www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 3 March 2017, Page No. 20699-20704
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i3.54

Fraud Resilient Device Offline Micro-Payments using Bit-Exchange Algorithms

R.Bargavi, Dr. L.Jaba Sheela

Student , Department of Computer science and engineering, Panimalar engineering college chennai,India

ravibharkavi@gmail.com

Professor Department of Computer science and engineering ,Panimalar engineering college,India

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, Security*

1.INTRODUCTION

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 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 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.

2.OBJECTIVE

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.

3.LITERATURE SURVEY

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 research is as follows:

FORCE: Fully off-line secure credits for mobile micro payments[8]

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 on-line 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.

Algorithm:

- FORCE
- Secret key extraction Algorithm

Disadvantages:

They are limited to customer authentication whilst blindly relying on trusting the bank for transactions (as for credit cards).

- The problems affecting digital currencies, such as digital change, are beyond the scope of the proposed solution and will not be analyzed here.

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.

- **Algorithm:**
- CASHMA Authentication
- Continuous Authentication Algorithm
- **Demerits:**
- Device Cost High.
- CASHMA some time misbehave.

A Survey on Continuous User Identity Verification Using Biometric Traits for Secure Internet Services

Authors: Harshal A. Kute1, D. N. Rewadkar2

Abstracts: Security of the web based services is become serious concern now a days. Secure user authentication is very important and fundamental in most of the systems User authentication systems are traditionally based on pairs of username and password and verify the identity of the user only at login phase. No checks are performed during working sessions, which are terminated by an explicit logout or expire after an idle activity period of the user. Emerging biometric solutions provides substituting username and password with biometric data during session establishment, but in such an approach still a single shot verification is less sufficient, and the identity of a user is considered permanent during the entire session. A basic solution is to use very short session timeouts and periodically request the user to input his credentials over and over, but this is not a definitive solution and heavily penalizes the service usability and ultimately the satisfaction of users. This paper explores promising alternatives offered by applying biometrics in the management of sessions. A secure protocol is defined for perpetual authentication through continuous user verification. Finally, the use of biometric authentication allows credentials to be acquired transparently i.e. without explicitly notifying the user or requiring his interaction, which is essential to guarantee better service usability.

- **Technique:**
- Biometric Device
- **Demerits:**
- Cost High (biometric device)

Hacking Point of Sale: Payment Application Secrets Threats and Solutions

Authors: S. Gomzin

Abstracts: Nearly five million point-of-sale (POS) terminals process about 1,500 credit and debit card transactions every second in the United States alone. 1, 2, 3 Most of these systems, regardless of their formal compliance with industry security standards, potentially expose millions of credit card records—including those being processed in memory, transmitted between internal servers, sent for authorization or settlement, and accumulated on hard drives. This sensitive data is often weakly protected or not protected at all. It is just a matter of time before someone comes along and takes it away.

Algorithm:

- 3DES

Disadvantages:

it's possible to brute-force in finite time on modern processors, so no-one uses it for anything serious anymore. Also, some password systems secured with 3DES were limited to 8 characters and would silently truncate otherwise-secure passwords (match only the first 8 characters).

IV.OVERVIEW

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.

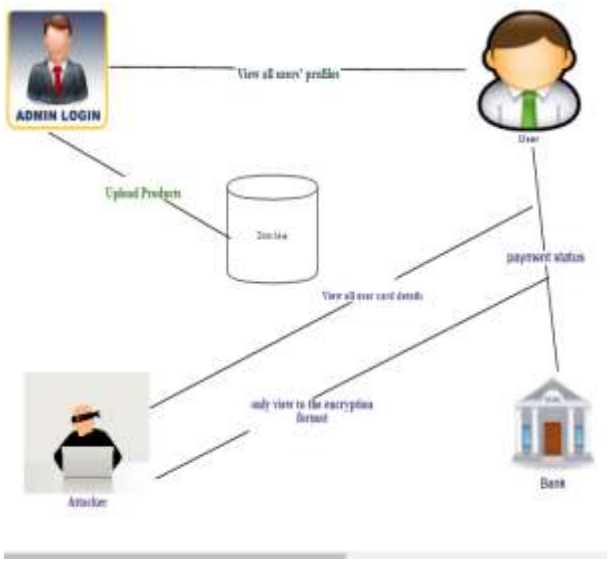
V. EXISTING SYSTEM

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.

VI.PROPOSED SYSTEM:

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 profiling.

VII. SYSTEM DESIGN



ADMIN

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.

Sent one acknowledgement and transfer the amount:Bank first gives the acknowledgements to users after that transfer the amount to bank and Logout.

User

Register:First user registration must with all information after that user can login.

Login:This is second step to user after registration here user can login for account details and can view all products details.

View all products:Here only user can view the products details so this is the sub module of user module.

Buy:Buy sub module of user module this is using for buy the product and after reach the payment details so here all detail put about the product.

Transfer amount (all card details encryption)

After Buy sub module next sub module Transfer amount so here all data about user card detail sends in encrypted form.

Attackers

Login:Attackers first get information about user login and password after hack The details of user so this is first step to attack. View all user card details (but only view to the encryption)

This step happens at the time of user doing transaction that time. At transaction Time one session time is start so that session only limited time that time only transaction can done if session time expire then cannot happen transaction so attackers also try to use that session time that time easily they can hack all information with transaction.

VIII. IMPLEMENTATION DETAILS

The algorithmic details & techniques used in system in experimentation are explained here. The different algorithmic strategies & technique is used

Bit Exchanging Method:

Encryption taken on the secret message file using simple bit shifting and XOR operation.

The bit exchange method is introduced for encrypting any file.

Algorithm

Step 1:Read the all Content and Find the all character to covert the ASCII value

Step 2:That ASCII value converted in Binary value

Step 3:Encryption taken on the secret message file using simple bshifting and XOR operation. Like a 1001110.

Step 4:The bit exchange Method is introduced for encryption any file

Step 5:Read one by one byte from the secret data and convert each byte to 8 bits. Then apply one bit right shift operation. Like this 0100 1110.

Step 6:Divide the 8 bits into to block and then perform XOR operation with 4 bit on the left and 4 bits on the right side (1010).

Step 7:The same thing repeated for all bytes in the file.

IX. PAYMENT PHASE

The FORCE payment phase is depicted in Figure 1.2 and it is composed by the following steps

1. The customer sends a purchase request to theVD asking for some goods;

2. The vendor computes the total amount and sends it back to the customer;

$$Enc_{Salt}(Req)=C_{Req}$$

3. The customer checks for the amount and either confirms or denies the transaction. If the transaction is confirmed, the CD creates a reply for the VDwith the indexes of all the credits that are still available in the card. If the ith index number is present in the reply, it means that the ith credit register can be read in order to retrieve the ith digital credit within the card;

3) Once the private request has been built, it is sent to the customer;

$$Enc_{IeSK}(Req)= PrReq$$

4) 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.

5)Once the coin request is in plain-text, the value of the coin is retrieved from the coin element (as depicted in Fig. 11). 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 the authenticity of the response) and at the end with the public key of the vendor—to ensure that only the right vendor device can decrypt

$$Dec_{VPK}(PrivateResponse)=EncValue$$

6) The coin value has now to be encrypted twice. The first encryption layer is needed in order to prove the authenticity of the coin. The second encryption layer is needed such that only the right identity element will be able to read

7) The response is encrypted with the private key of the card thus providing authenticity and integrity

The vendor decrypts the *ERes* in two steps

$$Dec_{CPK}(ERes) = Res$$

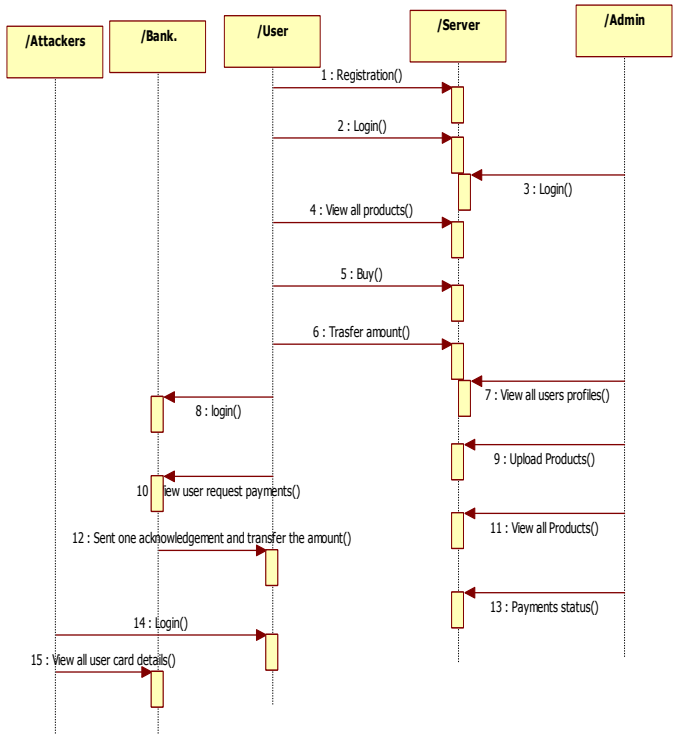
$$Dec_{Salt}(Res) = CreditVal$$

8) Finally the content of the credit is decrypted with the public key of the bank/card issuer

$$Dec_{BPK}(CreditVal) = FRes$$

9). Now that all messages exchanged between the customer

and the vendor device have been introduced, it is possible to show how the identity and the coin elements interact:If the credit value is correct, a new entry is stored in the storage device of the vendor after having being encrypted with the private key.



FORCE payment phase is depicted in Figure 1.2

X. INPUT DESIGN

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 user-oriented 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

RESULTS :

ATTACKER	Data in Transit	Data at Rest	Data in Memory
Off-line NFC payments with electronic vouchers	✓	•	•
An anonymous fair off-line micro-payments scheme	✓	•	•
User efficient recoverable off-line e-cash	✓	•	•
Efficient and practical fair buyer-anonymity exchange scheme	✓	•	•
FRoDO - Fraud Resilient Device for Off-line micro-payments	✓	•	•
Fraud Resilient Device Offline Micro-Payments using Bit-Exchange Algorithms	✓	✓	✓

X1.CONCLUSION:

In this project we have introduced FRODO that is, to the best of our knowledge, the first data-breach-resilient fully online micropayment approaches. 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. 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 on line transactions while maintaining the same level of security and usability.

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 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.

Author Profile

R.Bargavi is a B.E student from Computer Engineering Department, Panimalar Engineering college at Chennai Having interest in Cyber Security