IDL - International Digital Library Of
Technology & Research
Volume 1, Issue 2, Mar 2017

Available at: www.dbpublications.org

International e-Journal For Technology And Research-2017

Fraud Resilient System for Off-Line Micro-Payments

MS. RAJANI D [1], MRS. SHASHIREKHA H [2]
Dept. of Computer Science
[1] MTech, Student– VTU PG Center, Mysuru, India
[2] Guide, Assistant Professor– VTU PG Center, Mysuru, India

SURVEY PAPER

1 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 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.

2 INTRODUCTION

PoS systems act as gateways and require some sort of network connection in order to contact external credit card processors. This is mandatory to validate transactions. To reduce cost and simplify administration and maintenance, PoS devices may be remotely managed over these internal networks. Mobile payment solutions proposed so far can be classified as fully on-line, semi off-line, weak off-line or fully off-line.

The previous work called FORCE that, similarly to FRoDO, was built using a PUF based architecture. FORCE provided a weak prevention strategy based on data obfuscation and did not address the most relevant attacks aimed at threatening customer sensitive data, thus being vulnerable to many advanced attack techniques Market analysts have predicted that mobile payments will overtake the traditional marketplace, thus providing greater convenience to consumers and new sources of revenue to many companies. This scenario produces a shift in purchase methods from classic credit cards to new approaches such as mobile-based payments, giving new market entrants novel business chances. Widely supported by recent hardware, mobile payment technology is still at its early stages of evolution but it is expected to rise in the near future as demonstrated by the growing interest in crypto currencies. The first pioneering micro-payment scheme was proposed by Rivets and Shamir back in 1996. Nowadays, crypto-currencies and decentralized payment systems are increasingly popular, fostering a shift from physical to digital currencies. However, such payment techniques are not yet commonplace, due to several unresolved issues, including a lack of widely-accepted standards, limited interoperability among systems and, most importantly, security.

Off-line scenarios are harder to protect, customer data is kept within the PoS for much longer time, thus being more exposed to attackers. Skimmers: in this attack, the customer input device that belongs to the PoS system is replaced with a fake one in order to capture customer's card data. The main issue with a fully off-line approach is the difficulty of checking the trustworthiness of a transaction without a trusted third party. In fact, keeping track of past transactions with no available connection to external parties or shared databases can be quite difficult, as it is difficult for a vendor to check if some digital coins have already been spent. This is the main

reason why during last few years, many different approaches have been proposed to provide a reliable off-line payment scheme. Although many works have been published, they all focused on transaction anonymity and coin enforceability. However, previous solutions lack a thorough security analysis. While they focus on theoretical attacks, discussion on real world attacks such as skimmers, scrapers and data vulnerabilities is missing.

3 SURVEY

3.1 Fraud Resilient Device for Off-line micro-payments "Here author vanisa daza said market analysts have predicted that mobile payments will overtake the traditional marketplace, thus providing greater convenience to consumers and new sources of revenue to many companies. This scenario produces a shift in purchase methods from classic credit cards to new approaches such as mobile-based payments, giving new market entrants novel business chances. Widely supported by recent hardware, mobile payment technology is still at its early stages of evolution but it is expected to rise in the near future as demonstrated by the growing interest in crypto-currencies. The first pioneering micro-payment scheme. Nowadays, crypto-currencies and decentralized payment systems are increasingly popular, fostering a shift from physical to digital currencies. However, such payment techniques are not yet commonplace, due to several unresolved issues, including a lack of widely-accepted standards, limited interoperability among systems and, most importantly, security".

3.2 Secure Payment Solutions Fully Off-Line Functions on Frodo "In this survey says 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 entrant's 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 this 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".

3.3 OFF-Line Secure Credits For Micro Payments Using FRoDO Resilient Device "This survey mainly concentrate on micro payments, with network security and its consists of the policies and practices adopted to prevent and monitor access, misuse, modification, or denial of a computer network and network-accessible resources.

Network security involves the authorization of access to data in a network, which is controlled by the network administrator Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Here other survey says that

NetBill is a transactional payment protocol with many advanced features (atomicity, group membership, pseudonyms, etc.) that requires communication with the NetBill server for each transaction, thus exhibiting the same drawback with respect to micropayments as the simpler online protocols already mentioned. Other general-purpose payment protocols are unattractive for micropayments for these same reasons.

NetCents and Millicent [Man95] are scrip-based off-line-friendly micropayment protocols. As the monetary unit used in these protocols is vendor-specific, double-spending is made very difficult (if not impossible). The assumption behind both protocols is

that people tend to re-use the same merchants repeatedly."

3.4 Preserving Micro-Payments in Deception of Resilient Devices "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 remote access connections and stolen credentials involved in PoS intrusions".

3.5 A Resilient and Energy-saving Incentive System for Resource Sharing "Current sales indicate a significant increase in the popularity of smart phones and evidently show a trend towards feature-rich mobile devices. Besides offering computing and storage resources almost comparable to desktop PCs ten years ago, such devices offer a variety of other resources, including different communications capacities like 3G, WiFi, and Bluetooth, as well as sensors for position, acceleration, light, and temperature.

Combining the resources provided by multiple devices enables new and exciting applications. These are typically observed as a natural subset of pervasive computing and find increasing interest in many other disciplines of distributed computing, e. g., in Grid computing and service overlays. Example applications range from pooling capacities of the cellular connections of multiple devices to speed up downloads to people-centric sensing exploiting the sensors of thousands of smart-phones. Unfortunately, despite of the growth in resource variety, processor speed, memory size, and communication bandwidth, battery capacity remains the limiting factor for realizing the vision described above. Providing resources for applications running on remote devices may consume a significant amount of energy, limiting the operating time of a mobile device for the owner's personal use. In fact, mechanisms are required to motivate device owners that are not known to each other in general and, thus, do not pursue a common goal spend energy on behalf of others. Such mechanisms can be provided by incentive systems. These systems could recompense the energy spent for serving a remote resource request, and allow to use the refund in turn to recompense others for using their resources. Many incentive systems for motivating cooperation among users have been proposed with different application scenarios in mind, e. g. MilliCent, NetPay, and Micromint.

However, most of them cannot be used to motivate resource sharing among mobile devices, since they either require trusted hardware, connections to a central broker or other third parties on each interaction that requires a refund, or utilize refunds that cannot be reused without opening the door for fraud. An even more important drawback when it comes to providing incentives for spending energy is that must systems consume lots of energy by themselves, e. g., by requiring the use of public key cryptography on each payment, contradicting the primary goal of the incentive system".

3.6 Offline Micropayments without Trusted Hardware "Current electronic payment systems are not well matched to occasional, low-valued transactions. (For the purposes of this discussion, we use the term "electronic payment system" broadly, to encompass conventional credit cards, stored-value cards, online and offline digital cash, etc.) A central requirement for any electronic payment system is that a single compromise or failure should not have catastrophic consequences. For example, it should not be possible to double spend in a digital cash system, nor should the compromise of a client's authorization secret entail unlimited client liability or uncollectible transactions. Traditional payment systems are designed to prevent such failures. Unfortunately, the prevention mechanisms are generally too expensive to support occasional, low-valued transactions. Typically, such systems require online transactions, trusted client hardware such as smartcards, or must assume conditions that are not always true, such as that payers can be held responsible for any and all fraud or misuse of their authorization secrets. In this paper, however, we present a new approach that focuses instead on risk management. Our central observation is that in some applications we can relax many of the expensive requirements associated with electronic payment systems while still keeping fraud or uncollectible transactions within acceptable levels.

We shift the security functions performed by online authorization of transactions to certified code that can authorize offline transactions under certain conditions. These conditions are customized to each client according to a risk management strategy customized to the application. There are three main contributions in this paper. First, we describe a framework in which certified offline authorizations created by a risk management strategy replace online authorizations for occasional, low-valued transactions. We then describe architecture for a practical payment system in which a trust management system is used to encode the client risk management strategy. Finally, we describe a prototype implementation based on the KeyNote trust management toolkit, in which users can purchase vending machine items using credentials stored on conventional palmtop computers.

This is the main reason why during last few years, many different approaches have been proposed to provide a reliable offline payment scheme. Although many works have been published, they all focused on transaction anonymity and coin enforceability. However, previous solutions lack a thorough security analysis. While they focus on theoretical attacks, discussion on real world attacks such as skimmers, scrapers and data vulnerabilities is missing".

4 CONCLUSION

Our survey mainly conclude that the first data-breach-resilient fully off-line 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.

OTHER 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 2015.

[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 secuRe CrEdits 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] G. Vasco, Maribel, S. Heidarvand, and J. Villar, "Anonymous subscription schemes: A flexible construction for on-line services access," in SECRYPT '10, July 2010, pp. 1–12.

[12] K. S. Kadambi, J. Li, and A. H. Karp, "Near-field communication-based secure mobile payment service," in ICEC '09. ACM, 2009.

[13] V. C. Sekhar and S. Mrudula, "A complete secure customer centric anonymous payment in a digital ecosystem," ICCEET '12, 2012.

