International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 07
June 2017

Device Resolving Frodo for Payments Micro Descalcified

1. K YAMINI 2. B.N.V. MADHUBABU 3. DR. K NAGESWARARAO

[1]Pg Scholar, Department of CSE, Mother Teresa Institute of Science and Technology, Sathupally
kumpatiyamini@gmail.com

[2]Associate Professor , Department of CSE, Mother Teresa Institute of Science and Technology, Sathupally
bnvmadhubabu2014@gmail.com.

[3]Professor & HOD, Department of CSE, Mother Teresa Institute of Science and Technology, Sathupally
nageswararaokapu@yahoo.com.

Abstract— Credit and debit card data theft is one of the earliest forms of cybercrime. Still, it is one of the most common now a days.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.

I.INTRODUCTION

Credit and debit card data theft is one of the earliest forms of cybercrime. S till, 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 online 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.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 offline secure credits for mobile micro payments[8]

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 online, 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 offline. 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.

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.

III 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.

IV PAYMENT PHASE

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

1. The customer sends a purchase request to the VD 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;EncIeSK(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). 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 c an decrypt 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 stepsDecCPK(ERes) = Res DecSalt(Res) =CreditVal8)Finally the content of the credit is decrypted with the public key of the bank/card issuer DecBPK(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

V SECURITY ANALYSIS

In this section the robustness of FRoDO is discussed. FRoDO uses both symmetric and asymmetric cryptographic primitives in order to guarantee the following security principles: Authenticity. It is guaranteed in FRoDO by the onthefly 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 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; Integrity. It is ensured with the encryption of each digital coin by the bank or identity/coin element issuer. Coin seeds and coin helpers are written into the coin element registers by either the bank or coin element issuer such that the final coin value given as output corresponds to an encrypted version of the real digital coin. As such, by using the public key of the bank or identity/coin element issuer, it is always possible to verify the integrity of each coin. Furthermore, the integrity of each message exchanged in the protocol is provided as well. In fact, both the identity and the coin element use their private/public keys. The private key is not stored anywhere within the identity/ coin element but it is computed each time as needed. 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 (details in 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. As FRoDO shares the assumption that each element built on top of a PUF is tamper-evident. This assumption is based on the size of nowadays integrated circuits (for short, IC) and on the impossibility for a casual attacker to open the device without causing an alteration in PUF behavior. This assumption is no longer valid if an expert attacker with access to highly sophisticated and expensive tools, such as scanning electron microscopes or focused ion beams, is taken into account. However, such tools can cost thousands of dollars and applying this kind of attack on each single device to steal a few dollars doesnot provide an incentive to attack the system.

VI CONCLUSION

In this paper we have introduced FRoDO that is, to the best of our knowledge, the first data-breach-resilient fully offline micro-payment 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.

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.

[26] R. T. Collins, "Mean-shift blob tracking through scale space," in Proc. IEEE Comput. Soc. Conf. CVPR, Jun. 2003, pp. II-234–II-240.