isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6 Issue: 2 Dec,2016,ISSN_NO: 2321-3337

REMD: Racket Eradicate Mechanism Designed for On-line Operating Cost

S.r. ranjith
Department of CSE
Panimalar engineering college
Chennai,india
ranjithrajendrann@gmail.com

K.Gunasekaran
Assistant professor
CSE DEPARTMENT
Panimalar Engineering College
karguna.it@gmail.com

ABSTRACT:

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 REMD, 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, REMD 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 REMD architecture, components, and protocols. Further, a thorough analysis of REMD functional and security properties is provided, showing its effectiveness and viability.

Keywords-mobile secure payment, architecture, algorithm,racket-resilience

INTRODUCTION-

A user can efficiently recover the e-cash scheme in off-line with fast anonymity revoking is proposed recently they focused on security requirements of e-cache system such as anonymity, unlink ability, double sending, checking and rapid anonymity revoking on double sending. The market analysts have predicted that the mobile payment will overtake the traditional marketplace thus providing a greater enhance to the customer and a new idea of source to the company like mobile based payment with a new market entrant's novel business chance this idea is widely supported by using hardware firstly the mobile payment is in the early stage of evolution for the enhancement of this growing interest in the crypto-currencies. The first pioneering micro-payment scheme was proposed by Rivets and Shamir in 1996.crypto-currencies and decentralised payment systems are increasingly popular Truly unalienable tokens (PUFs) were introduced These are so complex that it is infeasible to fully read out the data contained in a token or to make a computer model that predicts the outputs of a token This

makes PUFs suitable for online protocols as well as verification involving physical probing by untrusted devices. A PUF is a physical system designed such that it interacts in a complicated way with stimuli (challenges) and leads to unique but unpredictable responses. A PUF challenge and the corresponding response are together called a Challenge-Reponses-Pair (CRP). A PUF behaves like a keyed hash function; The physical system consisting of many `random' components is equivalent to the key. Inorder to be hard to characterize, the system should not allow evident extraction of the relevant properties of its interacting components by measurements. Physical systems that are produced by an uncontrolled production process, e.g. Random mixing of several substances, turn out to be good candidates for PUFs.Because of this randomness, it is hard to produce a physical copy of the PUF.Furthermore, if the physical function is based on many complex interactions, then mathematical modelling is also very hard. The prior research work has almost focused on providing security for online payment system. But the need of security for offline payment system has been highlighted in my previous work. The investigation for m-payment has attracted the researchers for long time and has also posted significant issues in m-commerce to build its security. It has been seen that in the current mobile payment system, the third party and the financial institutions are considered to be trustworthy and reliable while there is not much focus on the internal threats by any untrusted party. However, there is always feasibility that the employees of any financial institutions might pose a lethal threat sometimes. micropayments, exceptional is required, otherwise the cost of the mechanism will exceed the value of the payments. As a consequence, our micropayment schemes are light-weight compared to full micropayment schemes. We \don't sweat the small": a user who loses a micropayment is similar to someone who loses a nickel in a candy machine. Similarly, candy machines aren't built with expensive mechanisms for detecting forged coins, and

yet they work well in practice, and the overall level of abuse is low. Large-scale and/or persistent fraud must be detected and eliminated, but if the scheme delivers a volume of payments to the right parties that is roughly corrected, it is critical to evaluate security in payment system in terms of the internal threats and attacks by some untrusted parties if the mobile cash system is deployed in real time. it has become standard business

their developed IP blocks. This is only guaranteed if designs are properly protected against theft, cloning, and grey market overproduction. Cryptography traditionally,
string, nor does it get reproduced precisely each time it is measured. Similarly, a long pass-phrase (or answers to 15 questions [9] or a list of favourite movies) is not uniformly random and is difficult to remember for a human user. For many applications that need to identify and authenticate users,system security is based on the protection of secret
store, and reliably retrieve such strings. Strings that are neither uniformly random nor reliably reproducible seem to be more plentiful. For example, a random person's fingerprint or iris scan is clearly not a uniform random
relies on uniformly distributed random strings for its secrets. Reality, however, makes it difficult to create

RELATED WORKS-

Yalin Chen. *et al*., 2012 [1] Crypto-analyses on user efficient recoverable off-line e-cash's scheme with fast anonymity revoking the methodology is to withdrawal the Payment Protocol and the bank can be authenticating the user through a secure channel in this project the enhancement about Security such as verifiability and Unforgettably is achieved and the problem addressed is Suffers from Likability and Identity Leakage.

Ulrich Ruhrmair. et al., July 2013 [2] Modelling Attacks on Physical Inclinable Function in this project the problem issued is Machine Learning output is difficult and more CRP's needed. And the advantage of this paper is Security is achieved by PUF designers. To enhance the idea, the implementation of CRPs obtained from real PUFs are subject to noise and random error is done due to its complex of disorder structure a PUF can avoid some of the shortcoming associated with digital keys.

Ulrich Ruhrmair. et al., Nov 2012 [3] PUFs in Security Protocols: Attack Models and Security Evaluations and the problem addressed in this project is about New attack models and Security Definitions must be developed. The merits about the paper is the searcher Used to protect Secret Keys. To enhance from this paper is to get through from Bad PUF model and challenge-logging PUFs. Physically obfuscated key is used by the pok.

VanesaDaza. Et al., July 2011 [4] Fully Off-line Secure Credits for Mobile Micro Payments(FORCE) the problem addressed in this project is Allows each off-line credit to be spent once. And the merits discussed in this paper is Mobile Micro Payment were users can be fully off-line. The enhancement which is covered is Scribed how our solution provides a higher security Level without any trust worthiness assumption over the Devices involved in the payment protocol.

practice to include third party Intellectual Property (IP) into products. This trend has led to the realization that internally developed IP is of strategic importance, for two reasons: (i) it decreases the design cycle by implementing re-use strategies and (ii) it is a source of additional licensing income from external parties. However, licensing IP to external parties' forces IP vendors to ensure that they can generate revenues from

Ey up S.Canlar . et al. 2013, [5] Windows Mobile LiveSD Forensics the problem we faced in this paper is Reconstruction of file system from raw dump of EEPROM and the advantage about this paper is that Perform on-device live data acquisition in which efficiency is achieved. To enhance the paper This new methodology is based on an in-house developed application that acquires evidence from the RAM. it also leverages HaRET, which is used to boot into Linux, to acquire the evidence on the EEPROM.
Roberto Battistoni,. Et al., 2011 [6] A Live Digital Forensic system for Windows networks the problem issued in the project is FOXP agent and FOXP Management Console have not been implemented. Supports network LDF and detecting malicious activities at kernel level. The enhancement done in this is project isTested this construction on FPGAs with embedded in block RAM memories which is not reset at power-up.

W. Paul Griffin. Et al., May 2012 [7] Circuit Level IC Protection Through Direct Injection of Process Variations the problem issued in this project is to proceed only if the unlocking key is correct. And the merits is Separate the internal key used from external unlocking key and security is achieved.to enhance we notice that the unique identifiers derived from the PUFs could be useful for tracking purposes.

B.Skorie. Et al.,2007 [8] Robust Key Extraction from Physical Uncloneable Function the problem issued in this project is Approximation is not clear. And the methodology used in this project is Robustness of bit-string extraction is improved. Also in this project the enhancement is about Reveal the location as well as the structure here the data is generated during the enrolment and applied at the time of verification.

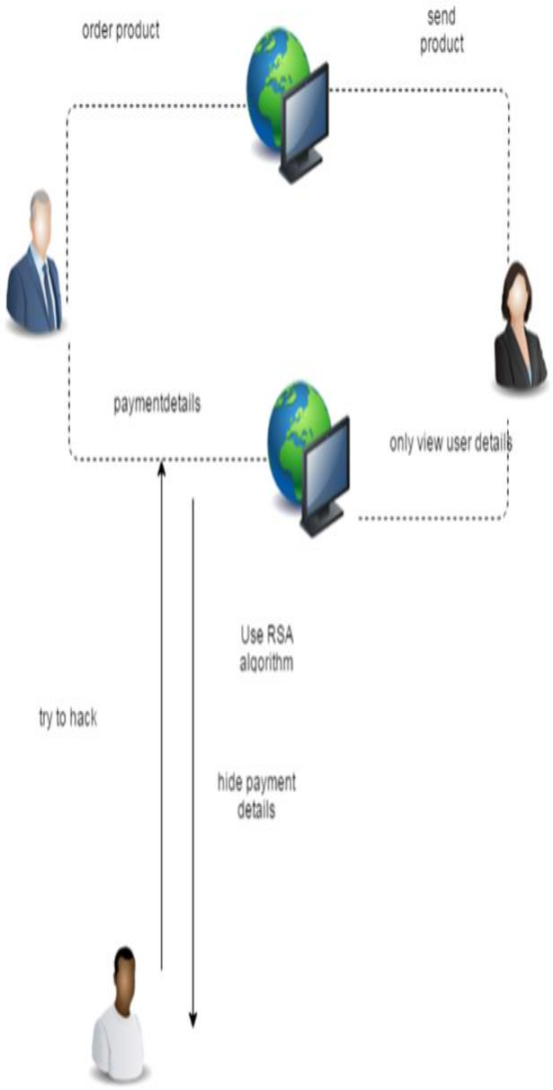
Daihyun Lim,. Et al., Oct 2005 [9] Extracting Secret Keys From Integrated Circuits the problem issued in this project is Environmental variations such as temperature and power supply voltage variations are the primary causes of noise in PUF responses. According to the merits Arbiter-based PUF's are realizable and amount of delay variation is measured.the enhancement is about the test chip was builted in TSMC's 0.18-m, single-poly, six-level metal process with standard cells in this extraction

Chaitra Kiran N . Et al., 2011 [10] Reliable OSPM Schema for Secure Transaction using Mobile Agent in Micropayment System the problem faced in this project is that Hash value is been needed. And the merits about this paper is Ensure better security and less network overhead. The enhancement in this project is OSPM

scheme thereby renders a novel, cost-effective, and secure network with better business role in m-commerce.

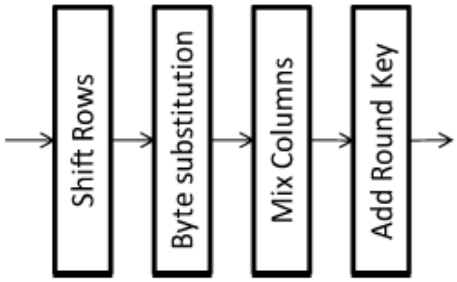
SYSTEM MODEL-

In this model customer order a product and the dealer send the product after the payment during the payment the transaction is done in secret manner where the hacker can get the security code and documentation initialization process and from that array key expansion is done. Thus the keys formed total W43 which are used further for next 10 rounds. Each round uses 4 word key along with plaintext/cipher textEach Round consists of mainly 4 phases, mainly of four different transformations: SubByte, ShiftRow, Mix
Column and key addition (xoring) and same at decryption same inverse transformation is their InvSubByte, InvShiftRow, InvMixColumn, and key addition.



AES ALGORITHM

This AES is one of the four current algorithms proposed under NIST.AES performs bulk encryption of information as ECB code type.AES is a symmetric algorithm which process 128bit stream in 10 rounds. It is symmetric algorithm as it uses same key for encryption and decryption. It uses 4 stage structures in single round to form a cipher text for respective round

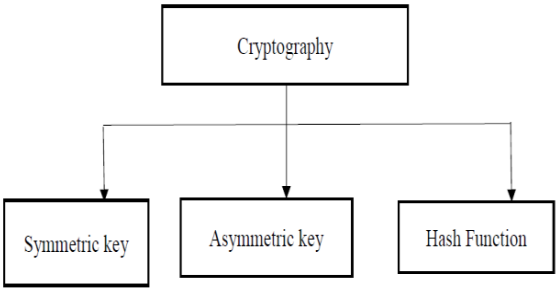


The basic unit of AES algorithm process is a byte and this algorithm is based on Substitution Permutation network it means it has series of linked mathematical operations. AES consist of two dimensional array called as state. The AES algorithm is basically used in ATM machines for security of transactions .It is also used in Windows Vista fault analysis program software to provide configuration file security.AES mainly implemented in many platforms of languages i.e. Matlab, C and Java, but as for reconfiguration purpose we propose design for FPGA i.e. in VHDL language. This is somewhat useful for direct hardware implementation and synthesis as by using RTL and Technical Views at the time of simulation gives brief idea for logic capacity and CLBs.

RSA ALGORITHM

The RSA algorithm is one of the most commonly used efficient cryptographic algorithms. It provides the required amount of confidentiality, data integrity and privacy. This paper integrates the RSA Algorithm with round-robin priority scheduling scheme in order to extend the level of security and reduce the effectiveness of intrusion. It aims at obtaining minimal overhead, increased throughput and privacy. In this method the user uses the RSA algorithm and generates the encrypted messages that are sorted priority-wise and then sent. The receiver, on receiving the messages decrypts them using the RSA algorithm according to their priority. This method reduces the risk of man-in-middle attacks and timing attacks as the encrypted and decrypted messages are further jumbled based on their priority. It also reduces the power monitoring

attack risk if a very small amount of information is exchanged. It raises the bar on the standards of information security, ensuring more efficiency



In secret key crypto there is only one key. It is used for both encryption and decryption. A key refers to any code that yields plain text when applied to cypher text.This key is shared by both sender and receiver. If the key is disclosed the secrecy of the information is compromised. The key is known to both the sender and the receiver, hence does not protect the sender from the receiver forging a message & claiming is sent by sender. Lengthy keys are used to increase the security and to decrease the chances of identifying the key through brute force. It is relatively fast as it uses the same key for encryption and decryption [8]. However, more damage if can occur if the key is compromised. When someone gets their hands on a symmetric key, they can decrypt everything that was encrypted with that key. Since symmetric encryption is used for two-way communication, both sender and receiver end data gets compromised.

MODULES-

User Module:
This module used to users are going to online website. 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 data received in input and sent as output by the identity element. Key Generator is used to compute on-the-fly the private key of the coin element.

Attacker:
Credit/Debit card data theft is attacking user details but those details have been encrypted so they can't able to hacking sensitive details like accounts, payment details. because user have private, public keys to send their mail but hacker does not retrieve private keys.

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 hack 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.

Admin module:
This module is used to admin to work their website and add products like product name, description, warranty period, etc., and admin view all users purchase products but cannot view user account details. And to view which product is delivered or not.

Conclusion:

we have introduced REMD that is, to the best of our knowledge, the first data-breach-resilient fully off-line micropayment approach. The security analysis shows that REMD does not impose trustworthiness assumptions. Further, REMD 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 REMD 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] Crypto-analyses on user efficient recoverable off-line e-cashs scheme with fast anonymity revoking yalin Chen. et al., 2012
[2] Modelling Attacks on Physical Unclonable Function Ulrich Ruhrmair. et al., July 2013
[3] PUFs in Security Protocols: Attack Models and Security Evaluations Ulrich Ruhrmair. et al., Nov 2012
[4] Fully Off-line Secure Credits for Mobile Micro Payments(FORCE) VanesaDaza. Et al., July 2011
[5] Windows Mobile LiveSD Forensics Ey up S. Canlar . et al. 2013
[6] A Live Digital Forensic system for Windows networks Roberto Battistoni,. Et al., 2011
[7] Circuit Level IC Protection Through Direct Injection of Process Variations W. Paul Griffin. Et al., May 2012
[8] Robust Key Extraction from Physical Uncloneable Function B.Skorie. Et al.,2007
[9] Extracting Secret Keys from Integrated Circuits Daihyun Lim, Et al., Oct 2005
[10] Reliable OSPM Schema for Secure Transaction using Mobile Agent in Micropayment System Chaitra Kiran N. Et al., 2011
[11]REMD: Fraud Resilient Device for Off-line micro-payment Vanesa Daza, Roberto Di Pietro, Flavio Lombardi

Volume: 6 Issue: 2 Dec,2016,ISSN_NO: 2321-3337

Volume: 6 Issue: 2 Dec,2016,ISSN_NO: 2321-3337