Mobile phone based RFID architecture for secure electronic Payments using RFID credit cards

Geethapriya Venkataramani and Srividya Gopalan
Applied Research Group, Satyam Computers Services Limited
SID Block, Entrepreneurship Centre, IIISC Campus, Bangalore 560012, India
Email: {Geetha_Priya, Srividya_Gopalan}@satyam.com

Abstract

Online shopping using electronic payment scheme has gained a lot of popularity in recent years. In an electronic payment scheme using normal credit cards there is no way to genuinely identify owner of the credit card. Credit card fraud is the fastest growing crime all over the world. Any effort to plug the security hole especially for online payment is considered worthwhile.

RFID enabled credit cards are becoming increasingly popular as contactless credit cards [1]. We envision a future where RFID credit cards will be used for online shopping. RFID system has tremendous potential to render electronic payments more secure than normal credit cards. The word RFID enabled credit cards may bring in mixed passion, enthusiasm and perhaps even rage! This is partly paranoia and partly reality. The reality is that an intruder can read RFID cards without the user even noticing it. This brings in a zone of discomfort and leads to paranoia. Certain interactivity should exist to bring back this comfort to the user. This paper tries to make an effort in that direction. In this paper we propose mobile phone based architecture for secured electronic payments using RFID credit cards.

1. Introduction

While consumer’s shopping experiences have been enriched with the ability to buy commodities online it has raised a lot of security concerns too. One of the issues identified with the existing electronic payment scheme is incapability to recognize the true owners of credit card. A stolen credit card can be used to make genuine online purchases.

RFID technology is an amazing invention of its kind, which has the ability to convey embedded information in a tag without any physical contact with it. The reference [11] is an excellent tutorial on RFID basics. RFID is the next revolutionary step for various businesses such as supply chain management, apparel industry, inventory control, toll pay on fly etc. It has also found its way through credit card transaction system. Popularly called as RFID credit cards or contactless cards [1], they store data on a microchip that is embedded in the card’s plastic.

RFID is vulnerable to security breaches such as cloning, clandestine tracking and inventorying. These threats have raised reservations among credit card users to switch from normal credit cards. Problems and solution proposals related to privacy and security in RFID domain is well articulated in the survey paper by Juels [6]. Authors in [7] show how an intruder can use Ghost and Leech devices to read and emit information from a tag without the user being aware of it. This could result in charging somebody else’s credit card for a purchase. Consequently there is a need for an additional entity that can authenticate true owners of a credit card.

RFID credit card use is not widespread yet. The electronic payment for most part is still done using normal credit cards. We visualize a future where RFID credit cards are used for both in-person and online shopping. Many experts think that it is inevitable for contactless technology to converge on the mobile phone [1]. The advent of mobile-based RFID solutions has made this thought a promising reality. Companies like Nokia, etc are integrating RFID system with mobile phones either in tag mode or in reader mode or both [5]. These phones can enable online transactions using RFID credit cards in the near future but they must ensure security of the same. While research community is focusing on in-person transactions using RFID credit cards and related security concerns [2], there is a need for exploring the use of contactless credit cards for highly secure electronic payments.

Our contribution here is a first-cut presentation of a novel mobile-based architecture using RFID credit
cards to enable online transactions. We have addressed the concerns of credit card users who have qualms towards using a RFID credit card over normal ones and have proposed a system that strengthens the RFID credit card transactions against security breaches by incorporating intelligence at various RFID components. Our major goal is to enhance the security of electronic payments by using RFID credit card and mobile phone.

Our proposal includes the following:

a) We propose the features required for a secure contactless credit card (RFID credit card).

b) We identify a mobile RFID reader architecture and propose its functionalities to enable secure online transactions.

c) We propose the functionalities of RFID middleware collocated with the authentication server to provide security against fraud. The functionalities designed at the RFID middleware eliminate the need for users to remember any PIN or other key information.

This paper is organized as following. Section 2 provides related work in this field; Section 3 is the motivating scenario depicting the need for a secured online credit card transaction. Section 4 provides an overview of existing system for online transactions (with normal credit cards). Section 5 describes the proposed architecture in detail and discusses various attack scenarios rendered useless by our proposal and Section 6 concludes this paper with the scope for future extensions.

2. Related Work

M-Wallet [3] concept that has been recently introduced by Motorola involves storing credit card information in user’s mobile phone and used with PIN number during purchases. The possible drawback of this approach is the loss of mobile phone, which is as good as loosing an entire set of credit cards all at once. One might need to reload software, re-enter all the credit card information, go through re-validation process like getting new PIN numbers from every credit card company etc. To make matters worse data in the mobile phones can be hacked [4] and a stranger can view the types of credit cards with relevant information and all the receipts from one’s previous orders. Most of the credit card security schemes address information security on air but it is equally important to address security breaches where valid information is supplied from a stolen credit card.

Other payment methods such as Paypal etc offers mediator’s role for electronic payments with normal credit cards. To offer protection against purchases made with stolen credit cards, we need a genuine way to identify information from the stolen card versus the original one.

Our work looms at solutions to security aspect by authenticating the credit card and the user together rather than authenticating the validity of the credit card information alone.

3. Motivating Scenario

Jack forgot to pick up his credit card from a purchase counter at a shop, which was eventually picked up by a miscreant. Since then Jack has been using other credit cards and is not even aware of the credit card loss. The miscreant buys lots of expensive goods through phone and web. Miscreant’s data goes to the authorization server in encrypted mode and Credit card authentication servers authenticate his payments as credit card numbers and three digit verification code matches with their records. Miscreant collects his items and moves out of that address. Jack receives his monthly statement from the credit card company and is charged premium dollars for a set of purchases that he is not even aware of. He then calls up the credit card company and during this process he opens his wallet and realizes that his credit card is missing. The rest is the actual trauma Jack has to go through to prove his innocence by filing dispute and other timely follow up procedures that can go on and on. Here the victims are Jack, who has lost his mental peace and the Credit Card Company, wasting their time and money investigating this dispute.

4. Current Credit card Transaction system for Remote Shopping

In this section we analyze current credit card transaction system for online shopping. Figure 1 shows the credit card transaction system flow for online transactions.

A consumer logs into an e-commerce website provided by merchant and types in the credit card details (which might include 3 or 4 digit verification code, home phone number etc). The Credit card information is forwarded to issuing bank through the merchant’s acquiring bank where the payment is authorized or declined based on the interaction with the authentication server, credit limit available etc. If the transaction is approved, the transaction amount is reserved on the cardholder’s account and settled with the merchant subsequently.
The security hole here is that the credit card number and verification code on the back of credit card are the main inputs provided by buyers. Any one with this information can get away with online purchases. There is no way to identify the real owner of credit card.

5. Proposed RFID architecture for remote credit card transactions

In this section we propose our mobile phone based architecture for secured electronic payments using RFID credit cards.

5.1 System Requirements

In this sub-section we analyze the architectural requirements for online transactions using RFID credit cards. Figure 2 shows the system requirements that are required in addition to the existing infrastructure for electronic payments. The three additional components of the proposed architecture are identified as, a RFID credit card, a mobile phone with RFID reader and a RFID middleware collocated with the authentication server.

5.1.1 RFID credit card

We propose RFID credit cards to have encrypted information on its tag that can be decrypted only with private keys. There are various other options mentioned in Juels [6] but we find encrypted tag to be more suitable considering the credit card application. Information on the tag is encrypted during the supply of RFID card by credit card vendors. A private key is obtained by public key cryptography method and stored at the RFID middleware collocated with authentication server. As the data is already encrypted and etched on tag of the RFID credit card, there is no need for publishing the corresponding public key. Hence credit card companies can have their proprietary cryptographic principles for encryption and decryption. The private key generated to decrypt the encrypted tag information is stored in RFID middleware and it will be referred as Tag decryption key (TDKEY) in this document. We also propose that the contactless cards and corresponding PIN number be sent to the consumer’s mail address as two different mails.

5.1.2 Mobile phone with RFID reader

A mobile phone with RFID reader performs following functions.

a) Registers RFID credit card with RFID middleware collocated with authentication server
b) Downloads and stores encryption key provided by RFID middleware after successful registration.
c) During transactions, it encrypts the tag information using the key obtained during registration and transmits the encrypted tag information to RFID middleware through user’s wireless Internet service.
d) Can initiate reset phase during credit card loss or other security violation scenarios.

The mobile phone with RFID reader executes above functionalities in two phases, Registration or Activation phase and Transaction phase as detailed in the following sub-sections.

Role of RFID Reader during registration/activation Phase: When consumer reads the contactless card for the first time, the mobile reader transmits it to RFID

![Figure 1. Normal Credit Card Transaction System for remote shopping](image1)

![Figure 2. System requirements proposed for remote RFID credit card transactions](image2)
middleware. RFID middleware initiates the activation procedure and requests for personalized information from mobile device. The user enters personalized information through a vendor specific application that runs in the mobile device. The information is transmitted through mobile device’s Internet connection to RFID middleware collocated with authentication server. When server authenticates information the mobile reader’s application downloads personalized encryption key transmitted by RFID middleware. The encryption/decryption keys are dealt in detail under ‘Key generation and Management at RFID middleware’ heading.

Role of RFID Reader during Transaction Phase: During transaction phase (during online shopping), the mobile reader reads encrypted tag, performs second level encryption of the tag information with the encryption key that was provided by RFID middleware after successful registration. This doubly encrypted data is fully decrypted at RFID middleware before sending the same to authentication server. The second level of encryption at mobile reader ensures the legitimacy of the user.

An interesting architecture for Mobile Based RFID reader is proposed in a reference [9]. We think that the software protocol architecture referred in this document, for most part meets our requirements for reader architecture. Figure 3 shown is an adaptation from the software architecture described in reference [9]. Mobile Phone with RFID reader consists of layers as shown in Figure 3. A detailed description of the layers shown in figure can be obtained from reference [9]. We will analyze only the WIPI based application layer in this document.

WIPI (Wireless Internet Platform for Interoperability) is the standard specifications for the mobile platform made by the Mobile Platform Special Subcommittee of the Korea Wireless Internet Standardization Forum (KWISF) [10]. These are standard specifications necessary for providing an environment for mounting and implementing applications downloaded via the wireless Internet on the mobile communication. Any RFID mobile device can access GSM, 3G or other wireless Internet services using applications developed at the WIPI layer. Using WIPI backbone, content providers can develop applications that run seamlessly on any mobile platform.

We propose that the RFID credit card transaction application must be provided by the vendors (credit card suppliers) at the WIPI layer to interface with the RFID reader protocol stack to effectively read and transmit tag information. Vendor specific application should also take care of storing encryption keys and performing encryption procedures. User APIs along with other software components must also be a part of this application to provide user interface during registration and transaction phases such as invoking tag reading mode during online transactions and sending encrypted tag information using mobile user’s internet service.

5.1.3 RFID Middleware at the authentication server

We propose RFID middleware architecture to be collocated with authentication server such that the activation and authentication requests go only through the RFID middleware rather than going directly from third party banks or servers. RFID middleware is bestowed with following functions

a) It interacts with the mobile phone (with RFID reader) to register and activate the contactless credit card for online transactions.

b) At the end of successful registration, RFID middleware provides a secret and personalized encryption key to the mobile device. The associated decryption key is stored in RFID middleware.

c) During transactions, RFID middleware performs decryption procedures to decrypt tag information and provides it to authentication server for further
authentication. The tasks of RFID middleware are explained in detail under System Operation in section 5.2.

Before we go into the details of system operation it is important to understand key generation, key supply and key management functionality of RFID middleware. There are 3 types of keys associated with the RFID credit card that is managed by RFID middleware collocated with authentication server. The keys are meant for providing security without users having to remember PIN numbers or any other information during transactions. The key operations are non-transparent to the users.

Tag decryption Key (TDKEY): This is a decryption key generated when tag information is encrypted and etched on the card plastic. It is a private key that can be generated using public key cryptography and is stored at RFID middleware. The encrypted tag information is further etched on the RFID credit card. Original tag information can be decrypted only with this key.

Mobile Reader Authentication key (MRAKEY): This key is generated by RFID middleware and is issued to the credit card owner’s mobile phone at the end of activation phase during card registration. It is a public key with digital signature. This key must be securely transmitted to the mobile phone and should not be published. The mobile device must store this key and use it for all future transactions. The user need not be aware of this key. The vendor specific application at mobile phone is responsible for storing and using this key during transactions.

Mobile Reader Verification Key (MRVKEY): This is a decryption generated and stored at RFID middleware during the generation of MRAKEY. It is a private key for decrypting data encrypted with MRAKEY. It is used to verify the source (credit card owner’s mobile phone) from which the information was received. The role of various keys is shown in Table 1. The letter E refers to encrypted value.

<table>
<thead>
<tr>
<th>Table 1. Role of Keys at RFID entities</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFID credit card Tag: E_{TDKEY}(Data)</td>
</tr>
<tr>
<td>Reader: E_{TDKEY}(Data) _MRAKEY _ E_{TDKEY}(Data)</td>
</tr>
<tr>
<td>RFID middleware (collocated with transaction server): E_{E_{TDKEY}(Data)} _MRVKEY _ E_{TDKEY}(Data)</td>
</tr>
<tr>
<td>E_{TDKEY}(Data) _ TDKEY _ Data</td>
</tr>
</tbody>
</table>

Please note that the actual cryptosystem details for generating keys are out of scope for this document. Only the need for cryptography is pointed out here.

5.2 System Operation

In this section we explain the detailed operation of the remote transaction system using contactless credit cards. The system operation can be classified into 3 phases

(i) Registration Phase
(ii) Transaction Phase
(iii) Reset Phase

5.2.1 Registration/Activation Phase

Figure 4. Information exchange during Registration Phase

During this phase the consumers register their contactless card for remote transactions. This is equivalent to credit card activation procedure. We assume that the credit card company sends RFID credit cards to the consumer’s address by mail and PIN number in the subsequent mail. This is analogous to the ATM card delivery through mail. The information exchanged during registration phase is depicted in Figure 4. The user reads his contactless credit card using mobile phone. This data is sent to the credit card company for registration or transaction process. RFID middleware collocated with authentication server maintains a table with MRVKEY values against encrypted tag value. When tag information is obtained at the RFID middleware, the encrypted tag information is verified against MRVKEY value.
5.2.2. Transaction Phase

During transaction phase consumer uses his mobile phone to buy an item online. The user’s mobile phone reads user’s RFID credit card and performs encryption with keys that was provided by RFID middleware after successful registration. This doubly encrypted information is transmitted to merchant’s website. Flowchart shown in Figure 7, describes the flow of events in the mobile phone with RFID reader during transaction phase.

From the merchant’s perspective there is no difference between RFID credit card transaction and normal credit card transaction. The online merchant transmits this doubly encrypted information to its acquiring bank, which is eventually routed to the RFID middleware through the credit card company’s issuing bank.

At the RFID middleware information decryptions occur to retrieve the original tag information. The original tag information is the actual credit card detail that is authenticated by the authentication server. The flow of events at RFID middleware during transaction phase is depicted in Figure 8. We denote encryption procedure by $E$ and decryption procedure by $D$. Let $E(T)$ represent the encrypted tag information.
Following the roles of keys as mentioned in Table 1, the encryption/decryption procedures can be represented as shown in a flowchart in Figure 8. Here T represents the original credit card information that is being transmitted to the authentication server for final authentication/approval.

5.2.3. Reset Phase

During reset phase the MRVKEY is deleted from the MRVKEY table and associated MRAKEY is useless at the mobile phone. Reader information encrypted using MRAKEY is rendered useless, as it cannot be decrypted at the RFID middleware. This is a de-activation mechanism and can be used if a credit card loss is reported or during other security violations.

5.3 Overall System Flow

In this section we analyze the overall system flow for a complete understanding of the proposed framework. The user obtains a RFID credit card and associated PIN from the credit card company. The tag in the RFID credit card contains encrypted information whose decryption key is stored at the RFID middleware (collocated with transaction server) and not published. This key is referred as TDKEY and is reserved against the owner of the credit card. The user registers the card by reading the encrypted tag using his RFID enabled mobile phone.

During the registration process the credit card application on the mobile phone transmits this information to the RFID middleware using consumer’s wireless ISP. Registration phase is initiated where the user provides personal information (PIN number etc.) that is verified by RFID middleware (on behalf of the credit card company). On successful registration, RFID middleware generates MRAKEY and associated MRVKEY using advanced cryptosystems with digital signatures. (Information encrypted with a particular MRAKEY can be decrypted with an associated MRVKEY only). MRAKEY is transmitted to the consumer, which is downloaded and stored in the user’s mobile phone.

During transaction phase, a consumer logs into the merchant’s e-commerce website and selects items for purchase with RFID as a payment mode. The application in the mobile phone starts the user APIs and other related modules, sets the mobile phone in tag read mode, reads the tag, encrypts the tag information further using MRAKEY (stored in mobile phone). When consumer confirms the payment amount and submits the same, the online merchant receives a set of encrypted information that is sent to merchant’s acquiring bank and then to the issuing bank. Issuing bank sends this information to authentication server via the proprietary RFID middleware.

RFID middleware decrypts the information using MRVKEY first, and then performs another level of decryption using TDKEY. The second level of decryption with TDKEY results in original credit card information and is sent to authentication server. The rest of the steps follow the online transaction process for normal credit cards. It is very important to note that there is absolutely no need for users to deal with or remember any keys [TDKEY, MRAKEY or MRVKEY] for transaction. TDKEY and MRVKEY are available at the RFID middleware while MRAKEY is downloaded into the mobile phone. The mobile user need not be aware of MRAKEY as the application will take care of encryption using required keys. Personal information exchange occurs only during the initial registration process.

5.4 System Security

In this section we analyze some credit card loss scenarios and justify how the proposed infrastructure can provide security to the credit card owner.

Scenario 1: Consider the motivating scenario mentioned in section 3. Let us assume that Jack has RFID credit card instead of the normal one and has registered it with the credit card company for online transactions using his mobile phone. Jack’s mobile phone has a valid MRAKEY. When the miscreant uses Jack’s RFID card for online purchases using his own mobile phone, the authentication fails since the...
mobile phone has no valid re-encryption key [MRAKEY] (it is available only in Jack’s mobile phone). Since the mobile phone did not encrypt the tag information using a valid MRAKEY (available with Jack’s mobile phone), decryption using MRVKEY and TDKKEY further results in invalid data resulting in authentication failure. Even if the miscreant is a registered owner of his own RFID credit card, reading a stolen RFID credit card results in authentication failure because of the key mismatches at RFID middleware. A user can trigger a reset phase by calling the credit card company or repeated authentication failures can enable a temporary reset phase for security reasons.

Scenario2: If a Mobile Phone is lost, a mobile phone with MRAKEY without a contactless credit card is no good anyways. The user can call the credit card company to initiate a reset phase after which a new credit card with a new mobile phone can be registered.

Scenario3: The extreme case is when both the mobile phone and the contactless credit card are lost. While this case cannot be ruled out (happens to users when their hand bag is lost) we believe an external user input such as biometrics or PIN for every transaction can be explored. Also, it is reasonable to assume that a bag loss is more noticeable than the loss of a credit card alone to deactivate the card immediately and avoid any misuse of the card.

5. Conclusion and Future enhancements

In this paper we have proposed an application framework using RFID credit cards for electronic payments. Most of the credit card frauds thrive either because an owner is unaware of the physical loss of the card or the card information is stolen by a miscreant. The proposed architecture beats the first odd by requiring mobile phone and the credit card together for validating a transaction and the second odd by etching an encrypted tag in RFID credit cards.

Current electronic payment system does not uniquely identify the credit card owner. A stolen credit card can be used for genuine online purchases. With more contactless cards being issued and more merchants accepting contactless payments every day, it is estimated that $11.6 billion will be transacted via contactless payment systems by 2009 [1]. When RFID credit cards dominate future it is very likely to be used for electronic payments also. We believe that RFID credit cards, mobile phone together with a RFID middleware collocated with authentication server can offer a more secure electronic payment infrastructure. RFID middleware can be functionally elaborated further to alert fraud purchases to the owners and provide context related information from other marketing prospective.

Acknowledgements

We like to thank Mr. Gopi.K.L of Satyam Computer Services Limited, for his valuable inputs and reviews.

7. References

[1]. Contact less credit cards consumer report 2006 http://www.findcreditcards.org/reports/contactless.html
[2]. How safe are the new contact less payment systems http://www.cioinsight.com/article2/0,1540,1829513,00.asp
[8]. Haedong Lee, Dooho Choi, Sokjoon Lee, and Howon Kim, “A Study on RFID Privacy Mechanism using Mobile Phone”, TRANSACTIONS ON ENGINEERING COMPUTING AND TECHNOLOGY DECEMBER 2005
[10]. Wireless Internet Platform for Interoperability (WIPI), http://wipi.or.kr