International Journal
of Computer Sciences
ISSN Number: 4142 3453

Fraud Resilient Mechanism for Digital Payments Using Coin Management

Kata Chandrakanth[1], P. Krishnaiah[2]

[1]M.Tech (CSE),PG Scholar ,Department of CSE, Srinivasa Institute of Technology and Science Kadapa,AP.

[2]Associate Professor ,Department of CSE, Srinivasa Institute of Technology and Science Kadapa,AP.

Abstract- Credit and debit card data theft is one of the earliest forms of cybercrime. It is one of the most common problems now days. Attackers often aim at stealing such customer data by targeting the Point of Sale system, i.e. the point at which a retailer first acquires customer data. Modern Point of Sale systems are powerful computers equipped with a card reader and running specialized software. Increasingly often, user devices are leveraged as input to the Point of Sale. 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. A secure online micro-payment solution that is resilient 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 solution that can provide secure fully on 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 strong

Keywords: Mobile secure payment, architecture, protocols, cybercrime, fraud-resilience, Securit

1. INTRODUCTION

Nowadays online payments are one of the most popular, when the customer or buyer makes his payment transactions for the goods purchased with the use of the online money payment. In that the purchase methods from classic credit or debit cards to new approaches like mobile-based payments, giving new market entrants novel business probabilities. However, many of us still resist the attractiveness and ease of revolving credit transactions because of security issues. so far there are a high risk for taken cards, fraud so the purchasers worry debit-card fraud by merchants and different third parties. Payment transactions are usually processed by an electronic payment system (for short, EPS). The EPS is a separate function from the typical point of sale function, although the EPS and PoS system may be co-located on constant machine. In general, the EPS performs all payment process, whereas the PoS system is that the tool utilized by the cashier or shopper. Point of Sale is the time and place where a retail exchange is finished . At the point of sale, the dealer would set up a receipt for the client or generally figure the sum owed by the client and give choices to the client to make payment. In these transaction process, there is chance to attackers often aim at stealing such customer data by targeting the Point of Sale. Modern PoS systems are powerful computers equipped with a card reader and running specialized software. Increasingly typically, user devices are utilized as input to the PoS. In these scenarios, malware that can take card information when they are read by the device has thrived. So that we proposed FRODO techniques, a safe disconnected from the net transaction arrangement that is strong to PoS information breaches. Our solution enhances over exceptional methodologies as far as adaptability and security. The main objective of this project is to encrypt user's sensitive data when users payment processing takes place. This will ensure that the third party pos vendors or merchants can't able to see user's personal data like card no cvv number etc. This will be only visible to bank admin where they either accept or deny the payments. 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 on line micropayment 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 on 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

II. LITERATURER SURVEY

Mobile payment solutions proposed so far can classified as totally on-line [2] semi off-line [6], weak off-line or totally off-line [10]. The most issue with a totally off-line approach is that the problem of checking the trait of a dealings while not a trusty third party. In fact, keeping track of past transactions with no out there association to external parties or shared databases is quite tough, because it is tough for a trafficker to ascertain if some digital coins have already been spent. This is often the most reason why throughout previous couple of years, many alternative approaches are planned to produce a reliable offline payment theme. Though several works are revealed, all of them targeted on dealings namelessness and coin unforgeability. The introduction to security issues & its concern is described in previous section. In this literature we have studied earlier research papers related to conventional authentication systems it presents single time authentications of the user. The categorizations of security systems are

depend on strength of attack and are classified into strong and weak. The summarizing study of earlier The paper introduces a novel offline payment system in mobile commerce using the case study of micro-payments. The present paper is an extension version of our prior study addressing on implication of secure micropayment system deploying process oriented structural design in mobile network. The previous system has broad utilization of SPKI and hash chaining to furnish reliable and secure offline transaction in mobile commerce. However, the current work has attempted to provide much more light weight secure offline payment system in micro-payments by designing a new schema termed as Offline Secure Payment in Mobile Commerce (OSPM). The empirical operation are carried out on three types of transaction process considering maximum scenario of real time offline cases. Therefore, the current idea introduces two new parameters i.e. mobile agent and mobile token that can ensure better security and comparatively less network overhead. Limited interfaces and location within local networks, supporting kiosks and point of sale (POS) terminals can be challenging. Often they are located on networks that are not connected to the internet, making direct access impossible for most remote support tools. And even when an employee is present at the terminal, access restrictions and/or lack of technical knowledge makes communicating the solution to a problem difficult. To add complications, hackers are ramping up their efforts to steal payment card data by gaining access to POS systems and kiosks. A lightweight and secure key storage scheme using silicon Physical Unclonable Functions (PUFs) is described. To derive stable PUF bits from chip manufacturing variations, a lightweight error correction code (ECC) encoder / decoder is used. With a register count of 69, this codec core does not use any traditional error correction techniques and is 75% smaller than a previous provably secure implementation, and yet achieves robust environmental performance in 65nm FPGA and 0.13µ ASIC implementations. The security of the syndrome bits uses a new security argument that relies on what cannot be learned from a machine learning perspective. The number of Leaked Bits is determined for each Syndrome Word, reducible using Syndrome Distribution Shaping. The design is secure from a min-entropy standpoint against a machine-learningequipped adversary that, given a ceiling of leaked bits, has a classification error bounded by ε. Numerical examples are given using latest machine learning sults.

Vanesa Daza ; Roberto Di Pietro ; Flavio Lombardi ; Matteo Signorini Abstracts: Payment schemes based on mobile devices are expected to supersede traditional electronic payment approaches in the next few years. However, current solutions are limited in that protocols require at least one of the two parties to be on-line, i.e. connected either to a trusted third party or to a shared database. Indeed, in cases where customer and vendor are persistently or intermittently disconnected from the network, any online payment is not possible. This paper introduces FORCE, a novel mobile micro payment approach where all involved parties can be fully off-line. Our solution improves over state-of-the-art approaches in terms of payment flexibility and security. In fact, FORCE relies solely on local data to perform the requested operations. Present paper describes FORCE architecture, components and protocols. Further, a thorough analysis of its functional and security properties is provided showing its effectiveness and viability.

Continuous and Transparent User Identity Verification for Secure Internet Services Authors: Andrea Ceccarelli ; Leonardo Montecchi ; Francesco Brancati ; Paolo Lollini ; Angelo Marguglio ; Andrea Bondavalli Abstracts: Session management in distributed Internet services is traditionally based on username and password, explicit logouts and mechanisms of user session expiration using classic timeouts. Emerging biometric solutions allow substituting username and password with biometric data during session establishment, but in such an approach still a single verification is deemed sufficient, and the identity of a user is considered immutable during the entire session. Additionally, the length of the session timeout may impact on the usability of the service and consequent client satisfaction

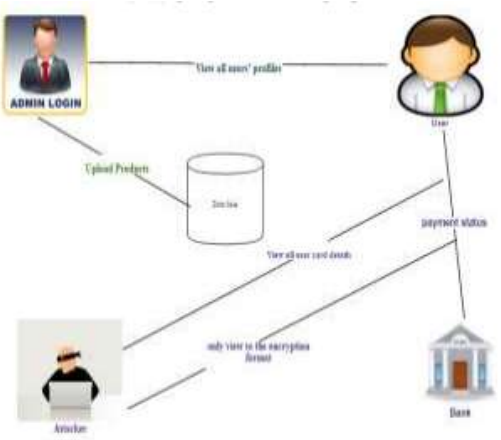
III. EXISTING SYSTEM

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 handles critical information and requires remote management. PoS System acts as gateways and requires network connection to work with external credit card processors. However, a network connection not be available due to either a temporary network service or due to permanent lack of network coverage. on solutions are not very efficient since remote communication can introduce delays in the payment process. Brute forcing rims in PoS intrusions. In the present system, we do online payments via providing our credit / debit card details or swipe our card in the vendor place where our personal data can be identified by the POS vendors and might steal our information. This breaches the security of our micro payments and causes a serious issue.Further this current scenario may mislead the user's potential information and can also be used to make duplicate credit or debit cards where the main information can be gathered at the POS area.

IV. PROPOSED WORK

In the proposed system we developed a novel algorithm that is current working scenario. We encrypt the entire user's personal data that is acquired via swiping using an encrypted hash key mechanism. This increases the overall security when we use any micro payments or swipe cards at the point of scale vendor's .The information acquired by the end users will be seen as a cipher text if any potential intruders attack the system. The information can only be visible to the bank area and needs to process the payment on the basis of POS

International Journal
of Computer Sciences
ISSN Number: 4142 3453



Client Module This module used to client are 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, warrenty period,etc., and admin view all users purchase products but cannot view user account details. and to view which product is delivered or not. 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. Availability The availability of the proposed solution is guaranteed mainly by the fully off-line scenario that completely removes any type of external communication requirement and makes it possible to use off-line digital coins also in extreme situations with no network coverage. Furthermore, the lack of any registration or withdrawal phase, makes FRoDO able to be used by different devices. Confidentiality Both the communications between the customer and the vendor and those between the identity element and the coin element leverage asymmetric encryption primitives to achieve message confidentiality. 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 equipment, such as pen drives, in order to make it even harder for an adversary to tamper with the transaction history Login:Here admin can directly login for the home page to see the all details about the users and bank accounts details. View all users' profiles:Here also admin view all Users profiles in a list and one by one can view also and about users all information can read. Upload Products:Here only admin can see about the product that one upload and download the product. Admin handle the all activity of the System. Who is uploading the product with name and time and date? View all Products:And here admin can view the all product list with name and with user name and time and date. So this is very useful to know the all product and handle the system. Who is one doing activity and user user uploading name. Payments status:And this sub module inside admin can see the payment status of users who is done payments and full information of payments which time user done own payment with date Finally logout the website BANK Inside of this module three sub modules available Login:Here Bank user can login for the view user request payment and sent one Acknowledgement and transfer the amount. View user request payments (bank has a decrypted key):Here Bank can view user request payments and bank has decrypted key also For the user information. So attackers cannot read the data that's why bank security very strong

V. RESULT AND DISCUSSIONS

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple.

The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things: What data should be given as input? How the data should be arranged or coded? The dialog to guide the operating personnel in providing input. Methods for preparing input validations and steps to follow when error occur.

OBJECTIVES

1.Input Design is the process of converting a useroriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3.When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

OUTPUT DESIGN A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements. 2.Select methods for presenting information.

3.Create document, report, or other formats that contain information produced by the system. The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action

VI.CONCLUSION

We have introduced FRODO that is, to the best of our knowledge, 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 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.

REFERENCE

[1]. Vanesa Daza, Roberto Di Pietro, Flavio Lombardi, And Matteo Signorini "Frodo: Fraud Resilient Device For Off-Linmicro-Payments", Dependable And Secure Computing, IEEE Transactions On (Volume:PP , Issue: 99), 12 June 2015

[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 Incorporated, 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 secuReCrEdits 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 network 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.

[11]. C. R. Group, "Alina & Other POS Malware," Cymru, Technical Report,2013.

[12]. N. Kiran and G. Kumar, "Reliable OSPM schema for secure transaction using mobile agent in micropayment system," in ICCCNT 2013, July 2013, pp. 1–6.

[13]. S. Gomzin, Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions, 1st ed. Wiley Publishing, 2014.

[14]. C. Wang, H. Sun, H. Zhang, and Z. Jin, "An improved off-line electronic cash scheme," in ICCIS 2013, June 2013, pp. 438–441.

[15]. C.-I. Fan, V. S.-M. Huang, and Y.-C. Yu, "User efficient recoverable off-line e-cash scheme with fast anonymity revoking," Mathematical and Computer Modelling, vol. 58, no. 12, pp. 227 – 237, 2013.

[16]. 1M.-D. Yu and S. Devadas, "Secure and robust error correction for physical unclonable functions," Design Test of Computers, IEEE, vol. 27, no. 1, pp. 48–65, Jan 2010.