ISSN 23499842(Online), Volume 2, issue 1 March 2017
International Journal of Innovative Trends and Emerging Technologies

PROVIDING SECURITY IN OFF-LINE TRANSACTION USING FRoDO AND PUF

M. SARMILA[1], **D. DEVI**[2]
[1]PG Scholar, Department of CSE, T.S.M Jain College of Technology, India
[2]Assistant professor, Department of CSE, T.S.M Jain College of Technology, India

Abstract

Credit and positive identification knowledge larceny is one in every of the earliest sorts of law-breaking. Still, it's one in every of the foremost common today. Attackers usually aim at stealing such client knowledge by targeting the point of sale system, i.e. the purpose at that a retail merchant first acquires client knowledge. Modern pos systems square measure powerful computers equipped with a card reader and running specialized software package. Progressively usually, user devices square measure leveraged as input to the pos. In these situations, malware which will steal card knowledge as before long as they're browse by the device has flourished. As such, in cases wherever client and marketer square measure persistently or intermittently disconnected from the network, no secure on-line payment is feasible. This paper describes FRoDo, a secure off-line micro-payment answer that's resilient to pos knowledge breaches. Our answer improves over up thus far approaches in terms of flexibility and security to the simplest of our data, FRoDo is that the first answer which will offer secure totally off-line payments whereas being resilient to any or all presently far-famed pos breaches especially, we tend to detail FRoDo design, components, and protocols. Further, an intensive analysis of FRoDo purposeful and security properties is provided, showing its effectiveness and viability.

Index terms: FRoDO, micro-payment

1. Introduction

Electronic devices have pervaded our everyday life to a previously unseen extent, and will likely continue to do so in the future. But their ubiquity also makes them a potential target for adversaries and brings about privacy and information security issues. Today's electronic devices are mobile, cross-linked and pervasive, which makes them a well-accessible target for adversaries. The well-known protective cryptographic techniques all rest on the concept of a secret binary key: They presuppose that devices store a piece of digital information that is, and remains, unknown to an adversary. It turns out that this requirement is difficult to realize in practice. Physical attacks such as invasive, semi-invasive or sidechannel attacks carried out by adversaries with one-time access to the devices, as well as software attacks like application programming interface (API) attacks, viruses or Trojan horses, can lead to key exposure and security breaks. Merely calling a bit string a "secret key" does not make it secret, but rather identifies it as an interesting target for the adversary. Indeed, one main motivation for the development of Physical Unclonable Functions (PUFs) was their promise to better protect secret keys.

A PUF is an (at least partly) disordered physical system P that can be challenged with socalled external stimuli or challenges c, upon which it reacts with corresponding responses r. Contrary to standard digital systems, these responses depend on the micro- or nanoscale structural disorder of the PUF. It is assumed that this disorder cannot be cloned or reproduced exactly, not even by the PUF's original manufacturer, and that it is unique to each PUF. Any PUF P thus implements a unique and individual function fP that maps challenges c to responses r = fP (c). Thereby the tuples (c, r) are usually called the challenge response pairs (CRPs) of the PUF. Due to its complex internal structure, a PUF can avoid some of the shortcomings of classical digital keys. It is usually harder to read out, predict, or derive PUF-responses than to obtain digital keys that are stored in non-volatile memory. The PUF-responses are only generated when needed, which means that no secret keys are present permanently in the system in an easily accessible digital form. Finally, certain types of PUFs are naturally tamper sensitive: Their exact behavior depends on minuscule manufacturing irregularities, often in different layers of the IC. Removing or penetrating these layers will automatically change the PUF's read-out values. These facts have been exploited in the past for different PUF-based security protocols. Prominent examples include identification, key exchange, and various forms of (tamper sensitive) key storage and applications thereof, such as intellectual property protection or read-proof.

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized 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. 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. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. Web applications also present new security and privacy challenges, partly because the un-trusted Internet has essentially become an integral component of such applications for carrying the continuous interaction between users and servers.

Defense-in-depth is the practice of implementing multiple layers of security. Effective defense-in-depth strategies do not limit themselves to focusing on technology, but also focus on operations and people. For example, a firewall can protect against unauthorized intrusion, but training and the implementation of well-considered security policies help to ensure that the firewall is properly configured.

2. Related Work

Point-of-sale system and security by Nedospasov.D, Schlosser.A, and Rivest.R.L [1] describes Security essentials bootcamp style course, “2014 will be the year of the retailer”. Over the last several months, several retail organizations have been victims of information security breaches targeting consumer payment card data. The most notable of these was the Target corporation breach. However, several other retail organizations have also been victims of payment card data theft over the past year to include Michaels Stores, Inc., Sally Beauty Holdings, Inc., and Neiman Marcus This is certainly not an all-inclusive list of retailers that have experienced payment card data theft in recent months. There are several additional examples within retail as well as other markets (e.g. Food and Beverage, Hospitality, Healthcare, etc.) However, the resources available to the breached organizations compared to the level of bad actor success paints a picture that more needs to be done to protect consumer payment card data.

Kramer.J, Nedospasov.D, Schlosser.A, and Seifert, J.p [2] presents a work called Differential Photonic Emission Analysis to exploit photonic emissions. We call this form of analysis Differential Photonic Emission Analysis (DPEA). After identifying a suitable area for the analysis, our system captures photonic emissions from switching transistors and relates them to the program running in the chip. The subsequent differential analysis reveals the secret key. They recovered leakage from the datapath's driving inverters of a proof of concept AES-128 implementation. Successfully performed DPEA and were able to recover the full AES secret key from the photonic emissions. The system costs for an attack are comparable to power analysis techniques and the presented approach allows for AES key recovery in a relevant amount of time. Thus, this work extends the research on the photonic side channel and emphasizes that the photonic side channel poses a serious threat to modern secure ICs.

To support withdrawing and storing money from all levels of the bank for the customers in the real world, a proxy blind signature scheme and an offline e-cash scheme based on the new proxy blind signature scheme has been proposed by Jianwei, LIU Jianhua, QIU Xiufeng [3]. The proposed proxy blind signature is proven secure in the random oracle model under chosen-target computational Diffie-Hellman assumptions, and the ecash scheme can satisfy the security requirements of unforgeability, anonymity, and traceability. Electronic cash (e-cash in short) scheme is an important electronic mechanism that can be widely used in the businesses over the Internet and wireless networks as a payment system. Generally, there are three types of entities involved in an e-cash scheme: the customer, the bank, and the merchant. Three transactions may occur between the three entities: withdrawal, payment, and deposit. Nowadays, the trusted platform module (TPM) is implemented in notebook computers for security. In the TPM is integrated into the bank system by a judge in the setup phase.

How several proposed Physical Unclonable Functions (PUFs) can be broken by numerical modeling attacks. Given a set of challenge-response pairs (CRPs) of a PUF, our attacks construct a computer algorithm which behaves indistinguishably from the original PUF on almost all CRPs. This algorithm by Ruhrmair.U, Sehnke.F, Solter.J, Dror.G, Devadas.S, and Schmidhuber.J [4] can subsequently impersonate the PUF, and can be cloned and distributed arbitrarily. This breaks the security of essentially all applications and protocols that are based on the respective PUF.The PUFs attacked successfully include standard Arbiter PUFs and Ring Oscillator PUFs of arbitrary sizes, and XOR Arbiter PUFs, Lightweight Secure PUFs, and Feed-Forward Arbiter PUFs of up to a given size and complexity. Our attacks are based upon various machine learning techniques, including Logistic Regression and Evolution Strategies.

3. Proposed Work

FRoDO is a secure off-line micro-payment approach using multiple physical unclonable functions (PUFs). FRoDO features an identity element to authenticate the customer, and a coin element where coins are not locally stored. The module list consists of Frodo, Puf, Identity and Coin, and Blacklists. FRoDO is a Paring protocol and it is to avoid brute force attack use the fail to ban approach. 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 [5] 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 FRoDO protocol has the following phases.

1) Pairing phase
2) Payment phase
3) Transaction dispute

PUF is a unique one which is used for authentication purpose. Coin selector Identity and coin selector includes the Identity Element which has been used for compute the private key of element. Cryptographic Element has been used for symmentric and asymmentric cryptographic algorithms. Furthermore, it uses Coin Registers and Coin Selector.

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 unforgeability. 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.

FRoDO is the first solution that neither requires trusted third parties, nor bank accounts, nor trusted devices to provide resiliency against frauds based on data breaches in a fully off-line electronic payment systems.
Furthermore, by allowing FRoDO customers to be free from having a bank account, makes it also particularly interesting as regards to privacy. In fact, digital coins used in FRoDO are just a digital version of real cash and, as such, they are not linked to anybody else than the holder of both the identity and the coin element. Differently from other payment solutions based on tamper-proof hardware, FRoDO assumes that only the chips built upon PUFs can take advantage from the tamper evidence feature. As a consequence, our assumptions are much less restrictive than other approaches. This paper introduces and discusses FRoDO, a secure off-line micro-payment approach using multiple physical unclonable functions (PUFs).

FRoDO features an identity element to authenticate the customer, and a coin element where coins are not locally stored, but are computed on-the fly when needed. The communication protocol used for the payment transaction does not directly read customer coins. Instead, the vendor only communicates with the identity element in order to identify the user. This simplification alleviates the communication burden with the coin element that affected previous approach. The main benefit is a simpler, faster, and more secure interaction between the involved actors/entities. Among other properties, this two-steps protocol allows the bank or the coin element issuer to design digital coins to be read only by a certain identity element, i.e., by a specific user. Furthermore, the identity element used to improve the security of the users can also be used to thwart malicious users. To the best of our knowledge, this is the first solution that can provide secure fully off-line payments while being resilient to all currently known PoS breaches.

A) Cryptographic Element

Cryptographic Element is used for symmetric and asymmetric cryptographic algorithms applied to data received in input and send as output by the coin element; Coin Selector is responsible for the selection of the right registers used together with the output value computed by the coin element PUF in order to obtain the final coin value; Coin Register is used to store both PUF input and output values required to reconstruct original coin values. Coin registers contain coin seed and coin helper data. Coin seeds are used as input to the PUF whilst coin helpers are used in order to reconstruct stable coin values when the PUF is challenged; Erasable PUF is a read-once PUF. After the first challenge, even if the same input is used, the output will be random.

B) Coin Reconstructor

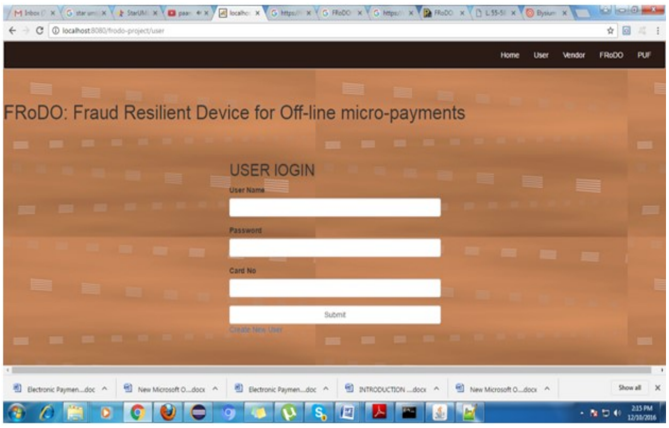
Coin Reconstructor is responsible to use the output coming from the PUF together with a coin helper in order to reconstruct the original value of the coin. The reconstructor uses helper data stored into coin registers to extract the original output from the PUF. Both the identity element and the coin element are built upon physically unclonable functions. As such, both of them inherit the following features: a) Clone Resiliency: It must be extremely hard to physically clone a strong PUF, i.e. to build another system which has the same challenge response behavior as the original PUF. This restriction must hold even for the original manufacturer of the PUF; b) Emulation Resiliency: Due to the very large number of possible challenges and the PUF's finite read-out rate, a complete measurement of all challenge-response pairs (for short, CRPs) within a limited time frame must be extremely hard to achieve; c) Unpredictability: It must be difficult to numerically predict the response of a strong PUF to a randomly selected challenge even if many other challenge-response pairs are known.

C) Blacklists

FRoDO uses two different elements: an identity element and a coin element, in order to improve the security of the whole payment system .In fact, the vendor device does not directly communicate with the coin element but has to go through the identity element. On the one hand this allows either the bank or the coin element issuer to design all the digital coins belong to a specific coin element to be read only by a certain identity element, i.e. by a specific user. This means that even though the coin element is lost or it is stolen by an attacker, such element will not work without the associated identity element. As such, the identity element can be considered as a second factor aimed at improving the security of customer coins. On the other hand, the identity element can be used to fight against attackers as well. In fact, as depicted, if an identity element is considered malicious and is blacklisted, no matter what the device is used by the user, any coin will not be accepted and processed by the vendor.

4. EXPERIMENTAL RESULTS

In our project using jsp to design the process of an application, JSP pages easily combine static templates, including HTML or XML fragments, with code that generates dynamic content. JSP pages are compiled dynamically into Servlets when requested, so page authors can easily make updates to presentation code. JSP pages can also be precompiled if desired. Fraud Resilient Device for off-line micro-payments login details are submitted as shown in figure 1.
Each JAVA program is both compiled and interpreted. With a compiler, you translate a JAVA program into an intermediate language called JAVA byte codes--the platform-independent codes interpreted by the JAVA interpreter. With an interpreter, each JAVA bytecode instruction is parsed and run on the computer. Compilation happens just once; interpretation occurs each time the program is executed.



FRoDO: Fraud Resilient Device for Off-line micro-payments

USER lOGIN

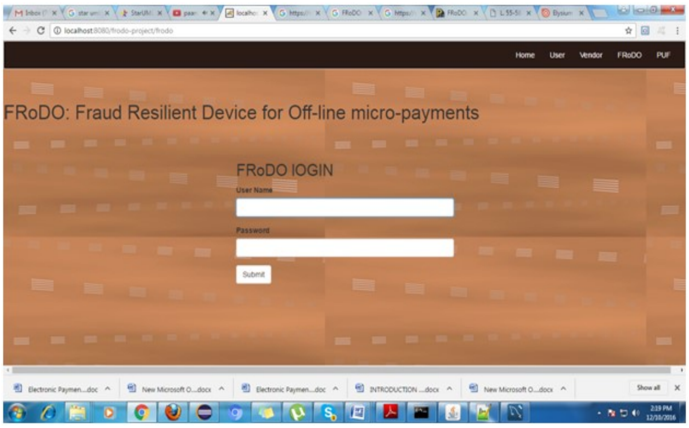
User Name

Password

Card No

Figure 1: FRoDo- Fraud Resilient Device for off-line micro-payments

You can think of JAVA byte codes as the machine code instructions for the JAVA Virtual Machine (JAVA VM). Every JAVA interpreter, whether it's a JAVA development tool or a Web browser that can run JAVA applets, is an implementation of the JAVA VM. The JAVA VM can also be implemented in hardware. JAVA byte codes help make "write once, run anywhere" possible. You can compile your JAVA program into byte codes on any platform that has a JAVA compiler. The byte codes can then be run on any implementation of the JAVA VM. For example, the same JAVA program can run on Windows NT, Solaris, and Macintosh. JAVA is an object oriented language, it is basically supports all concepts of c and c++ with some additional features. Other attractive feature JAVA is a platform independent language. The genesis of JAVA is complete without a look at the JAVA buzzwords.



FRoDO: Fraud Resilient Device for Off-line micro-payments

FRoDO lOGIN

User Name

Password

Figure 2: FRoDO LOGIN for off-line micro-payments

In this project threading concept is very important. A thread is a sequential path of code execution within a program. And each thread has its own local variables, program counter and lifetime. Like creation of a single

Thread, also create more than one thread (multithreads) in a program using class Thread or implementing interface runnable to make our project efficient and dynamic. In our project using request process with the help of multi threading concepts. In our project using a backend as SQL Server 2005, here create and maintaining the tables which are having values used for our processes. Maintaining the registration table, login table and to store the values which is entered by the system admins and as well as end users.

5. Conclusion

The introduced FRoDO that is, to the best of our knowledge, the first data-breach-resilient fully off-line micropayment 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, The investigating the possibility to allow digital change to be spent over multiple off-line transactions while maintaining the same level of security and usability. As for all the real-world payment schemes based on credit, debit and prepaid cards, FRoDO assumes that, in case of bank/coin element issuer private key renewal, a time-window is adequately.

7. References

[1] Nedospasov.D, Schlosser.A, and Rivest.R.L, "Point-of-sale system and security", 2014.

[2] Kramer.J, Nedospasov.D, Schlosser.A, and Seifert . J.-P, "Differential Photonic Emission Analysis", 10.1007/978-3-642-40026-1-1, 2013.

[3] Jianwei, LIU Jianhua, QIU Xiufeng, "A Proxy Blind Signature Scheme and off-Line Electronic cash scheme" IEEE 10.1007/s11859-013-0903-2, 2013.

[4] Ruhrmair.U, Sehnke.F, S¨olter.J, Dror.G, Devadas.S, and Schmidhuber.J, "Modeling Attacks on Physical Unclonable Functions," 2010.

[5] Incorporated T. M, "Point-of-sale system breaches," Trend Micro Incorporated, Technical Report, 2014.