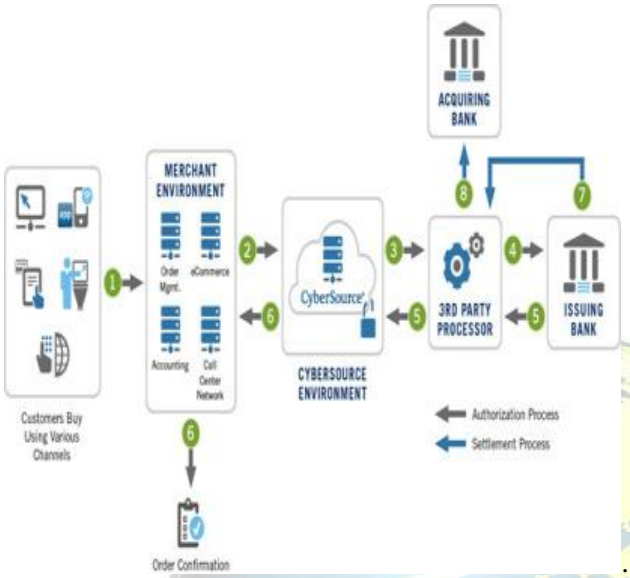

Fig.1. Payment Processing.

2. CONTRIBUTION

The FRoDO introduces a secure off-line micro-payment approach using multiple physical unclonable function. FRoDO introduces coin element and identity element. Vendor only communicate with the identity to identify the user. Identity element is used to improve the security of users.

3. BACKGROUND

Most of the payment transactions are processed by an electronic payment system(EPS). The EPS and PoS are located in same machine, where PoS is a tool used by cashier or consumer, while EPS performs all payment processing.

3.1. POS SYSTEMBREACHES

Attackers against PoS systems are muti-staged. First, attackers gain access to the victim's network called infiltration. The vendor gain access to the associated network and not directly to card-holder data environment. Install malicious software to steal data from the compromised system. PoS system have external network access, the stolen data waiting for attacker called exfiltration. POS system network-level hacking can be rendered by exploiting shared connections, open networks, or by cracking the password of the merchant's network. Networks can be monitored and protected against malicious activities. Network infiltration is one of the attack methods. In the adopted EPS model, the payment process iscomposed of two main processing phases, the authorization and the settlement. The authorization (see Fig 1) is the state of payment process where the purchase is verified and finalized. The

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

settlement comprises all actions happening after the authorization stage.

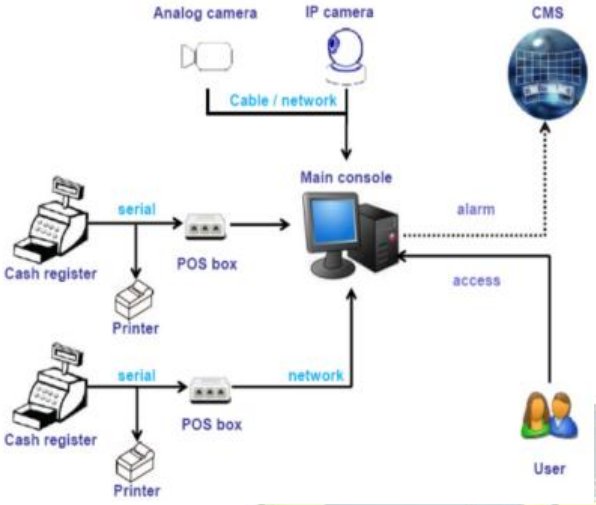

Fig.2.Point of Sale Architecture

3.2 PoS DEVICE BREACHES

POS device are the most important entities in an electronic payment system. All the attacks described and requires the POS to be connected to a network and attacker break the payment

system and infect either the POS itself or a specific component within the EPS. However, as already introduced in Section 2, EPS can also be fully off-line. In this scenario, no data is going to leave the POS and there is no way to infect the Poss. As such, breaches based on network-level hacking cannot be unleashed. However, data processed by the POS can still be eavesdropped by having physical access to the POS itself or by exploiting device vulnerabilities. In Section 4 a description of the possible breaches threatening POS systems will beprovided.

4. THREAT MODELS

Based on the capabilities and on the amount of devices that can be accessed during attack, attackers introduced as follows,

- **Ubiquitous:**It isan internal attacker who have an access to involve in all devices.
- **Collector:**It is an external attacker only exchange messages between customer and vendor device.
- **Malicious Customer:**This is an internal attacker can either physically open the customer device or inject malicious node within the customer device to hack the customer details.
- **Malicious Vendor:**This is an internal attacker that can get information from vendor device or inject malicious code into the PoS machine to alter its behaviours.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

5. PROPOSED MODEL

The Strong physical unclonable functions may perform any pre- computed challenge-response pair. Physical Unclonable Functions were introduced by Ravikanth [4] in 2001. He showed that, every transistor in an integrated circuit has slightly different physical properties that lead to measurable differences in electronic properties. 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. It 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. 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. As depicted in Figure4 ,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 thevendor.

5.1 FRoDO PROTOCOL

5.1.1 Pairing Phase

FRoDO relies on pairing protocol such as Bluetooth Passkey pairing process. The customer and vendor device will share the public key used for message integrity and authenticity.

5.2.2 Payment Phase

FRoDO Payment Protocol will be described in two different points of view. The encrypted message exchanged between vendor and customer using Identity Element and Coin Element.

6. SECURITY ANALYSIS

- **Authenticity:**For authentication process, FRoDO used computation of private keys. The coin element and key element use key generator to compute private key needed to encrypt and decrypt all messages exchanged in the protocol.
- **Non-denial:**By deleting past transactions and keep the storage device physically safe. The content of storage device is backed up and exported to secondary devices.
- **Confidentiality:**To achieve confidentiality, communication between customer and vendor message is encrypted.

6. ATTACK MITIGATION

To improve the security of whole payment system two different elements will be using by FRoDO. They are coin element and identity element. The vendor device does not directly communicate with the coin element but has to go through the identity element.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

On the other hand, the identity element can be used to fight against attackers, if an identity element is considered as malicious and is blacklisted, the device used by user, any coin will not be accepted and processed by the vendor.

7.CONCLUSION

FRODO introduces off-line micro payment approach for data-breaches. FRoDO does not impose trustworthiness but has customer satisfaction . FRoDO is highly secure micro-payment solution. And also introducing flexibility in payment medium. To improve the level of security and usability multiple off-line transaction are allowed in the transaction. The current off-line solution adopt a withdrawal-phase producing tokens which are pre-computed and pre-cached within a device. Thus FRoDO is secure and flexible for consumer.

REFERENCES

[1] V. Daza and R. Di Pietro, "FORCE -Fully Off-line secuReCrEdits for Mobile Micro Payments," in SCITEPRESS, 2014.
[2] W. Whitteker, "Point of Sale (POS) System and Security," SANS Institute InfoSec Reading Room, 2014.
[3] U. Rhrmair and C. Jaeger,"An attack on PUF-Based Exchange and a Hardware-based Countermeasure:Erasable PUFs," in LNCS 2012.
[4] B. Kori and P. Tuyls, "Robust key extraction from physical uncloneable functions," in Applied Cryptography and Security, 2005.
[5] G. Van Damme and H. Karahan, "Offline NFC Payments with Electronic Vouchers," in MobiHeld, 2009.
[6] Yalin Chen and Jue Sam Chou, "User Efficient Recoverable Off-line E-cash Scheme with Fast Anonymity revoking," in International Journal of Network Security, 2015.
[7] DebasisGiri and ArpitaMazumdar, "A Secure Offline Electronic Payment System Based on Bilinear Pairings and Signcryption,"in IJSCE, 2013.
[8]]T. Nishide and K. Sakurai, "Security of offline anonymous electronic cash systems against insider attacks by untrusted authorities revisited," ser. INCOS '11. Washington, DC, USA: IEEE Comp. Soc., 2011, pp. 656–661.
[9] ChitraKiran.N , Narendra Kumar .G, Suchitra Suresh, "'Prototype Framework of Mobile -to-Mobile Payment System for effective Security," Proceedings of 07th International conference , India, ISBN, 2014.
[10] Jan Solter and Frank Sehnke,"Modeling attacks on Physical Unclonable functions," ser, ACM CCS;10 , 2010,pp.237-249.
[11] [13] V. C. Sekhar and S. Mrudula, "A Complete Secure customer centric anonymous payment in a digital ecosystem," ICCEET 12, 2012.
[12] G. Vasco, Maribel, S. Heidarvand, and J. Villar, "Anonymous subscription schemes: A flexible construction for on-line services access," in Security and Cryptography (SECRYPT) , July 2010.
[13]]S. Golovashych, "The technology of identification and authentication of financial transactions. from smart cards to NFC-terminals," in IEEE Xplore Conference: IDAACS: Technology and Applications, 2005.IEEE.
[14]]Trend Micro Incorporated, "Point-of-sale system breaches," A Trend Micro Research Paper, 2014.[15] Bomgar, "Secure POS & Kiosk Support with Bomgar," Technical Report,2014