OFF-LINE SECURE FOR MICRO PAYMENTS USING FRODORESILIENT SECURE DEVICE

Kasarla Shiva kumar [1], Prof. Dr. K Sridhar[2]

1. **M.Tech Scholar, Department of CSE, Vaageswari College of Engineering, Karimnagar, Telangana, India – shivakumar55@gmail.com, 8019733795**
2. **Associate Professor, Department of CSE , Vaageswari College of Engineering, Karimnagar, Telangana, India - sridhark529reddy@gmail.com, 9985676333**

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.

I.INTRODUCTION

What is Secure Computing?

Computer security (Also known as cyber security or IT Security) is information security as applied to computers and networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters. Otherwise, in the computer industry, the term security -- or the phrase computer security -- refers to techniques for ensuring that data stored in a computercannot be read or compromised by any individuals without authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

Diagram clearly explain the about the secure computing

Working conditions and basic needs in the secure computing:

If you don't take basic steps to protect your work computer, you put it and all the information on it at risk. You can potentially compromise the operation of other computers on your organization's network, or even the functioning of the network as a whole.

1. **Physical security:**

Technical measures like login passwords, anti-virus are essential. (More about those below) However, a secure physical space is the first and more important line of defense.

Is the place you keep your workplace computer secure enough to prevent theft or access to it while you are away? While the Security Department provides coverage across the Medical center, it only takes seconds to steal a computer, particularly a portable device like a laptop or a PDA. A computer should be secured like any other valuable possession when you are not present.

Human threats are not the only concern. Computers can be compromised by environmental mishaps (e.g., water, coffee) or physical trauma. Make sure the physical location of your computer takes account of those risks as well.

2. **Access passwords:**

The University's networks and shared information systems are protected in part by login credentials (user-IDs and passwords). Access passwords are also an essential protection for personal computers in most circumstances. Offices are usually open and shared spaces, so physical access to computers cannot be completely controlled.
To protect your computer, you should consider setting passwords for particularly sensitive applications resident on the computer (e.g., data analysis software), if the software provides that capability.

3. **Prying eye protection:**

Because we deal with all facets of clinical, research, educational and administrative data here on the medical campus, it is important to do everything possible to minimize exposure of data to unauthorized individuals.

4. **Anti-virus software:**

Up-to-date, properly configured anti-virus software is essential. While we have server-side anti-virus software on our network computers, you still need it on the client side (your computer).

5. **Firewalls:**

Anti-virus products inspect files on your computer and in email. Firewall software and hardware monitor communications between your computer and the outside world. That is essential for any networked computer.

6. Software updates:

It is critical to keep software up to date, especially the operating system, anti-virus and anti-spyware, email and browser software. The newest versions will contain fixes for discovered vulnerabilities.
Almost all anti-virus have automatic update features (including SAV). Keeping the "signatures" (digital patterns) of malicious software detectors up-to-date is essential for these products to be effective.

7. Keep secure backups:

Even if you take all these security steps, bad things can still happen. Be prepared for the worst by making backup copies of critical data, and keeping those backup copies in a separate, secure location. For example, use supplemental hard drives, CDs/DVDs, or flash drives to store critical, hard-to-replace data.

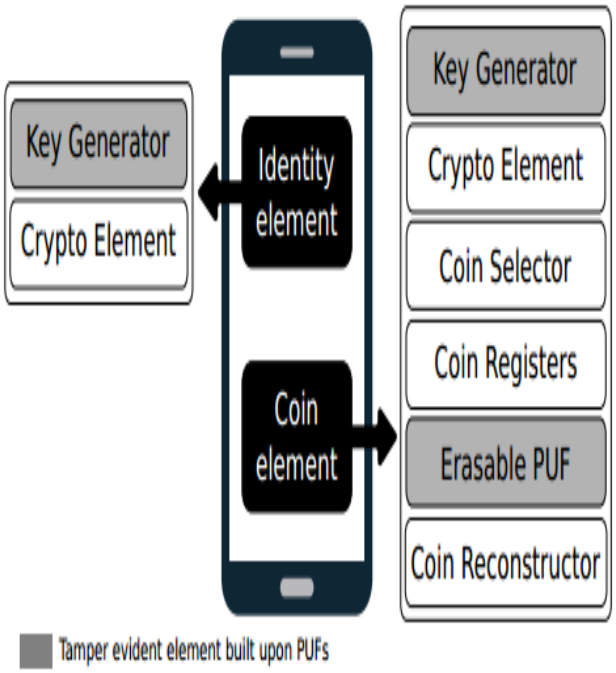
8. Report problems:

If you believe that your computer or any data on it has been compromised, your should make a information security incident report. That is required by University policy for all data on our systems, and legally required for health, education, financial and any other kind of record containing identifiable personal information.

Benefits of secure computing:

- **Protect yourself - Civil liability**:
  You may be held legally liable to compensate a third party should they experience financial damage or distress as a result of their personal data being stolen from you or leaked by you.
- **Protect your credibility - Compliance**:
  You may require compliancy with the Data Protection Act, the FSA, SOX or other regulatory standards. Each of these bodies stipulates that certain measures be taken to protect the data on your network.
- **Protect your reputation – Spam:**
  A common use for infected systems is to join them to a botnet (a collection of infected machines which takes orders from a command server) and use them to send out spam. This spam can be traced back to you, your server could be blacklisted and you could be unable to send email.
- **Protect your income - Competitive advantage:**
  There are a number of "hackers-for-hire" advertising their services on the internet selling their skills in breaking into company's servers to steal client databases, proprietary software, mergerand acquisition information, personnel details*et al*.
- **Protect your business – Blackmail**:
  A seldom-reported source of income for "hackers" is to·break into your server, change all your passwords and lock you out of it. The password is then sold back to you. Note: the "hackers" may implant a backdoor program on your server so that they can repeat the exercise at will.
- **Protect your investment - Free storage:**
  Your server's harddrive space is used (or sold on) to house the hacker's video clips, music collections, pirated software or worse. Your server or computer then becomes continuously slow and your internet connection speeds deteriorate due to the number of people connecting to your server in order to download the offered wares.

II.SYSTEM ARCHITECTURE



III.EXISTING SYSTEM

- 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

Disadvantages of Existing System

- 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.

IV.PROPOSED SYSTEM

- In this paper, 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.

Advantages of Proposed System

- FRoDO has been designed to be a secure and reliable encapsulation scheme of digital coins.
- FRoDO also applicable to multiple-bank scenarios. Indeed, as for credit and debit cards where trusted third parties (for short, TTPs) such as card issuers guarantee the validity of the cards, some common standard convention can be used in FRoDO to make banks able to produce and sell their own coin element.
- The identity and the coin element can be considered tamper-proof devices with a secure storage and execution environment for sensitive data.

V.IMPLEMENTATION

MODULES:

- System Construction Module
- Identity Element
- Coin Element
- Attack Mitigation

MODULES DESCSRIPTION:

System Construction Module

- In the first module, we develop the System Construction module with the various entities: Vendor, User, FRoDO, PUF, Attacker. This process is developed completely on Offline Transaction process.
- We develop the system with user entity initially. The options are available for a new user to register first and then login for authentication process. Then we develop the option of making the Vendor Registration, such that, the new vendor should register first and then login the system for authentication process.
- 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.

Identity Element

- In this module, we develop the Identity Element module functionalities. FRoDO does not require any special hardware component apart from the identity and the coin element that can be either plugged into the customer device or directly embedded into the device.
- Similarly to secure elements, both the identity and the coin element can be considered tamperproof devices with a secure storage and execution environment for sensitive data. Thus, as defined in the ISO7816-4 standard, both of them can be accessed via some APIs while maintaining the desired security and privacy level. Such software components (i.e., APIs) are not central to the security of our solution and can be easily and constantly updated. This renders infrastructure maintenance easier.

Coin Element

- In this module, we develop Coin Element. In this coin Element we develop Key Generator and Cryptographic Element. The Key Generator is used to compute on-the-fly the private key of the coin element. The Cryptographic Element used for symmetric and asymmetric cryptographic algorithms applied to data received in input and send as output by the coin element;
- The 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;
- The Coin Registers 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

Attack Mitigation

- In this module we develop the Attack Mitigation process. The read-once property of the erasable PUF used in this solution prevents an attacker from computing the same coin twice. Even if a malicious customer creates a fake vendor device and reads all the coins, it will not be able to spend any of these coins due to the inability to decrypt the request of other vendors.
- The private keys of both the identity and coin elements are needed to decrypt the request of the vendor and can be computed only within the customer device. The fake vendor could then try to forge a new emulated identity/coin element with private/ public key pair. However, identity/coin element public keys are valid only if signed by the bank. As such, any message received by an unconfirmed identity/coin element will be immediately rejected;

- Each coin is encrypted by either the bank or the coin element issuer and thus it is not possible for an attacker to forge new coins

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.

VII.REFERENCES

[1] J.Lewandowska. (2013). [Online]. Available: http://www.frost.com/prod/servlet/press-release.pag?docid=274238535

[2] R. L. Rivest, "Payword and micromint: Two simple micropayment schemes," in Proc. Int. Workshop Security Protocols, 1996, pp. 69–87.

[3] S. Martins and Y. Yang, "Introduction to bitcoins: A pseudoanonymous electronic currency system," in Proc. Conf. Center Adv. Stud. Collaborative Res., 2011, pp. 349–350.

[4] Verizon, "2014 data breach investigations report," Verizon, Tech. Rep., 2014, http://www.verizonenterprise.com/DBIR/2014/

[5] T. Micro, "Point-of-sale system breaches, threats to the retail and hospitality industries," University of Zurich, Department of Informatics, 2010.

[6] Mandiant, "Beyond the breach," Mandiant, 2014, https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf

[7] Bogmar, "Secure POS & kiosk support," Bogmar, 2014, http://www.bomgar.com/assets/documents/Bomgar_Remote_Support_for_POS_Systems.pdf

[8] V. Daza, R. Di Pietro, F. Lombardi, and M. Signorini, "FORCEFully off-line secure credits for mobile micro payments," in Proc. 11th Int. Conf. Security Cryptography, 2014, pp. 125–136.

[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 Proc. IEEE Int. Conf. Progress Informat.Comput., Dec. 2010, vol. 1, pp. 441–448.

[10] 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.

[11] G. Vasco, Maribel, S. Heidarvand, and J. Villar, "Anonymous subscription schemes: A flexible construction for on-line services access," in Proc. Int. Conf. Security Cryptography, Jul. 2010, pp. 1–12.

[12] K. S. Kadambi, J. Li, and A. H. Karp, "Near-field communicationbased secure mobile payment service," in Proc. 11th Int. Conf. Electron. Commerce, 2009, pp. 142–151.

[13] V. C. Sekhar and S. Mrudula, "A complete secure customer centric anonymous payment in a digital ecosystem," in Proc. Int. Conf. Comput., Electron.Elect. Technol., 2012, pp. 1049–1054.

[14] S. Dominikus and M. Aigner, "mCoupons: An application for near field communication (NFC)," in Proc. 21st Int. Conf. Adv. Inf. Netw. Appl. Workshops, 2007, pp. 421–428.

[15] 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.

[16] W.-S. Juang, "An efficient and practical fair buyer-anonymity exchange scheme using bilinear pairings," in Proc. 8th Asia Joint Conf. Inf. Security, Jul. 2013, pp. 19–26.

[17] M. A. Salama, N. El-Bendary, and A. E. Hassanien, "Towards secure mobile agent based e-cash system," in Proc. Int. Workshop Security Privacy Preserving e-Soc., 2011, pp. 1–6.
[18] C. Wang, H. Sun, H. Zhang, and Z. Jin, "An improved off-line electronic cash scheme," in Proc. 5th Int. Conf. Comput. Inf. Sci., Jun. 2013, pp. 438–441.
[19] J. Guajardo, S. S. Kumar, G.-J.Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in Proc. 9th Int. Workshop Cryptographic Hardware Embedded Syst., 2007, pp. 63–80.
[20] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical oneway functions," Science, vol. 297, no. 5589, pp. 2026–2030, 2002.
[21] S. Gomzin, Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions, 1st ed. New York, NY, USA: Wiley, 2014.
[22] Trustwave, "2013 global security report," Trustwave, 2013, http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf
[23] 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.
[24] G. Hong and J. Bo, "Forensic analysis of skimming devices for credit fraud detection," in Proc. 2nd IEEE Int. Conf. Inf. Financial Eng., Sep. 2010, pp. 542–546.
[25] C. R. Group, "Alina& other POS malware," Cymru, 2013, https://www.team-cymru.com/ReadingRoom/Whitepapers/
[26] W. Whitteker, "Point of sale (POS) systems and security," SANS Inst., Fredericksburg, VA, USA, 2014, http://www.sans.org/reading-room/whitepapers/bestprac/point-sale-pos-systemssecurity-35357
[27] U. R€uhrmair, F. Sehnke, J. S€olter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in Proc. 17th ACM Conf. Comput. Commun. Security, 2010, pp. 237–249.
[28] U. Rhrmair, H. Busch, and S. Katzenbeisser, "Strong PUFs: Models, constructions, and security proofs," in Towards Hardware- Intrinsic Security, series Information Security and Cryptography, A.-R. Sadeghi and D. Naccache, Eds. New York, NY, USA: Springer, 2010, pp. 79–96.
[29] P. S. Ravikanth. (2001). Physical one-way functions.Ph.D. dissertation, Massachusetts Inst. Technol., Cambridge, MA, USA [Online]. Available: http://cba.mit.edu/docs/theses/01.03. pappuphd.powf.pdf
[30] U. Rhrmair, C. Jaeger, and M. Algasinger, "An attack on PUFBased session key exchange and a hardware-based countermeasure: Erasable PUFs," in Proc. 15th Int. Conf. Financial Cryptography Data Security, 2012, vol. 7035, pp. 190–204.