ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Issue 3, March 2016

# Providing Security In Off-Line Transaction Using Frodo and PUF

[1]Mrs.A.Kumarideepika, M.E., [2]G.Yogeswari,
[1,2]Assistant Professor,
Dhanalakshmi Srinivasan College of Engineering and Technology, Chennai.

**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, 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

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.

## II. SECURITY TERMINOLOGY

Every industry has its own "language," the jargon that describes concepts and procedures peculiar to the field. Computer networking is infamous for the "techno talk" and the proliferation of acronyms that often mystify outsiders. Specialty areas within an industry often have their own brands of jargon, as well, and the computer security sub-field is no exception. It is not possible to provide a complete glossary of security-related terms within the scope of this chapter, but in this section, we will define some of the more common words and phrases that you may encounter as you begin to explore the fascinating world of computer security:

- ✓ **Attack** In the context of computer/network security, an attack is an attempt to access resources on a computer or a network without authorization, or to bypass security measures that are in place.
- ✓ **Audit** To track security-related events, such as logging onto the system or network, accessing objects, or exercising user/group rights or privileges.
- ✓ **Availability of data** Reliable and timely access to data.
- ✓ **Breach** Successfully defeating security measures to gain access to data or resources without authorization, or to make data or

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Issue 3, March 2016

resources available to unauthorized persons, or to delete or alter compute files.

- ✓ **Brute force attack** Attempt to "crack" passwords by sequentially trying all possible combinations of characters until the right combination works to allow access.
- ✓ **Buffer** A holding area for data.
- ✓ **Buffer overflow** A way to crash a system by putting more data into a buffer than the buffer is able to hold.
- ✓ **CIA triad** Confidentiality, Integrity, and Availability of data. Ensuring the confidentiality, integrity, and availability of data and services are primary security objectives that are often related to each other. See also availability of data, confidentiality of data, and integrity of data.
- ✓ **Confidentiality of data** Ensuring that the contents of messages will be kept secret. See also integrity of data.
- ✓ **Counter measures** Steps taken to prevent or respond to an attack or malicious code.
- ✓ **Cracker** A hacker who specializes in "cracking" or discovering system passwords to gain access to computer systems without authorization. See also hacker.
- ✓ **Crash** Sudden failure of a computer system, rendering it unusable.
- ✓ **Defense-in-depth** 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.

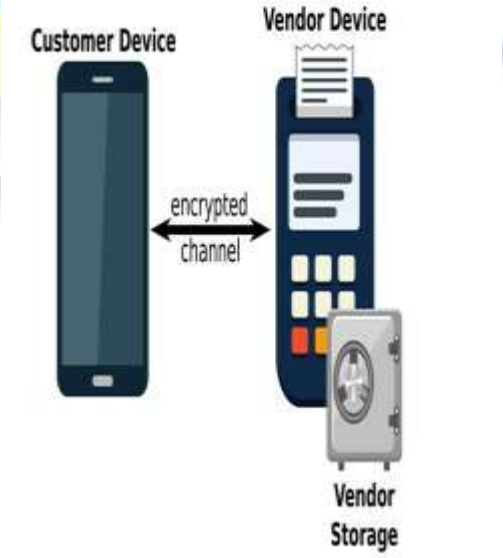
## III. EXISTING SYSTEM

Over the last years, several retail organizations have been victims of information security breaches and payment data theft targeting consumer payment card data and Personally Identifiable Information (PII). Although PoS breaches are declining, they still remain an extremely lucrative endeavor for criminals. Customer data can be used by cybercriminals for fraudulent operations, and this led the payment card industry security standards council to establish data security standards for all those organizations that handle credit, debit, and ATM cardholder information. Regardless of the structure of the electronic payment system, PoS systems always handle critical information and, oftentimes, they also require remote management.

## IV. PROPOSED & MODIFICATION SYSTEM

Table 1 depicts the most relevant attacks and attacker models that have been analyzed in this work. As such, it shows both the attacks that can be unleashed against the customer device or the
Transaction protocol, and the attacks aimed at threaten customer sensitive data.
Based on the capabilities and on the amount of devices that can be accessed during the attack, a taxonomy of the attackers is first introduced as follows: Collectorthis is an external attacker able to eavesdrop and alter messages being exchanged between the customer and the vendor device; Malicious Customer: (M. Customer) this is an internal attacker that can either physically open the customer device to eavesdrop sensitive information or inject malicious code Within the customer device in order to alter its behavior; Malicious Vendor: (M. Vendor) it is an internal attacker that can either eavesdrop information from the vendor device or inject malicious code in it in order to alter its behavior; Ubiquitous: this is an internal attacker with complete access
to all the involved devices. In FRoDO no restrictions are made on the capabilities oftheattacker that is always considered as ubiquitous.

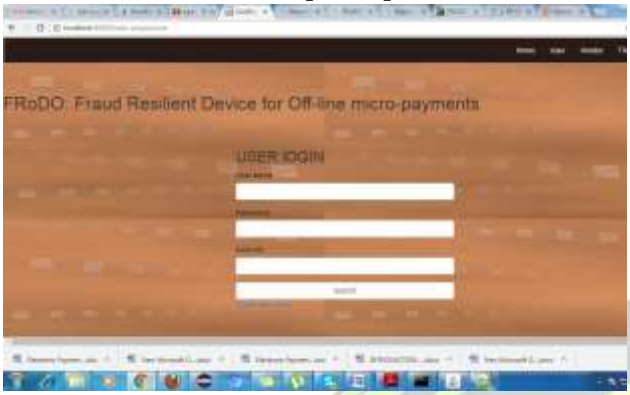
## V. FRoDO Model

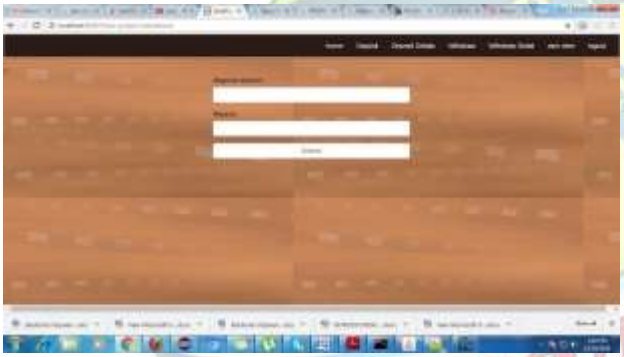


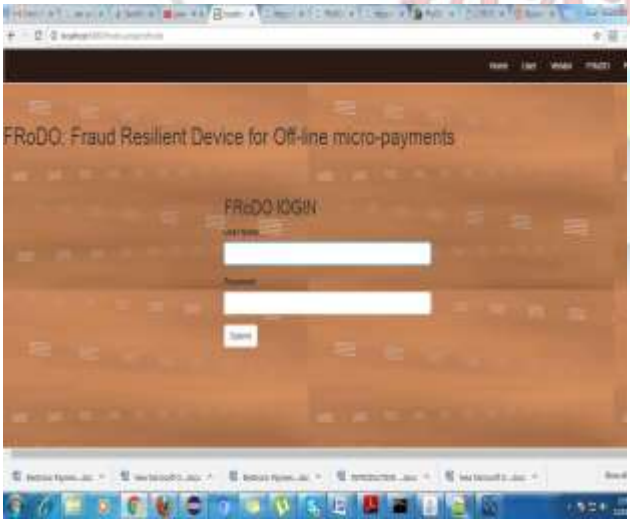
ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

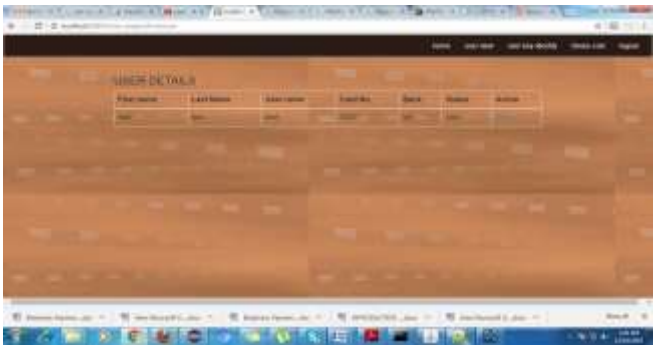
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Issue 3, March 2016

## VI. Sample output





## VII. 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.

## REFERENCES

[1] Bogmar, “Secure POS & kiosk support,”Bogmar, Technical Report, 2014.

[2] Chen.W, Hancke.G, Mayes.K, Lien.Y, and Chiu J.-H, “Using 3G network components to enable NFC mobile transactions anauthentication,”in IEEE PIC ’10, vol. 1, Dec 2010, pp. 441 –448.

[3] Daza.V, Di Pietro.R, Lombardi.F, and Signorini.M, “FORCE – Fully Offline secuReCrEdits for Mobile Micro Payments,” in 11th Intl. Conf.on Security and Cryptography, SCITEPRESS, Ed., 2014.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Issue 3, March 2016

[4] Golovashych.S, "The technology of identification and authentication of financial transactions. from smart cards to NFC-terminals," in IEEEIDAACS '05, Sep 2005, pp. 407–412.

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