Macquarie University, Sydney

Overview of Micropayment Technology

Final Project Report

Vishal Bharat Sharma

Supervisor: Josef Pieprzyk

Abstract

Payment System is a system to supports transfer of funds between two parties. It can be defined as a set of rules, protocols to complete a transaction. There are number of payment systems available for a consumer to pay for the services/goods, but all these payment systems can be divided into two main types, traditional payment system and electronic payment system. But these systems have their own limitations, which are mostly related to very small payments. To overcome these limitations new payment system known as micropayment system is proposed. It is not as that this payment system can't be used for large payments but the system is designed in such a way to provide convenience to users and that too at fast speed. Radio Frequency Identification (RFID) technology is used in these systems. Few RFID based systems are already in use the most common example is electronic toll tax system, in some countries it is used in public transport system for ticketing, and etc. RFID system consists of three main components RFID tag/card, RFID reader and middleware. RFID is a powerful emerging technology it offers number of advantages but has some drawbacks too. Exploiting these weaknesses different groups have successfully attempted to hack these systems. There are number of issues that authorities need to considered, before deploying payment system based on this technology. The aim of this work is to provide an overview of RFID as a technology to be used in future payment systems. This project starts with the study of basic payment systems, followed by study of current micropayment system in use at various locations in different applications. In recent time successful attacks have been launched against vulnerabilities of this technology, these attacks have been analyzed and studied in detail to get the ideas for building new systems in future. The outcome of this work is the deep understanding of RFID as a technology to be used in payment systems, discussing its main strengths and vulnerabilities.

Acknowledgement

Thanks to Josef Pieprzyk for his guidance and support, and Robert Dale for useful feedback on this work. And also I would like to express my gratitude to all those who gave me the possibility to complete this report.

Contents

1 Introduction

Payment systems are systems used to settle financial transactions. Currently there are two payment systems in use traditional (that deals mainly with cash) and electronic payment system (that deals with all digital transactions). Micropayment system is considered different as it uses different mechanism for authentication and authorization of a transaction.

1.1 Payment Systems

Payment systems are one of the fundamental pillars of modern economies and it can be defined as a collection of technologies, laws, protocols, and customs that make it possible for people and companies to pay money to each other (Kniberg, 2002). All payment systems have definite characteristics and qualities and they find their application in various systems on the basis of these qualities and characteristics. Payment systems currently in use can be divided into mainly two types.

- Traditional Payment System
- Electronic Payment System

Traditional Payment System

The traditional payment systems cover all the payments which are made using cash and paper documents such as bank checks, drafts and money orders. This is the most convenient mode of payment. The main advantage of using cash is that it doesn't need any authentication from external party and secondly it provides anonymity as there are very less details of cash payments in general. So why don't we just stick to cash? The fundamental problem with cash is that two parties can't exchange money without meeting, third party can be involved but it slows down process. Another problem with cash is that a currency has a fixed set of denominations, which makes it difficult to handle extremely large or extremely small transactions. There is nothing wrong with cash other than the fact that there are occasions when people don't have any and have to rush off to find an ATM, or there are occasion when you need the exact change and you have nothing but notes. Or there may be times when you have too much change and your pockets are bulging with the inconvenience of it (Juniper, N. D.). Examples of traditional payment system are all the businesses supporting cash.

Electronic Payment System

A payment system, in which the transactions take place digitally – usually through network connection, can be defined as an electronic payment system (Jari Kytojoki, 2000). An electronic payment system covers all card based payments, internet based transactions, and payments made through mobiles. In the transactions

made by card the main task of electronic payment systems is to authenticate the user requesting for transaction using some mechanism (PIN number or Signature) that it is the legitimate user and authorization for the transaction on the basis of checking his account. This authentication and authorization is done by the card issuing or service providing authority. Whereas in mobile payments, authentication is not required as the SIM card issued by the operator is used for this authentication and authorization is either made by sending message on special number or by making a call on special number. On internet authentication is done on the basis of the information feed by user on computer, and authorization is done on the basis of that information. All these systems have been developed by thinking of macro-payments considering high security.
Transactions made by cards have to pay some transaction cost (fixed and percentage) which depends upon the merchant, therefore some merchant support very low amount to be paid by card and some don't. The cards (magnetic stripe/optical memory) are the main source of payments in electronic payment system. Although these cards are widely used, but they posses some limitations, first the technology used in this system is too slow it takes around 1-2 seconds to process one magnetic stripe card[1], and the authentication and authorization for transaction involves the issuing authority, which adds up extra delay. The payments made by mobile and internet also support only some specific types of payments, and moreover are dependent on cards. Therefore they can't be considered as an alternative to current electronic payment system. Example, all the major businesses support card payments.

Micropayment Systems

Micropayment systems also fall in the category of electronic payment systems, but these are considered different from the normally used cards & systems due to following reasons.

- The technique used in this system is RFID, in which card needs to be in proximity of reader to complete the transaction.
- It is faster than all the techniques used.
- Authentication and authorization is done on the spot, without contacting main server. But, not in all cases, there are few exceptions.
- It is mainly pre-paid based system (User need to reload[2]).

Example of this payment system is electronic toll collection system, E-tags.

(Kniberg, 2002) in his work on micropayment systems, revealed the main characteristics that system should posses to be successful in micropayments. Following should be taken in account by authorities while designing micropayment sys-tem.

Important characteristics

[1] http://www.card-reader.com/idscan_magnetic.htm
[2] http://www.octopuscards.com/consumer/payment/reload/en/index.jsp

- Ease of joining: It should be easy to join as user could be scared away if the payment system is too complex.
- Ease of use: Systems should be easy to use and load/reload otherwise it won't be successful.
- Pervasiveness: It is not worth joining a new payment system just to make one single payment; it is only worth it if the same system can be used in many different situations.
- Fixed transaction cost: The transaction cost shouldn't be there as the payment is so low, in some cases it may be more than the amount to be transferred.
- Transaction speed: Most people make small payments relatively often as compared to large payments. Delay in payment system transactions would add up more problems.
- Security: System should be able to provide at least basic level security.

1.2 Technologies In Use In Payment Systems

In electronic payment system numbers of technologies are in, these technologies have different characteristics which decide their use in various systems. Despite the very advantages and benefits, RFID create security issues unique to it.

Magnetic Stripe Cards

Magnetic Stripe Cards are in use from a while, in these cards there is a magnetic stripe which stores information. These cards are read by physical contact while swiping past a reading head. These magnetic stripes allows to edit or new data onto them. These can be programmed to be used with some authentication mechanism or even without it (Halliday, 1997).

Optical Memory Cards

Optical memory cards use a technology similar to the one used for music CDs or CDROM's. A panel of the "gold colored" laser sensitive material is laminated in the card and is used to store information. The material is comprised of several layers that react when a laser light is directed at them. The laser burns a tiny hole in the material which can be sensed by a low power laser during the read cycle (Halliday, 1997).

RFID Cards

Radio Frequency Identification Cards also known as contactless cards, these cards consists of an antenna and integrated circuit. Antenna is used for transmitting and receiving signals and integrated circuit is for storing and processing information, modulating and demodulating a radio frequency signal. These are generally of two types; active which contain a battery and thus can transmit its signal autonomously, and passive which have no battery and require an external source to

initiate signal transmission. (Halliday, 1997); (Curtin J., 2007); (Feldhofer M., 2004).

Smart Cards

These cards have an embedded micro-chip in them; they differ from magnetic stripe cards in mainly two ways: the amount of information that can be stored is much greater, and some of them can be reprogrammed to add, delete or rearrange data. There are two types of smart cards. The first is a just a memory card, these are used to store information. The second type of card is a true "smart" card where a microprocessor is embedded in the card along with memory. This card has the ability to make decision about the information stored on it (Halliday, 1997).

Table1 given below compares some of the characteristics of the cards mentioned above, it compares the max data capacity, cost and their transaction time.

	Maximum Data Capacity	Processing Power	Cost of Card	Average Transaction Time
Magnetic Stripe Cards	140 bytes	None	$0.20 - $0.75	25 Seconds
Optical Memory Cards	4.9 Mbytes	None	$7 - $12	Not Available
RFID Cards	1Kbyte – 4 Kbytes	None	$0.40-	15 Seconds
Smart Cards (IC Memory Cards)	1 Kbyte	None	$1 - $2.50	Not Available
Smart Cards (IC Processor Cards)	8 Kbytes	8-bit CPU, moving to 16- and 32-bit	$7-$15	Not Available

Table1. Comparison of different characteristics of different types of cards

Internet & Mobile

In the past few years, the Internet has grown at rapid rate. It has become the global data communications and sharing infrastructure. The tremendous growth of the Internet, particularly the World Wide Web (WWW), has led to a critical mass of consumers and firms participating in a global on-line marketplace. Internet and on-line market has grown exponentially but the there aren't much advancement in relation to payment system. Till date Credit Card based payments are widely

accepted, although the techniques used to protect data have improved over the time. Now a day's few systems have started supporting transactions from bank accounts. But there isn't any successful system for micropayments till date. Some payment systems are there which are good for dealing with some specific type of goods/information/services but there isn't any universally accepted payment system for all internet based transactions. There are some systems which works with mobiles, but aren't much successful.

There are number of ways in which a payment can be made from a mobile. Some methods are popular in some region and others are common in other region. For example method of paying for digital content by sending Premium Rate SMS is common in Europe, whereas in Far East and China, users take their mobile phone to the store to pay for goods via contactless credit/debit card scheme (Howard Wilcox, 2008). Mobile can be used to pay remotely and also by physically being present there.

Internet and mobile as support only specific types of payments are not studied in detail and moreover the payments made through these systems depends upon the cards that are currently in use. These are considered as an alternative technology for micropayment systems.

1.3 Security Technology Used

In electronic payment system, the transaction is authentication and authorization is done through system. Cryptography is one of the security mechanism that is mostly used in different manners to achieve the required level of security.

Cryptography

Cryptography is the science of using mathematics to encrypt and decrypt data. It enables you to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient. Cryptography is necessary when communicating over any un-trusted medium, which includes just about any network. (Trappe, 2006)

Specific Security requirements

- Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
- Non-repudiation: A mechanism to prove that the sender really sent this message.

There are, in general, three types of cryptographic schemes typically used to accomplish these goals: (Trappe, 2006) (GovernmentSecurity.Org, N. D.)

- Secret Key Cryptography: Uses a single key for both encryption and decryption.
- Public Key Cryptography: Uses one key for encryption and another for decryption.
- Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information.

In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into ciphertext (using cipher), which will in turn be decrypted into usable plaintext.

There are several widely used secret key cryptography schemes and they are generally categorized as being either stream ciphers or block ciphers.

- Stream ciphers operate on a single bit, byte, or (computer) word at a time, and implement some form of feedback mechanism so that the key is constantly changing.
- A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same ciphertext when using the same key in a block cipher whereas the same plaintext will always encrypt to different ciphertext in a stream cipher.

Cipher

In cryptography, a cipher (or cypher) is an algorithm for performing encryption and decryption, a series of well-defined steps that can be followed as a procedure. When using a cipher the original information is known as plaintext, and the encrypted form as ciphertext. The ciphertext message contains all the information of the plaintext message, but is not in a format readable by a human or computer without the proper mechanism to decrypt it; it should resemble random gibberish to those not intended to read it. The operation of a cipher usually depends on a piece of auxiliary information, called a key. The encrypting procedure is varied depending on the key, which changes the detailed operation of the algorithm. A key must be selected before using a cipher to encrypt a message. Without knowledge of the key, it should be difficult, if not nearly impossible, to decrypt the resulting ciphertext into readable plaintext. (GovernmentSecurity.Org, N. D.)

2 Micropayment Systems Currently in Use

There are number of micropayment systems currently in use and use different technologies to perform authentication and authorization in order to complete the transaction.

- Public Transport System
- Toll Tax Collection Systems
- Payment of fuel at Service Stations
- Consumer Transactions

2.1 Public Transport System

RFID based contactless card are being used in number of countries for ticketing systems around the world. These cards are mostly prepaid, user need to load some amount in them before using. In this system user just need to waive their card in front of a reader at the time of boarding and alighting from public transport, the fare is then calculated and deducted from the user's account. The system is able to complete the whole transaction in just 0.3 seconds.

First such a system was launched in Sept. 1997 in Hong Kong for the territory's mass transit system. The name of the card is Octopus. The use of Octopus card system has grown from territory's mass transit system into a widely used payment system for virtually all public transport in Hong Kong. According to Octopus Cards Limited, operator of the Octopus card system, there are more than 17 million cards in circulation, more than twice the population of Hong Kong. The cards are used by 95 percent of the population of Hong Kong aged 16 to 65, generating over 10 million daily transactions worth a total of about HK$29 billion a year.

The similar system was launched in Moscow Metro in 1998 and the cards used are called Transport Cards. Initially these cards were available as 'unlimited' and 'social' tickets. The unlimited card can be programmed for 30, 90, and 365 days. The social cards are free for elderly people and some privileged categories of citizens; they are available to school pupils and students at a heavily reduced price. And later on become available for 1, 2, 5, 10, 20 and 60 journeys versions. The Moscow Metro became the first metro system in Europe to fully implement smartcards on September 1, 1998. Magnetic cards were stopped being accepted in late 2008, making Moscow metro world's first major public transport system to run fully on contactless automatic fare collection system based on Philips NXP MIFARE technology.

The EZ-Link card is a contactless smart card based on the Sony FeliCa smartcard technology and used for the payment of public transportation fares in Singapore, with limited use in the small payments retail sector. Established in 2001, it was promoted as the means for speedier boarding times on buses. As of 2007[update], there are over 10 million. EZ-Link cards in circulation, with 4 million card-based transactions occurring daily.

The implementation of SmartRider was originally planned for January 2005, but due to problems with implementation of reader technology, the key dates changed a number of times. SmartRiders became available to members of the public from January 14, 2007.
The SmartRider was rolled out progressively to different groups of customers:

Car Parking: From 22nd October to 4th November 2007, new Pay'n'Display machines were trialled at the Stirling Interchange car park so that SmartRider users can pay for their parking with their SmartRider This facility has since been extended to 13 other stations on the network.

The card was first issued to the public in July 2003 with a limited range of features and there continues to be a phased introduction of further functions. By March 2007 over 10 million Oyster cards had been issued, and more than 80% of all journeys on services run by Transport for London used the Oyster card.

2.2 Toll Tax Collection System

Electronic toll collection (ETC), an adaptation of military "identification friend or foe" technology, aims to eliminate the delay on toll roads by collecting tolls electronically. It determines whether the cars passing are enrolled in the program, alerts enforcers for those that are not, and electronically debits the accounts of registered car owners without requiring them to stop.

Norway has been the world's pioneer in the widespread implementation of this technology. ETC was first introduced in Bergen, in 1986, operating together with traditional tollbooths. In 1991, Trondheim introduced the world's first use of completely unaided full-speed electronic tolling. Norway now has 25 toll roads operating with electronic fee collection (EFC), as the Norwegian technology is called (see AutoPASS). In 1995,

Portugal became the first country to apply a single, universal system to all tolls in the country, the Via Verde, which can also be used in parking lots and gas stations. The United States is another country with widespread use of ETC in several states, though many U.S. toll roads maintain the option of manual collection.

2.3 For Payment of fuel at Service Stations

Speedpass is a keychain RFID device introduced in 1997 by Mobil Oil Corp. (which merged with Exxon to become ExxonMobil in 1999) for electronic payment. It was originally developed by Verifone. As of 2004, more than seven million individuals possess Speedpass tags, which can be used at approximately 10,000 Exxon, Mobil and Esso gas stations worldwide.

Speedpass was one of the first widely deployed consumer RFID payment systems of its kind, debuting nationwide in 1997 far ahead of today's VISA and MasterCard RFID trials, and the RFID/EPC (Electronic Product Code) privacy controversy.

2.4 Consumer Transactions

There is no dedicated contactless card that can be used for consumer transactions. There is both success and failure story of two successful based cards, when used

for consumer transaction. Octopus is one of the few cards that are supported by selective merchants. It was introduced for fare payment on the MTR initially, but can now be used to make purchases for consumer products at many stores in the territory; it is accepted by more than 1,000 merchants. The card can be used in many soft drink vending machines, pay phones, photo booths, parking meters, and car parks.

On the other hand, Speedpass was deployed experimentally in fast-food restaurants and supermarkets in select markets. McDonald's alone deployed Speedpass in over 400 Chicagoland restaurants. Additionally, Stop & Shop grocery chain tested Speedpass at their Boston area stores and removed the units in early 2005. The test was deemed a failure and McDonald's removed the scanners from all their restaurants in mid 2004. Speedpass has also been previously available through a Speedpass Car Tag and Speedpass-enabled Timex watch.

Keeping in mind the convenience and speed, number of credit card companies has started issuing contactless credit cards to their clients. But at the moment they are combined with magnetic stripe card and can be used in either way. (November 18, 2005)

Chase Bank USA is testing Visas and MasterCards with RFID technology called "blink," which eliminates the need for purchasers to sign and swipe. Instead, the buyer just waives the card in front of a scanner.

Contactless cards fitted with RFID chips are now available, and solution providers should expect to see opportunities in the POS market for new systems and upgrades.

The process involves waving a credit card with the embedded RFID chip in front of a scanning device that connects it with the credit account. The card must be within 20 centimeters of the scanner in order to be read.
Purchases can be made almost instantly without a swipe of a magnetic strip or a signature. In spite of technological bells and whistles, credit cards will still carry magnetic strips for use at more traditional points of sale and will continue to display account numbers.

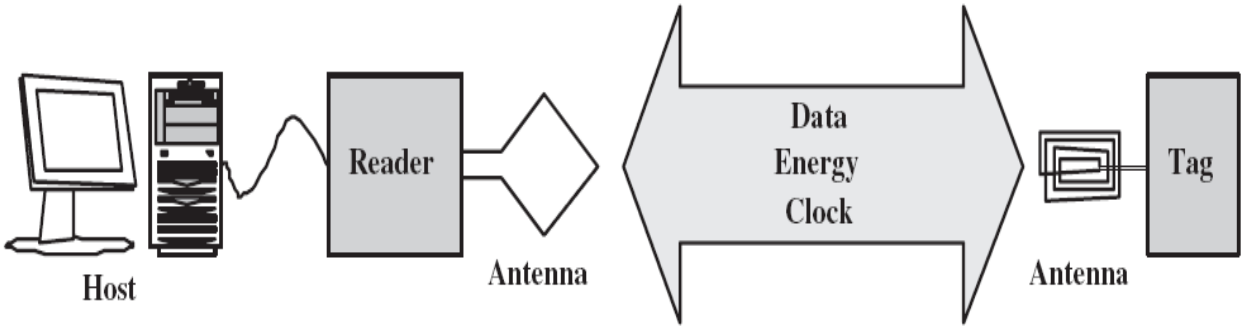
3 Micropayment Technology (RFID)

Radio Frequency Identification (RFID) is a general term that is used to describe a system that transmits the identity (in the form of a unique serial number) of an object wirelessly, using radio waves. There are three main components of an RFID system. RFID is an emerging technology in payment systems, it offers number of advantages over existing technologies, but it has some unique weaknesses.

3.1 Introduction[3]

RFID as name implies is a wireless technology, which works on Radio Frequency. In RFID systems an active or passive RFID tag is attached to, or embedded in, an item which communicates its identity to an RFID reader using radio frequency wave. The RFID tag provides the reader with a sequence of data that encodes a unique identity for that object. In the case of passive RFID tags, the radio frequency waves power the tags to enable it to communicate, when it is within the reading-range of the RFID reader. RFID systems do not require line-of-sight and work contactless. Figure 1 [4]shows the basic structure of RFID system.

Realization of the benefits of the RFID in the business community is fostering explosive growth in RFID-enabled systems in different applications at a tremendous rate. Number of these system have been deployed in number of industries such as logistics, supply chain management, library item tracking, medical implants, road tolling, building access control, transportation and etc. An important aspect of RFID technology is its utilization in a wide spectrum of applications. In some uses, the information held on the RFID is often unencrypted. But in other more demanding



applications — including credit cards, car keys, subway fare cards and high-security building access control keycards — the RFID's information is encrypted to prevent it from being read and potentially exploited by anyone with an RFID reader device.

Figure 1 Structure of an RFID System

3.2 Basic components of RFID system

Basic RFID system consists of three main components tag, reader and middleware.

[3] This section summarizes the information from these sources (Curtin, Kauffman, and Riggins1q, 2007) (Feldhofer, Dominikus, and Wolkerstorfer, 2004)
[4] Figure obtained from Cryptographic Hardware and Embedded Systems - CHES 2004 [e-book]

3.2.1 Tag

Radio Frequency Identification [5]Tags consists of an antenna and integrated circuit. Antenna is used for transmitting and receiving signals and integrated circuit is for storing and processing information, modulating and demodulating a radio frequency signal. Some of the RFID tags known as chip tags consist of a microchip in addition to integrated circuit and antenna, there are the smart cards based on RFID technology. Most tags are only activated when they are within the interrogation zone of the interrogator; outside they "sleep". Chip tags can be both read-only or, at higher complexity and cost, read-write, or both. Chip tags contain memory. The size of the tag depends on the size of the antenna, which increases with range of tag and decreases with frequency.

- Passive tags which draw power from the reader are cheaper and smaller than active tags, these types of tags are mainly used and proposed for use in payment systems.
- Semi-passive tags use an internal battery to ensure data integrity, however the signal sent from the reader generates the power to transmit the signal from the tag.
- Active tags typically have internal read and write capability, their own batteries, and can transmit their signals over a longer distance.

3.2.2 Interrogator/Reader

Interrogators/readers are the devices which are connected to server. They read the whenever it comes in its interrogation zone/reading range and pass that information to the server connected. Depending on the application and technology used, some interrogators not only read, but also remotely write to, the tags. For the majority of low cost tags (tags without batteries), the power to activate the tag microchip is supplied by the reader through the tag antenna when the tag is in the interrogation zone of the reader, as is the timing pulse – these are known as passive tags.

3.2.3 Middleware

Middleware is the interface needed between the interrogator and the existing company databases and information management software. Middleware is required to manage the flow from readers and send data to back-end management systems. (Knowledgeleader, 2006) RFID middleware assist with the following:

- Retrieving data from readers.
- Filtering data feeds to application software.
- Generating inventory movement notifications.

[5] The term RFID tag, RFID card, contactless card and RFID transponder in this report are used alternatively for a RFID card. The different names are used by different vendors.

- Monitoring tag and reader network performance.
- Capturing history.
- Analyzing tag-read events for application tuning and optimization.

3.3 RFID Frequencies and Standards

Radio frequency ranges from 300 KHz to 3 GHz. This operating range is generally considered to be organized into four main frequency bands. Table2 shows these different radio wave bands and the more common frequencies used for RFID systems with their typical use.

Band	**LF Low frequency**	**HF High frequency**	**UHF Ultra high frequency**	**Microwave**
Frequency	30–300kHz	3–30MHz	300 MHz–3GHz	2–30 GHz
Typical RFID Frequencies	125–134 kHz	13.56 MHz	433 MHz or 865 – 956MHz 2.45 GHz	2.45 GHz
Approximate read range	less than 0.5 metre	Up to 1.5 metres	433 MHz = up to 100 metres 865-956 MHz = 0.5 to 5 metres	Up to 10m
Typical data transfer rate	less than 1 kilobit per second (kbit/s)	Approximately 25 kbit/s	433–956 = 30 kbit/s 2.45 =100 kbit/s	Up to 100 kbit/s
Characteristics	Short-range, low data transfer rate, penetrates water but not metal.	Higher ranges, reasonable data rate (similar to GSM phone), penetrates water but not metal.	Long ranges, high data transfer rate, concurrent read of <100 items, cannot penetrate water or metals	Long range, high data transfer rate, cannot penetrate water or metal
Typical use	Animal ID Car immobiliser	Smart Labels Contact-less travel cards Access & Security	Specialist animal tracking Logistics	Moving vehicle toll

Table2. General Frequency Bands for RFID

There are very few ISO standards for RFID cards, one of the main standard used for payment systems is ISO 18000-3 (13.56 MHz) and electronic toll collection "vicinity" cards (ISO 15693). ISO 14443 and ISO 15693 both operate at 13.56MHz (HF), but the first standard has a read range of about 10cm whereas the later has a read range of 1 to 1.5 meters. (Ward, 2006)

3.4 Advantages and Disadvantages

Contactless technology provides an edge to RFID cards over other cards currently in use. First, these cards do not require a physical contact with pad for communication they just need to be in proximity to communicate, since these device needs merely to be close enough to a terminal to work, they are easy to use. As they transmit data at far higher speeds than their analogues, since it has a serial communication lines that runs fast, it doesn't have to be in proximity for very long (Callas, 2008)

The use of contactless technology offers convenience and speed but it there are number of disadvantages as well. The tags can be read and write from are much greater distances than assumed (Trailertrailers.com, N. D.). As these cards can be accessed from distance and without the knowledge of user there is a threat of disclosure of personal information, and unauthorized tracking. (Wetpaint.com, N.D.) These tags can be read for very long time, and there could be poor read rate can occur if the reader and receiver are not properly aligned.

4 Security Violations

"*Analyzing systems and understanding how to break them gives you a lot of insight into how to build better systems."* (Evans, 2008)

4.1 ExxonMobil Speedpass Aug, 2005

ExxonMobil Speedpass (a RFID tag) was successfully hacked by a team of students and researchers. They did reverse engineering of Texas Instruments DST (i.e. Digital Signal Transponder, it is name given by manufacturer to the RFID tag)
The team was successfully able to recover cryptographic key from a target DST device, for arbitrary challenge-response pairs, they demonstrated that they can recover a key in under an hour using an array of sixteen FPGAs. When the challenge-response pairs derive from pre-determined challenges, i.e., in a chosen-plaintext attack, a time-space trade-off is possible, reducing the cracking time to a matter of minutes.

These DSTs are deployed in several applications.
Vehicle Immobilizers:

Electronic Payment: DSTs are used in the ExxonMobil SpeedPass system, with more than seven million cryptographically-enabled keychain tags accepted at 10,000 locations worldwide.

Basic working and security of DST
A DST contains a secret, 40-bit cryptographic key that is field-programmable via RF command. In its interaction with a reader, a DST emits a factory-set (24-bit) identifier, and then authenticates itself by engaging in a challenge-response protocol. The reader initiates the protocol by transmitting a 40-bit challenge. The DST encrypts this challenge under its key and, truncating the resulting ciphertext, returns a 24-bit response. It is thus the secrecy of the key that ultimately protects the DST against cloning and simulation.

Strategy, attack was divided into three phases:
Reverse engineering: The team started from a rough published schematic of the block cipher and underpinning the challenge-response, was able to derive the complete functional detailed cipher used in DST. "Oracle" or "Black-box" technique was used to accomplish this task, that is, by experimental observation of responses output by the device across selected programmed encryption keys and selected input challenges. This phase was the main phase of the attack.
Key cracking: Once they were able to drive the complete functional details of the cipher, they used an array of sixteen FPGAs operating in parallel to crack the 40bits long key. With this system, the team was able to recover a DST key in under an hour from two responses to arbitrary challenges.
Simulation: The last step was to simulate a DST to a Reader. After cracking the key (and serial number) of a DST, they were able to successfully simulate its RF output so as to spoof a reader.

Things that help them in launching an attack

- Keys of some DST devices are field-programmable; team used these DST devices to experiment with a set of chosen keys and inputs for DST40.

Key assumptions and observations team made

- Team assumed that, the cipher works as it was shown in the schematic diagram disclosed by Texas Instruments, but later they concluded that it doesn't.
- On the basis of schematic diagram, they concluded that a !0 key, i.e., string of '0' bits, will remain unchanged in the key register throughout the cipher execution. Using this key, it is possible to render each step of the algorithm independent of the round in which it takes place. And they used the !0 key for the experiments.
- Team observed that each cycle, i.e., each execution of F, results in only a small change to the state of the challenge register: The contents of the register are shifted right by one bit, and the output of the h-box is inserted into the leftmost bit position.

- By querying oracle, team determined that the key is updated every three cycles, beginning with the second cycle – not the first, as suggested by the Kaiser diagram. They also determined that while four bits are indeed exclusive-ORED together, these are not the bits shown in the diagram.

Attack Procedure

This section provides brief information about the attack launched by the team on DST. In this section their main problems, observations and outcomes are covered.

Obtaining a single-round output

- Team, did not know the contents of the f-boxes, or other critical details such as the configuration of the routing networks in DST40, so they could not directly verify that production DSTs, such as those that they obtained for their experiments, implemented the Kaiser cipher.
- Team first noted that the only round dependence of the Kaiser cipher is in the key scheduler. As seen in Figure 1, a !0 key, i.e., string of '0' bits, will remain unchanged in the key register throughout the cipher execution.
- Team next observed that each cycle, i.e., each execution of F, results in only a small change to the state of the challenge register: The contents of the

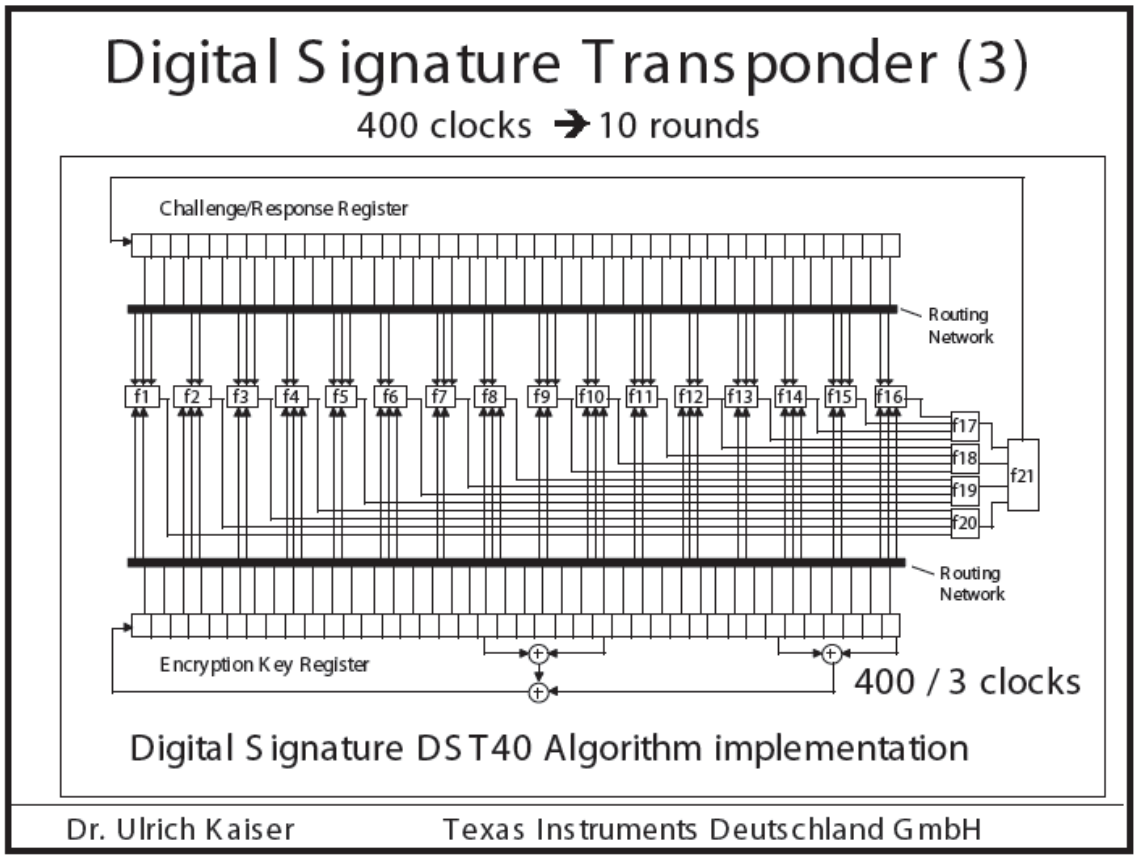


Fig. 1. Schematic of Kaiser Cipher.

register are shifted right by one bit, and the output of the h-box is inserted into the leftmost bit position. Consequently, for any given value submitted to the tag, the challenge register can assume only two possible values after one clock cycle, depending on whether the h-box outputs a '0' or a '1' bit.

- Using the DST as an oracle, team developed a test to recover the output of the h-box for any value in the challenge/response register. Unfortunately, this test failed to produce the results we expected, indicating that DST40, the algorithm in the production DST, differs from the Kaiser cipher.
- After submitting a number of properly-formed challenges to the DST, team discovered that the method of testing next-state challenge register values succeeded when we modeled the output of the h-box as two bits. For a given challenge C, this required that we instead compute four candidate next-state values, C00,C01,C10,C11, i.e., one for each of the possible output bit-pairs of the h-box. In our experiments, at least one of these four candidates always produced a response corresponding to the initial response R, but shifted right by two bits. One possible explanation was that the circuit alters its operation every other clock cycle, causing our test to malfunction.

Recovering the key schedule

- Problem: As experiments, relied on the assumption that the!0 key remains constant through every cycle of the encryption process. Using only the !0 key, however, would restrict our ability to experiment with the algorithm internals. Team required the ability to observe single-round outputs based on different values in the challenge and key registers. Using a non-zero key again made the algorithm round-dependent.

- Observation: By querying oracle, team determined that the key is updated every three cycles, beginning with the second cycle – not the first, as suggested by the Kaiser diagram. They also determined that while four bits are indeed exclusive-ORED together, they are not the bits shown in the diagram.

Uncovering the Feistel structure of DST40

- Further experimentation revealed that the two bits affect the first and second bit of the two-bit round output respectively. This indicated that the cycle output derived from the exclusive-or of these bits with the output of the F function.
- The XOR effect of bits c38 and c39 shed new light on the algorithm's design. Not only is the algorithm an invertible permutation, but it is a form of Unbalanced Feistel Network.
- The DST returns only a portion of the encrypted challenge – namely the last 24 bits of the challenge register – so decryption of DST responses is not possible. We suspect that the hope of using a one-way permutation in this

application was to bound the number of collisions, i.e., challenge values that produce any particular response.

Recovering the bit routing networks

- The structure of the Kaiser cipher is such that h receives a single input bit from each of the g-boxes, and produces one or four possible output values. This fact lays the groundwork for identifying which bits of the challenge and key are routed to each of the g-boxes.
- It is clear that altering a single input bit of h can at most produce two distinct output values. In consequence, altering the output of only one g-box can never cause h to output more than two distinct values, whereas altering the output of more than one g-box can produce up to four distinct output values. Using this simple but powerful observation, we devised a test to determine which groups of input bits from the challenge and key are routed into each of the four g-boxes. The test involves fixing a set of all but two challenge or key bits, and then iterating through all four combinations of these two bits. If at any time these four bit combinations produce more than two different outputs, then they cannot possibly be routed through the same g-box. It should be noted that this test of g-box membership produces false positives. In particular, it is very possible (and indeed common) that for two test bits that are not routed to the same g-box, and for a given set of fixed bits, different value assignments to the test bits still produce two or fewer distinct outputs from the h-box.
- Therefore this test requires many repetitions with different sets of fixed bits.

Building logical tables for the f, g, and h-boxes

- Once we identified the bits corresponding to each f-box, tables were constructed to represent the logical functions computed by the f, g, and h-boxes. To construct the f-box tables, we simply iterated through the $2^5 = 32$ possible input values for the set B of bits that corresponds to the f-box.
- Two different output values from F resulted (given a fortuitous setting of B). One of these values represented the case where the f-box outputs a '0' bit, and the other when a '1' is output. We had no way of telling whether the actual output of the f-box in question was a '0' or '1' bit; this is immaterial, however, as it may ultimately be treated as a naming convention. What learned from this experiment was, for each f-box, a partition of the 32 input values into two sets corresponding to complementary output-box values.

Key Cracking

- Team was able to verify that the reverse engineering of the DST40 algorithm done by them was successful. Team tested the responses computed by a software implementation of their hypothesized algorithm by matching those returned by an evaluation DST when given the same challenge and key. Team chose to implement the keycracker in hardware using FPGAs.

Final step

- RF protocol analysis and simulation
- Sniffing the protocol
- Putting together the pieces: the full DST protocol
- Simulating a DST device

4.2 Mifare Classic Cards

MiFare Classic card was developed by Philips, the global electronics giant. First introduced in 1994, sales in the intervening 15 years have purportedly made it the most popular single RFID chip, with over a billion sold worldwide. MiFare Classic chips are used in thousands of applications, in smart cards and tickets with dozens of different brand names. The MiFare Classic chip is used by millions of people to pay fares on several major mass-transit systems around the world, including the London Underground (known there as the Oyster card) (Nohl, et al., 2008; Gans, et al., 2008; Mifare, N.D.).

Mifare Classic is a memory card with some memory protection mechanism. The card is not programmable. The cryptographic operations it can perform are implemented in hardware, using a so-called linear shift feedback register (LSFR) and a `filter function'. The encryption algorithm this implements is a proprietary algorithm CRYPTO1 which is a trade secret of NXP. The security of the card relies in part on the secrecy of CRYPTO1 algorithm.

This card has been successfully hacked by number of times by different teams; all the teams approached differently and were able to clone the tag.

- January 8, 2008 (Nahl)
- 7 march 2008 (Garcia)

In this section, the details of the attacks launched by different teams are studied and discussed.

Starting from the, Structure of Mifare Classic Card

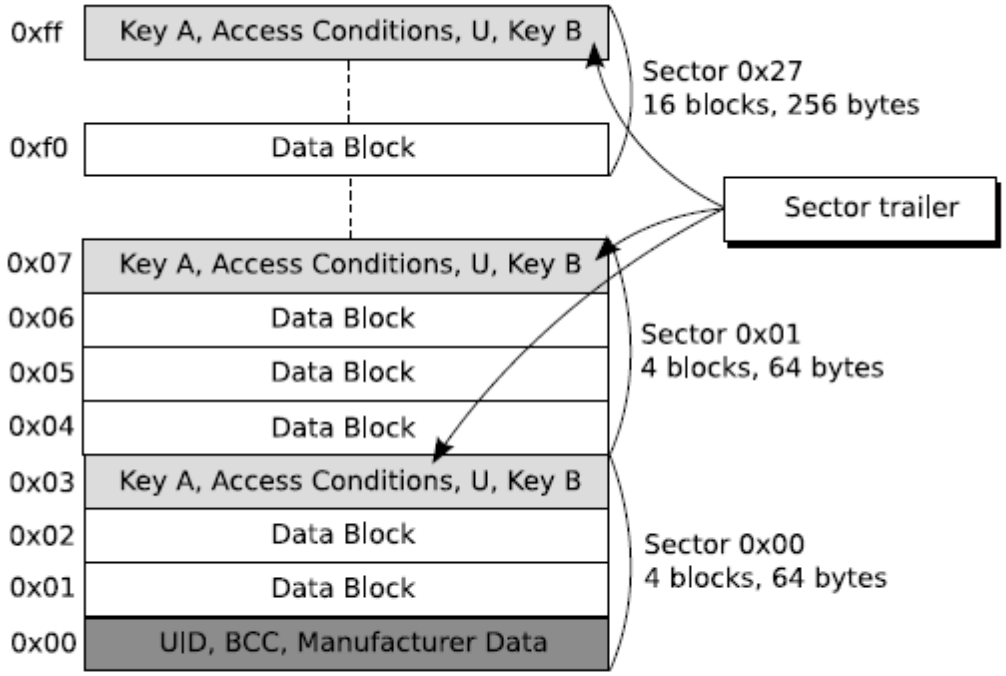


Fig. 1: MIFARE Classic 4k Memory

The card's memory (1Kbyte/4Kbyte) is divided into sectors, each protected by two cryptographic keys. Card with 1Kbyte (1024bytes) memory has 16 sectors, each sector having 4 blocks, and each block has the capacity to store 16 byte data. Block 0 of sector 0, of each card consists of special (5byte) data in which first 4 bytes store card ID and last byte Bit Count Check (BCC). Reader needs to authenticate for each sector for data access. Each sector has sector trailer, trailer consists of "A" & "B" secret keys used 4 authentication. These access conditions define the operations permitted on memory sector. Reader can't read key "A" can read key "B" in some cases (i.e. in which B is readable). Other than these keys there is one data byte U in section trailer which has no defined purpose. Data block can be used to store data or as value block.

Command set includes only six commands which include read, write, increment, decrement, transfer, and restore.

Security, communication is encrypted by crypto1 cipher, 48 bit keys in section trailer, authentication protocol (3way handshake)

Communication procedure

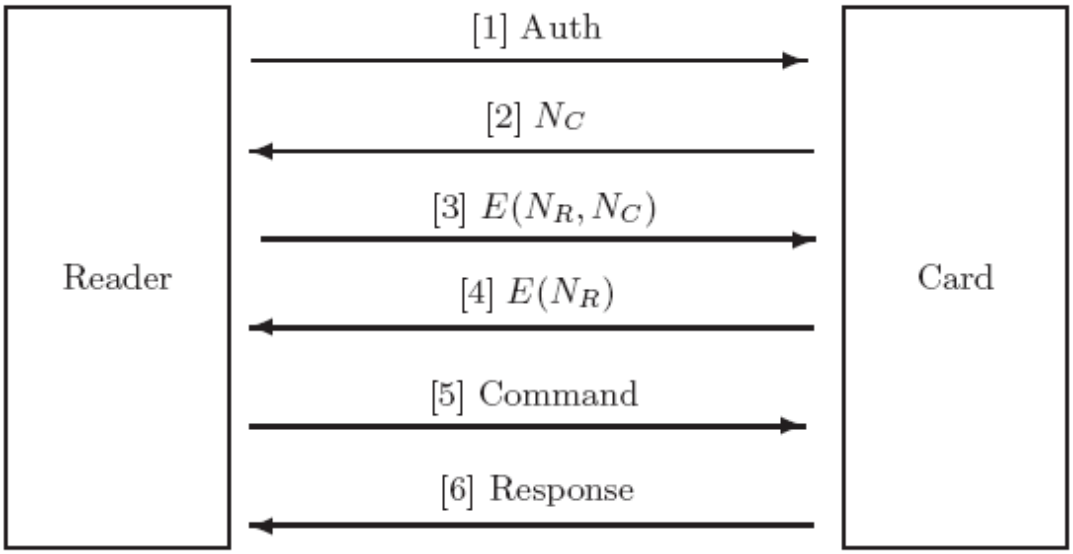


Fig. 3: Authentication followed by a command

1. The reader sends request for sector authentication
2. Card replies with 32 bit nonce (Nc)
3. Reader decrypt that key and replies with Nc+Nr encrypted + additional input (total= 8 byte).
4. Card decrypt check it's Nc and make sure reader possesses same key and replies with encrypted Nr
5. Reader decrypts it to make sure, and sent the command to be executed.
6. Card executes the command and replies with result reader.

First Attack (Reverse Engineering)

Karsten Nohl & on January 8, 2008

This team demonstrated that the encryption used by Mifare Classic card is much easier to break than previously thought. This team broke the encryption on one particular RFID chip – the MiFare Classic.

Attack Procedure

The first barrier to breaking the encryption of RFID chips like the MiFare Classic was being able to "listen" to the information that such chips broadcast, in encrypted or unencrypted form. (Eavesdropping)

Once Nohl's team could read the raw information transmitted by the MiFare Classic, breaking its encryption involved surmounting several technical challenges.

Nohl and his colleagues "dissected" the MiFare chip to reveal each of the five layers of circuitry that makes up the chip and produce the encryption. (Reverse Engineering)

Steps followed

- Team examined the chip under a conventional optical microscope, and used micro-polishing sandpaper to remove a few microns of material at a time to reveal each layer of circuitry, which then was digitally photographed.
- Team worked hard to recognize and clarify the different elements that made up each circuit, and then combined these clarified pictures from each of the chip's layers to produce a clear, three-dimensional picture of the entire circuitry.
- Analyzing the details of the circuit, Nohl deduced the algorithm (a mathematical formula involving many steps) created by the long series of hundreds of "logic gates."
- Knowing the algorithm defined the relatively narrow range of possible keys that would unlock the encryption, allowing team to find the right key in a matter of hours by trying all the possible keys until he found the right one. Having done that once or twice, he could pre-compute the possible keys and break the encryption on other examples of the MiFare chip in a matter of minutes.

In this attack, the main emphasis was on analyzing circuit and developing the similar algorithm. The approach was more electronic engineering based, studying the layout of the hardware implementing the algorithm on an actual Mifare Classic chip. After deducting the circuit, different keys of combination were tried.

Second Attack (Exploiting Pseudo Random Generator's weaknesses)

On March 7, 2008 researchers and students of the Digital Security group of the Radboud University Nijmegen have discovered a serious security flaw in a widely used type of contactless smartcard, also called RFID tag.

In this attack, the team demonstrated successful attack to exploit the weaknesses of the pseudo random generator used in Mifare Classic card. The team launched the attack by using the keystream which card had used earlier. The team was able to read all sectors of card without using key, retrieve all proprietary command codes, and in last was able to clone the card.

As this attack was based on the keystream which has already been used by the card, the team collected the information of the transaction between genuine card and genuine reader using eavesdropping attack.

Approach, the plaintext P1 in the communication is XOR-ED bitwise with a keystream K (i.e. generated by Pseudo Random Generator for encryption) which gives the encrypted data C1. Due to the weakness of the card, it is possible to use the same keystream with a different plaintext P2. And using the below equation, both P1 and P2 can be revealed, if either P1 or P2 is known.

P1 X-ORED K = C1
P2 X-ORED K = C2
» (C1 X-ORED C2) = P1 X-ORED P2 X-ORED K X-ORED K
» C1 X-ORED C2 = P1 X-ORED P2

The weak pseudo-random generator makes it possible to replay an earlier recorded transaction. Attacker can flip ciphertext bits to try to modify the first command such that it gives another result. Another result gives us another plain text. The attack is based on this principle.

Steps to launch attack:
1. Team recorded a trace of a successful authentication between a genuine card and reader.
2. Sent authentication requests until it got a nonce that is equal to the one in the original trace.
3. The recorded response was sent to this nonce. It consists of a valid response to the challenge nonce and challenge from the reader.
4. Team retrieved the response to the challenge from the card.
5. Now at this point, team made a point that they could resend the same command or attempt to modify it.

After step 4 the card is in a state where we have successfully authenticated for (in this case) sector 0 (block 3). Now it expects a command for this sector. If we send the same command we recorded earlier, we get the same encrypted response as in the original trace. Therefore the keystream is the same. Modifiying the communication under the keystream, will reveal data and commands that initially were encrypted. By following same procedure attacker can reveal lot of information and can access the memory sectors to edit or modify them.

4.3 Electronic-Toll System (FasTrak) Hacked

This attack was launched by a researcher Nate Lawson, against the RFID tag used in electronic toll collection system. The tag targeted in this attack was Texas Instruments MSP430 microcontroller which is used in FasTrak electronic toll collection system (Phillips, 2008).
Following were the main observations made by researcher (Lawson, 2008).

- There wasn’t any authentication
- There wasn’t any encryption
- Anyone can force the tag to take on a new ID

The only feature added on the name of security was that the

- Tag could not be read using JTAG cable, as manufacturer burnt the fuses.

This was the one of the easiest attack to be launched against a RFID tag. As tag was used connected to direct debit account, attacker hasn’t discussed anything about the details of account connected to it. Either that wasn’t

5 Issues with RFID (Payment Systems)

RFID tags and RFID readers communicate using radio waves, and use of radio-frequency as a transmissions channel raises number of concerns when deployed/used in practice.

5.1 Operational Issues

5.1.1 RFID Systems Can Be Easily Disrupted

Since RFID systems make use of the electromagnetic spectrum, they are relatively easy to jam using energy at the right frequency (Ilyas, et al., 2008). A serious threat to payment system RFID system vulnerable to such attacks could become a serious organizational weakness.

5.1.2 RFID Reader Collision

Reader collision occurs in RFID systems when the coverage area of one RFID reader overlaps with that of another reader. This situation is quite common at public transit system and toll tax collection system. Reader collision causes two different problems. Signal interference, the RF fields of two or more readers may overlap and interfere. This can be solved by having the readers programmed to read at fractionally different times. This technique (called time division multiple access - TDMA) can still result in the same tag being read twice. Multiple reads of the same tag, the problem here is that the same tag is read one time by each of the overlapping readers. The only

solution is to program the RFID system to make sure that a given tag (with its unique ID number) is read only once in a session (Ilyas, et al., 2008).

5.1.3 RFID Tag Collision

Tag collision in RFID systems happens when multiple tags are energized by the RFID tag reader simultaneously, and reflect their respective signals back to the reader at the same time. On 11 February 2009, *Sing Tao Daily* reported that the fail-safe is being abused for skipping fare through the railway station turnstile. A large amount of dishonest passengers at Sheung Shui Station and Lo Wu Station stacking up 4 or more cards before breaking through the turnstile, pretending their cards have been touched with the reader correctly but triggering the fail-safe deliberately to avoid card value deduction. This problem is often seen whenever a large volume of tags must be read together in the same RF field. The reader is unable to differentiate these signals; tag collision confuses the reader. Different systems have been invented to isolate individual tags; the system used may vary by vendor. For example, when the reader recognizes that tag collision has taken place, it sends a special signal (a "gap pulse"). Upon receiving this signal, each tag consults a random number counter to determine the interval to wait before sending its data. Since each tag gets a unique number interval, the tags send their data at different times (Ilyas, et al., 2008).

5.1.4 Unauthorized Tag Disabling

This is a form of Denial-of-Service (DoS) attack in which an attacker causes RFID tags to assume a state from which they can no longer function properly. This results in the tags becoming either temporarily or permanently incapacitated. Such attacks are often exacerbated by the mobile nature of the tags, allowing them to be manipulated at a distance by covert readers. Active RFID tags (those that use a battery to increase the range of the system) are more subject to these types of attacks as on being repeatedly interrogated wear the battery down, disrupting the system (Ilyas, et al., 2008)

5.2 Privacy & Security Issues

Since, publicly available radio frequency is used as transmission channel between RFID cards and readers, it is harder to secure than wires or cables. The factors (Lee, 2005) which make RFID tags especially dangerous to privacy, In short, RFID tags are designed for convenience of reading, but that convenience comes with a high cost to privacy and a high risk of identity theft.

- RFID tags are promiscuous: They are generally designed to be activated, and their transmissions receivable, by any compatible reader/sensor device.
- RFID tags are stealthy: When RFID tags are being read, the people carrying the tags don't know that it's happening.
- RFID tags are remotely readable, and can be read through many common substances (cloth, leather, paper).

5.2.1 Unauthorized Disclosure Of Personal Information

RFID tags also present security issues, such as "cloning" or duplication and card forgery. Since RFID cards become active when in vicinity of card reader, and start communicating, the attacker can exploit this feature to obtain the information use this without the holder's knowledge or consent. Any compatible reader within range of the RFID tag could read the stored data. Read range varies depending on the radio frequency being used, the power of the reading device, and many environmental factors. This could easily occur in "walk-through" application when the card is read from one's wallet, pocket or purse. Cloning the RFID tag alone might suffice for an illegitimate purpose (Ilyas, et al., 2008; Lee, 2005)

5.2.2 Unauthorized Tracking

An RFID card also enables others to secretly monitor its holder's whereabouts and possibly his or her actions. As the number of RFID readers in the social environment increases, the easier it will be to track RFID tags. Importantly, the tracking threat exists even if the RFID tag contains no name or other personal information. What matters is that the RFID tag contains a static unique number or pattern that is or can be persistently

associated with a person's identity. So long as the RFID tag or chip broadcasts this information, the person carrying that tag can be distinguished from any other person carrying a different RFID tag. It is a serious threat to privacy (Ilyas, et al., 2008; Lee, 2005).

5.2.3 The Unique ID Number Problem

Any unique ID number on the card may be a "key" to personal information stored in a database somewhere. Our society often uses unique ID numbers to index or organize personal information in databases, or as a linking or matching identifier across multiple databases. The worst-case scenario would be a commonly used unique number like a Social Security number, phone number, or a driver's license number, which is already used to index and link personal data (Lee, 2005).

5.2.4 Eavesdropping

Eavesdropping attacks are a well known risk for RFID devices and there are several claims about the possibility of these attacks on RFID tokens. It is another type of information disclosure threat. In eavesdropping, the attacker does not read the information directly from the RFID tag or card; instead, the attacker listens to the transmission between the RFID tag and an authorized RFID reader. The eavesdropping threat is the main reason why merely shielding RFID devices is inadequate to protect privacy, because the RFID card must be exposed in all legitimate transactions. No physical contact needs to be made with the reader, which simplifies operation and increases overall transaction speeds. A growing security concern with RFID devices is the possible release of the user's personal information, or location, to unauthorized parties (Lee, 2005). The suggested solution for it was better encryption and shielding (Kelter, 2006).

5.2.5 Forward Security

Since RFID cards are proposed to be used in payment systems, they may be used to store the information related to all the recent transactions. As these devices are highly vulnerable to number of attacks, there shouldn't be any information stored related to previous transactions. Forward-security is

important to guarantee the privacy of past transactions if the long-term key or current session key is compromised (Burmester, et al., 2007)

5.2.6 Relay Attack

It is a type of attack related to man-in-the-middle attacks, in which an attacker relays verbatim a message to a card reader. The card may not be aware of this communication. Since a contactless card communicate with other devices without any physical connection, the security of the payment system is based on a key feature of RFID-based systems that card works in very short range typical to operate at a range of 10cm. But it has been demonstrated by (Kfir, et al., 2005)) that contactless card technology is vulnerable to relay attacks. A setup was built that could remotely use a victim's contactless smartcard, without his knowledge. The suggested counter measures were to shield the contactless card against malicious attackers, and to activate the card only when the card owner wants to take some action.

5.2.7 Side Channel Attacks

This is an attack which is launched on the basis of information gained from the physical implementation of an equipment, rather than brute force or theoretical weaknesses. In these attacks the timing information, power consumption, electromagnetic leaks or even sound produced is exploited. (Oren, et al., 2007) have successfully launched this attack against RFID system. In which they demonstrated that power analysis can be carried out even if both the tag and the attacker are passive and transmit no data, making the attack very hard to detect and suggested that in order to achieve strong security in practice, research is needed into either making RFID hardware more resistant to such attacks, or developing obfuscating techniques for cryptographic computations.

6 Conclusion

The current payment systems are not able to keep the pace with the requirements of some new applications/systems. The main reasons behind the limitations of current electronic payment system are technology (is slow), the method opted for authentication and authorization (card issuing authority is involved), and other limitations such as its inability to support very small amount payments.

To overcome these limitations and improve the service new payment system known as micropayment system has been developed using Radio Frequency Identification technology. RFID offers number of advantages over the current card system. RFID is more fast and convenient to use. In this system some amount is loaded on the card which is deducted when ever anything is purchased or service is used. In some cases it directly connected with direct debit account, which implies that payee and payer need not to contact the central server for approval of transaction, it makes this transaction faster. In addition to it, authentication is done on the basis of code in RFID card, which also helps in performing transaction faster. As this technology offers number of advantages it has some limitations too. Various teams of researchers and students around the globe have successfully attacked the payment systems based on RFID.

In this work, I have studied and discussed the basic working of RFID and its main components. The main operational and security issues of RFID are also covered. In the recent time number of successful security attacks have came into light. As it has been said by David Evans, an associate professor of computer science in U.Va.'s School of Engineering and Applied Science that In order to build more secure systems, you have to understand why previous systems failed. Number of these violations have been studied and discussed in this work. The studies of these attacks help me gain the deep understanding of the vulnerabilities of the system and with how much efforts and apparatus they have been successfully exploited.

Bibliography

Ahson S., Ilyas M. 2008. *RFID Handbook.* North West, North America : CRC Press, 2008.

Amy, Williams L. 2007. Developments in Micropayment Systems. *http://www.dww.com/.* [Online] 2007. [Cited: May 18, 2009.] http://www.dww.com/?page_id=1158.

Avishai, Kfir Ziv and Wool. 2005. Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems. [Online] 2005. [Cited: April 10, 2009.] http://eprint.iacr.org/2005/052.pdf.

Burmester Mike, Medeiros D. Breno. 2007. RFID Security: Attacks, Countermeasures and. *http://www.cs.fsu.edu/.* [Online] 2007. [Cited: April 10, 2009.] http://www.cs.fsu.edu/~burmeste/133.pdf.

Callas, J. 2008. Position Statement in RFID S&P Panel: Contactless Smart Cards. *http://www.springerlink.com/.* [Online] 2008. [Cited: April 1, 2009.] http://www.springerlink.com.simsrad.net.ocs.mq.edu.au/content/t0w72522 4686664k/fulltext.pdf.

Curtin J., Kauffman R. J., and Riggins F. J. 2007. Making the 'MOST' out of RFID Technology. Information Technology and Management. *http://www.ftc.gov/.* [Online] 2007. [Cited: May 19 , 2009.] pp 87-110. http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf. 2.

Feldhofer M., Dominikus S., and Wolkerstorfer J.,. 2004. Cryptographic Hardware and Embedded Systems - CHES 2004. *http://www.springerlink.com/.* [Online] 2004. [Cited: April 10, 2009.] http://www.springerlink.com.simsrad.net.ocs.mq.edu.au/content/26tmfjfcju 58upb2/?p=246ed1cfc14b49048c8a154d311082f0&pi=7.

GovernmentSecurity.Org. N. D.. An Overview of Cryptography. *http://www.governmentsecurity.org/.* [Online] N. D. [Cited: May 27, 2009.] http://www.governmentsecurity.org/overview_of_cryptography.

Halliday, Steve. 1997. Identification Cards - Just the Ticket? *http://www.hightechaid.com/.* [Online] 1997. [Cited: April 10, 2009.] http://www.hightechaid.com/tech/card/id_cards.htm.

Harald, Kelter. 2006. Security threats around RFID. *http://www.rfidconsultation.eu/.* [Online] 2006. [Cited: May 20 , 2009.] http://www.rfidconsultation.eu/docs/ficheiros/Kelter.pdf.

Jari Kytojoki, Vesa Karpijoki. 2000. Micropayments - Requirements and Solutions. [Online] 2000. [Cited: March 20, 2009.] http://users.tkk.fi/vkarpijo/netsec99/.

Juniper, Research. N. D.. Whitepaper: The Big Micropayment Opportunity. [Online] N. D. [Cited: April 10, 2009.] http://juniperresearch.com/shop/viewwhitepaper.php?whitepaper=32.

Kniberg, H. 2002. What Makes a Micropayment Solution Succeed. *http://www.kniberg.com/.* [Online] 2002. [Cited: March 25, 2009.] http://www.kniberg.com/henrik/thesis/pdf/What-makes-a-micropayment-solution-succeed.pdf.

Knowledgeleader, What Every Internal Auditor Should Know About RFID. 2006. Overview of RFID components. [Online] June 2006. [Cited: 27 March, 2009.] http://www.theiia.org/download.cfm?file=93793.

Le V Tri, Mike Burmester, Medeiros D. Breno. 2007. Universally Composable and Forward-secure RFID Authentication and Authenticated Key Exchange. [Online] 2007. [Cited: April 10, 2009.] http://www.cs.fsu.edu/~burmeste/130.pdf.

Oren, Y. and Shamir, A. 2007. Remote Password Extraction from RFID Tags. *http://iss.oy.ne.ro/.* [Online] 2007. [Cited: April 20, 2009.] http://iss.oy.ne.ro/RemotePasswordExtractionFromRFIDTags.pdf.

Tien Lee, 2005. 2005. Testimony in support of the Identity Information Protection Act (S.B. 682). *http://w2.eff.org/.* [Online] 2005. [Cited: May 15, 2009.]
http://w2.eff.org/Privacy/Surveillance/RFID/tien_testimony_sb_682.pdf.

Trailertrailers.com. N. D.. RFID tags, The TrailerTrailer overview. *http://www.trailertrailers.com/.* [Online] N. D. [Cited: May 29, 2009.] http://www.trailertrailers.com/RFID-tags.htm.

Trappe, W. and Washington, C. L. 2006. *Introduction to Cryptography, Second Edition.* Washington : Prentice Hall, 2006.

Ward, M. and Kranenburg, V. R. 2006. RFID: Frequency, standards, adoption and innovation. [Online] May 2006. [Cited: March 23, 2009.] http://www.rfidconsultation.eu/docs/ficheiros/TSW0602.pdf.

Wetpaint.com. N.D.. RFID in Public Transportation. *http://rfidintro.wetpaint.com/.* [Online] N.D. [Cited: June 5, 2009.] http://rfidintro.wetpaint.com/page/5.Advantages+&+Disadvantages.