VALIDATE OPERATION BEHAVIOR IN THE BUSINESS PROCESS AS A SERVICE CONFIGURATION

CHEKURUMALLI LAVANYA[1], SHRABAN KUMAR APAT[2]

[1]M.Tech Student, Dept of CSE, St. Martin's Engineering College, Hyderabad, T.S, India

[2]Associate Professor, Dept of CSE, St. Martin's Engineering College, Hyderabad, T.S, India

ABSTRACT:

The main problem with using an unrelated method may be the inability to check the status of the transaction without a trusted third party. In fact, it can be very difficult to monitor previous transactions without external or shared databases available, as it is difficult for the seller to see if certain digital currencies are being used. Dismantling techniques will also be used with the idea of changing programs / programs to replace them with malicious functions. Regardless of the structure of the electronic payment system, point-of-sale systems always process information and often require remote management. In this article, DEDev may be the first solution to not require reliable organizations, accounts, or reliable devices that offer flexibility against fraud in the event of data breaches in fully indirect electronic payment systems. Our analysis means that DEDev is perhaps the only proposal that accepts all the attributes required for certain secure payment solutions, while offering diversity when thinking about the payment method. The identity as well as the gold coin element can be considered protective devices by manipulating a secure environment for storing and executing sensitive data.

Keywords: Point of Sale (PoS), Mobile secure payment, architecture, protocols, cybercrime, fraud-resilience, Deception Elastic Device (DEDev).

1. INTRODUCTION:

Brute forcing remote access connections and taking advantage of stolen credentials remain the main vectors for PoS intrusions. However, recent developments show the resurgence of RAM-scraping adware and spyware. Modern PoS systems are effective computers outfitted having a card reader and running specialized software. More and more frequently, user products are leveraged as input towards the PoS. During these scenarios, adware and spyware that may steal card data every time they are read through the device has

flourished. The communication protocol employed for the payment transaction doesn't directly read customer coins. Rather, the seller only 'talks' to the identity element to be able to find out the user [1]. However, previous solutions lack an intensive security analysis. When they concentrate on theoretical attacks, discussion on real life attacks for example skimmers, scrapers and knowledge vulnerabilities are missing.

Literature Survey: It's worth mentioning here our previous work known as Pressure that, much like DEDev, was built utilizing a PUF based architecture. Actually, monitoring past transactions without any available link with exterior parties or shared databases can be very difficult, because it is hard for a vendor to see if some digital coins happen to be spent [2]. Probably the most relevant variations between and DEDev may be the technology accustomed to compute digital coins. Actually, only one message is distributed in the vendor towards the customer and the other the first is delivered back in the customer towards the vendor that contains all of the needed digital coins, if available. However, the identity element may be used to thwart fraudsters.

2. TRADITIONAL METHOD:

POS systems behave like portals and you want some type of network connection to be able to connect to external credit card processors. It is indeed mandatory to validate transactions. To reduce costs and streamline management and maintenance, remote PoS devices can be managed from these internal systems. Mobile payment solutions that have been suggested so far can be considered to be entirely online, almost complete, low-cost, or completely off-grid. The previous work was called FORCE, which was built using a PUF-based architectural design, such as DEDev. The pressure provided an inadequate precautionary strategy due to data blackout and may not address the most relevant attacks aimed at threatening confidential customer data. The disadvantages of the current system: It is not easy to protect offline scenarios, where customer information is stored in the store longer, allowing attackers to better discover themselves. Filters: Within this attack, the client input device, which is a PoS product, is replaced with an imitation device that captures the data from the client card [3]. The main problem in the completely incomplete policy may be the inability to examine the status of the transaction without a trusted third party. In fact, it may be difficult to monitor past transactions that have nothing to do with external correspondents or shared databases, as it is difficult for the service provider to know whether certain digital parts are already used. This is the main reason in recent years to offer different methods to provide a reliable payment plan without an Internet connection. Although many print works, they all

focus on the anonymity of transactions and the possibility of using gold coins.

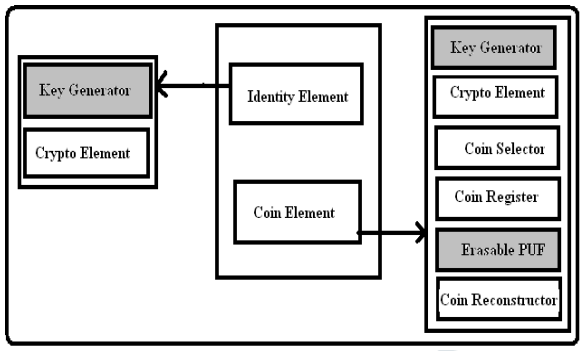

Fig.1.Proposed system architecture

3. ENHANCED METHOD:

Preliminaries: The payment process consists of two basic steps: processing, delegation and settlement. Network-level hacking of a point-of-sale system can be made by exploiting shared connections, open systems or by breaking the password of the merchant network. In fact, many all-in-one PoS systems are derived from bone OS for general purposes. It is not easy to protect off-network scenarios. In these cases, customer information within the POS system is stored longer and is therefore more vulnerable to attackers. This has been largely achieved by using a PUF structure that can be erased with a new protocol design. In addition, our proposal is still subject to in-depth discussions and is compared to the state of the art. Thus, the attacker clicks on the payment card data to be processed in your area. Disassembly techniques will also be used with the idea of changing programs / programs to replace them with malicious functions [4]. DEDev is perhaps the first solution to not require reliable organizations, accounts, or reliable devices to offer flexibility against fraud in the event of data breach in fully indirect electronic payment systems. In addition, it should be noted that DEDev is still designed to become a safe and reliable packaging plan for digital parts. Because these practical differences cannot be controlled during manufacturing, the physical properties of the device cannot be copied or cloned. Even in fully independent electronic payment systems, this attack is still available. In fact, the payment product usually consists of several items and the card information is shared between these items.

Framework: Therefore, in cases where the customer and the provider are permanently or permanently separated from the network, a secure online payment cannot be made. This document describes DEDev, a safe, indirect, secure, indirect payment solution that resists PoS data violations. Our solution is to improve existing approaches to diversity and security. In particular, we detail the structure, components and protocols of DEDev. In addition, a comprehensive analysis of the functional and safety characteristics of DEDev is presented, demonstrating its usefulness and utility. In addition, allowing DEDev users to reduce their bank accounts makes this account particularly fun to protect privacy. This paper discusses and discusses DEDev, a secure partial payment

approach, off-line using multiple breakable physical functions (PUFs). DEDev provides an element to document the client, in addition to a gold coin item, currencies are not stored in your area, but are calculated immediately if necessary. The connection protocol used in the payment transaction does not read the client's parts directly. Finally, some outstanding issues were identified and future work left [5]. In particular, we are exploring the possibility of allowing the use of the numeric key in multiple transactions offline while maintaining the same level of security and benefit. To our knowledge, DEDev can be the first solution that can provide completely secure payments without an Internet connection with the ability to adapt to any breaches at known or currently known Poss. Instead, the vendor "only" speaks to the identity element in order to find the user. This simplification reduces the burden of communication using the gold coin element that influenced the previous approach. Among other features, this two-step protocol allows the financial institution, or even the source of the gold coins, to create read-only digital coins with a specific identity element, that is, to say with a particular user. Additionally, the user identity element can be used to improve user security to frustrate malicious users. To our knowledge, this is actually the first solution that enables complete secure payments to be performed right now with flexibility in any of the currently known PDS violations. Advantages of the proposed system: DEDev design continues to be a safe and reliable packaging plan for digital parts. DEDev also covers multi-bank scenarios. In fact, for credit cards and credit cards secured by trusted organizations, such as card issuers, card health, a standard agreement can be used at DEDev to create banks capable of producing and selling cards. Special gold coin element.

Implementation: By using the payment solutions of their business differently depending on the anti-tampering devices, DEDev assumes that only PUF-based impurities can benefit from forgery protection. The DEDev structure is composed of two main elements: a name element with a gold coin element. Only a specific gold object can be read with a specific identity object. Each element of the identity, as well as the gold coin component, is created on physically non-digestible functions. It measures for the first time the main block 64 feet PUF, measures the main difference between two periods of delay, each created by the sum of the values of PUF 64. In the first step, the PUF is put to the test, thus generating outputs and additional information called auxiliary data. In the next step, the help information provides the same result as in the initial step, which allows the PUF to generate fixed values [6]. The Gold Seed Record will be used at the time of the transaction to allow you to challenge the erasable PUF. The acquired fact is combined with the gold coin data to recover the gold-coded currency again. DEDev relies on

standard pairing protocols, such as the simple matching process, to enter the Bluetooth authentication key. DEDev does not provide a transaction dispute resolution protocol. This type of dispute can be exploited outside the network by fraudsters or malicious vendors by injecting counterfeit issues into the transaction or by modifying previous transactions. In this article, we introduced the DEDev system, which is the best we have achieved in our understanding, the first partial payment approach totally without data communication. The security analysis indicates that DEDev does not impose confidence assumptions. In addition, DEDev may be the first solution in the literature in which client device data attacks cannot be exploited to influence the machine. Assistants in gold and gold seed are written in the gold coin records by the financial institution or source of gold coins so that the final value of the gold given out output corresponds to the form encrypted from the real gold coin. During the payment protocol, these tokens will be used to obtain a directory, allowing the payment process so that the seller can verify it, even without contacting an external bank. Choi and Kim are designed to protect keys in TPMs using PUF [7]. In fact, once the keys are saved in the memory and moved with the bus, their value is changed using PUF, which makes it unnecessary to tapped the PUF.

4. CONCLUSION:

In fact, the digital currency used in DEDev is simply a digital form of the real currency, and therefore, it is not related to others with respect to the holder of identity and the element of the gold coin. Stealing debit card data and credit is one of the first types of cybercrime. However, it is among the most common nowadays. Attackers are often designed to steal these customer data by targeting the purpose of the purchase system, the point at which the store first obtains customer data. Using their company's payment solutions differently based on anti-manipulation devices, DEDev assumes that chips based on PUF files only can take advantage of the tamper proof feature. As a result, our assumptions tend to be less restrictive than other methods. When the transaction and all types of connected parts that it uses tend to depart, the manner in which such parts are purchased / procured by the seller is outside the scope of the proposed protocol. The basic benefit is the simplest, fastest and safest interaction among the actors / entities involved.

REFERENCES:

[1] G. Van Damme, K. M. Wouters, H. Karahan, and B. Preneel, “Offline NFC Payments with Electronic Vouchers,” in Proc. ACM 1st ACM Workshop Netw., Syst., Appl. Mobile Handhelds, 2009, pp. 25–30.

[2] R. Battistoni, A. D. Biagio, R. Di Pietro, M. Formica, and L. V. Mancini, "A live digital forensic system for Windows networks," in Proc. 20th IFIP TC Int. Inf. Security Conf., 2008, vol. 278, pp. 653–667.

[3] B. Yahid, M. Nobakht, and A. Shahbahrami, "Providing security for e-wallet using e-cheque," in Proc. 7th Int. Conf. e-Commerce Develop. Countries: Focus e-Security, Apr. 2013, pp. 1–14.

[4] R. Maes, P. Tuyls, and I. Verbauwhede, "Low-overhead implementation of a soft decision helper data algorithm for SRAM PUFs," in Proc. 11th Int. Workshop Cryptographic Hardware Embedded Syst., 2009, pp. 332–347.

[5] T. Nishide and K. Sakurai, "Security of offline anonymous electronic cash systems against insider attacks by untrusted authorities revisited," in Proc. 3rd Int. Conf. Intell. Netw. Collaborative Syst.2011, pp. 656–661.

[6] Vanesa Daza, Roberto Di Pietro, Flavio Lombardi, and Matteo Signorini, "DEDev: Fraud Resilient Devicefor Off-Line Micro-Payments", ieee transactions on dependable and secure computing, vol. 13, no. 2, march/april 2016.

[7] S. Golovashych, "The technology of identification and authentication of financial transactions. from smart cards to NFC-terminals," in Proc. IEEE Intell. Data Acquisition Adv. Comput. Syst., Sep. 2005, pp. 407–412.