ANALYSIS OF SECURITY WEAKNESSES IN NFC APPLICATIONS ON ANDROID AND PROPOSE POLICY FRAMEWORK FOR ADOPTION

By

Naveed Ashraf Chattha

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Islamabad in partial fulfillment of the requirements for the degree of MS in Information Security

February, 2017

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS Thesis written by Mr./~~MS~~ **Naveed Ashraf Chattha,** Registration No. **NUST2013-63035-MMCS25213F**, of **Military College of Signals** has been vetted by undersigned, found complete in all respect as per NUST Statutes/Regulations/MS Policy, is free of plagiarism, errors and mistakes and is accepted as partial, fulfillment for award of MS degree. It is further certified that necessary amendments as pointed out by GEC members and foreign /local evaluators of the student have been also incorporated in the said thesis.

Signature: _____
Name of Supervisor_____
Date: _____

Signature (HoD): _____
Date: _____

Signature (Dean/Principal): _____
Date: _____

Declaration

I certify that this research work titled "*Analysis of Security Weaknesses in NFC Applications on Android and Propose Policy Framework for Adoption"* is my own work. The work has not been presented elsewhere for assessment. Material used from other sources has been properly acknowledged / referred.

_____

Naveed Ashraf Chattha

Copyright Statement

Acknowledgements

I am thankful to Allah Subhana-Wa-Taala to have guided me through this work at every step and for every new thought which came to my mind to improve it. Indeed I could have done nothing without Your priceless help and guidance. Whosoever helped me throughout the course of my thesis, whether my parents or any other individual was Your will, so indeed none be worthy of praise but You.

I am thankful to my beloved parents who raised me when I was not capable of walking and continued to support me throughout my life.

I would also like to express special thanks to my supervisor Dr. Imran Rashid for his help throughout my thesis.

I would also like to pay special thanks to Waleed Bin Shahidfor his tremendous support and cooperation. I appreciate his patience and guidance throughout the whole thesis.

I would also like to thank Dr. Baber Aslam and Lec Waleed Bin Shahid for being on my thesis guidance and evaluation committee.

Finally, I would like to express my gratitude to all the individuals who have rendered valuable assistance to my study.

Dedicated to my parents, wife and children whose fabulous support and cooperation led me to this achievement

ABSTRACT

Portable and mobile devices have already made their place in our society for private as well as public use. These devices are under continuous evolution and innovation and advancement in every aspect is being observed on daily basis. Availability of new technologies for creating convenience to users is threatened by the information security aspects being violated or not catered for at the initial stage. Android has emerged as the most popular operating system in portable handheld communication devices. More than 80 % of the devices at present are running Android operating System at their core to provide hardware functionality coupled with the software. Near Field Communication (NFC) has been in use for quite some time by many users in mobile devices. Its use is increasing by the rapid increase in the availability of the NFC enabled devices in the market. NFC enables data transfer by bringing the two devices in close proximity, about 3-5 inches. It is designed for integration with mobile phones, which can communicate with other phones (peer-to-peer) or read information on tags and cards (reader). An NFC device can also be put in card emulation mode, to offer compatibility with other contactless smart card standards. This enables NFC enabled smart-phones to replace traditional contactless plastic cards used in public transport ticketing, access control, ATMs and other similar applications. NFC is a new and innovative technology with futuristic uses, but technology comes at a price both in terms of financial effects as well as the maintenance costs. The most pertinent concern would be that how much vulnerable the new technology is. There had already been instances where the security of NFC has been put to questions. It is vulnerable to numerous kinds of attacks. This research will list down the basic working principles of NFC, the protocols involved, vulnerabilities reported so far. Behavior of various applications on android operating system with emphasis on the weaknesses/ vulnerabilities and possible countermeasures and framework is proposed.

Table of Contents

List of Figures

CHAPTER 1: NEAR FIELD COMMUNICATION

1.1 Introduction

Near Field Communication operates at limited range using wireless communication technology. It uses the basic communication schemes of Radio Frequency Identification (RFID). It operates on 13.56 MHz frequency with data rate of up to 424 kilobits per second at a distance of 10 centimetres [1]. NFC enabled devices can communicate with each other when these are touched against each other or are in the operating range. NFC technology has been the source of many implementations in various businesses like assets identification and tracking in supply chain management, public ticketing in transportation system, access control systems and identification of persons by use in identity cards and passports.

NFC has three typical device operating modes: (1) Card Emulation mode, (2) Reader/Writer mode, and (3) Peer-To-Peer mode [2]. NFC model involves two devices for the communication, an initiator and a target. Initiator starts the communication and is typically an active NFC device. Initiator is responsible for energizing the target in case the target device is a passive device as it possesses an energy component which can generate power for the target as well. The target device can either be an RFID tag, RFID tag based card or an RFID based NFC device. The target devices respond to the requests generated by the initiator in the form of responses [3].

The communication between the devices takes place over a single RF band which is shared by the devices in half-duplex mode [3]. One device transmits at a single point of time and the other device is in listening mode. The second device starts its transmission once the first device has finished its transmission.NFC based mobile devices typically smart-phones can be used in both reader and tag modes simultaneously by easily using the interface available on the mobile screen. Applications developed for smart-phones include a variety of uses of NFC technology.

The research work in this dissertation has been presented in five parts. First part is related to the NFC vulnerabilities and defense taken from the paper published by the author [4].

1.2 NFC Modes of Operation

1.2.1 Card Emulation

Smart-phone devices act like a contactless smart card when used in card emulation mode. This mode is used in NFC based payment and ticketing systems on smart-phones. The applications on the smart-phones use libraries of existing infrastructure of smart cards. ISO-14443 smartcard behaviour is simulated by the NFC controller of the smart-phone operating system. These mobile devices can be used in place of the typical smart cards used for payments or physical access control etc. The NFC controller acts as a gateway to tunnel the data and commands from the card application on the mobile device to the receiving hardware. The NFC controller itself does not carry out any computation. This implementation is now referred to as Host-based card emulation and has been bundled by Google with the Android 4.4, Kitkat. Operating system generates response to the NFC traffic received from external readers.

1.2.2 Reader/Writer

It allows the smart-phones to read data from NFC devices or smart cards containing RFID tags. The same phone can be used in writer mode as well where it is used to write tag information data on the blank and un-initialized tags.An NFC enabled smart device can read NFC tags, such as NFC smart poster tags. A user can retrieve tag information stored in the tag for further actions afterwards. Typical arrangement of this mode as described by NFC forum is as shown in Figure 1.1 [5].

1.2.3 Peer-To-Peer

Two devices can act as sender and receiver or active and passive device. Bidirectional communication takes place between two NFC enabled mobile phones to exchange information. The communication between the two devices takes place using the same channel in half duplex mode. NFC Data Exchange Format or NDEF [6] is a standardized format which is used to store data on tags. It also specifies the standards for transportation of data between two NFC devices in Peer-to-Peer mode [5]. Typical arrangement of this mode as described by NFC forum is as shown in Figure 1.2.

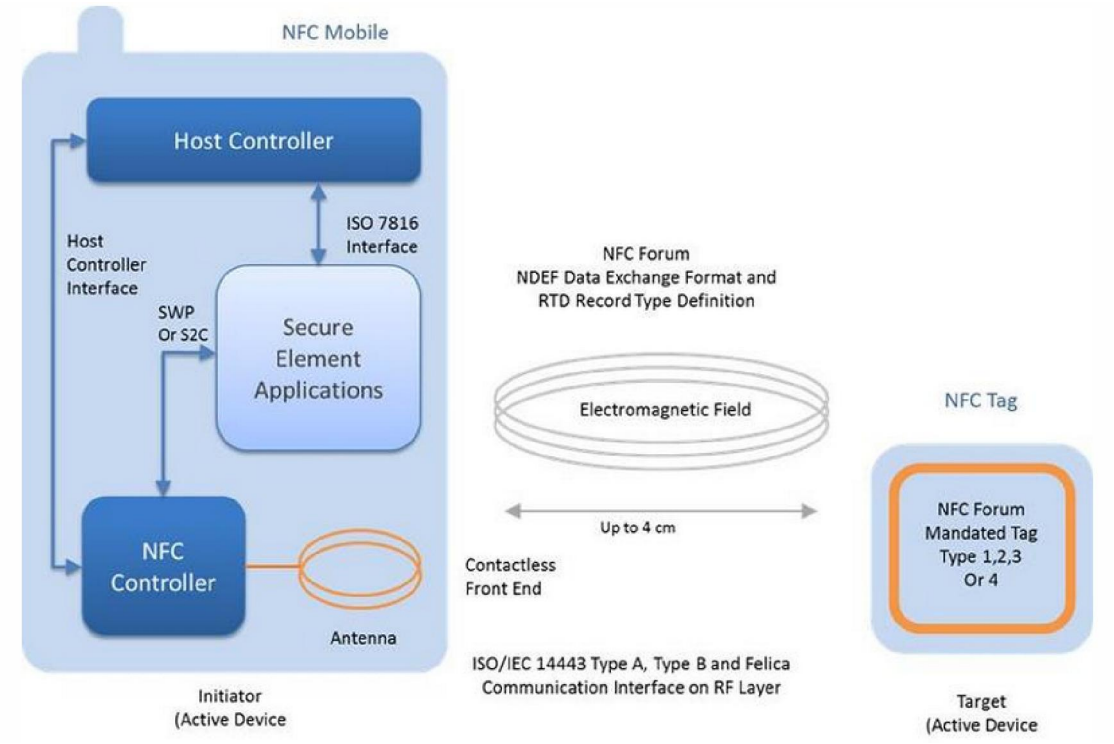

Figure 1.1: Reader/Writer Mode in NFC Enabled Mobile Phone

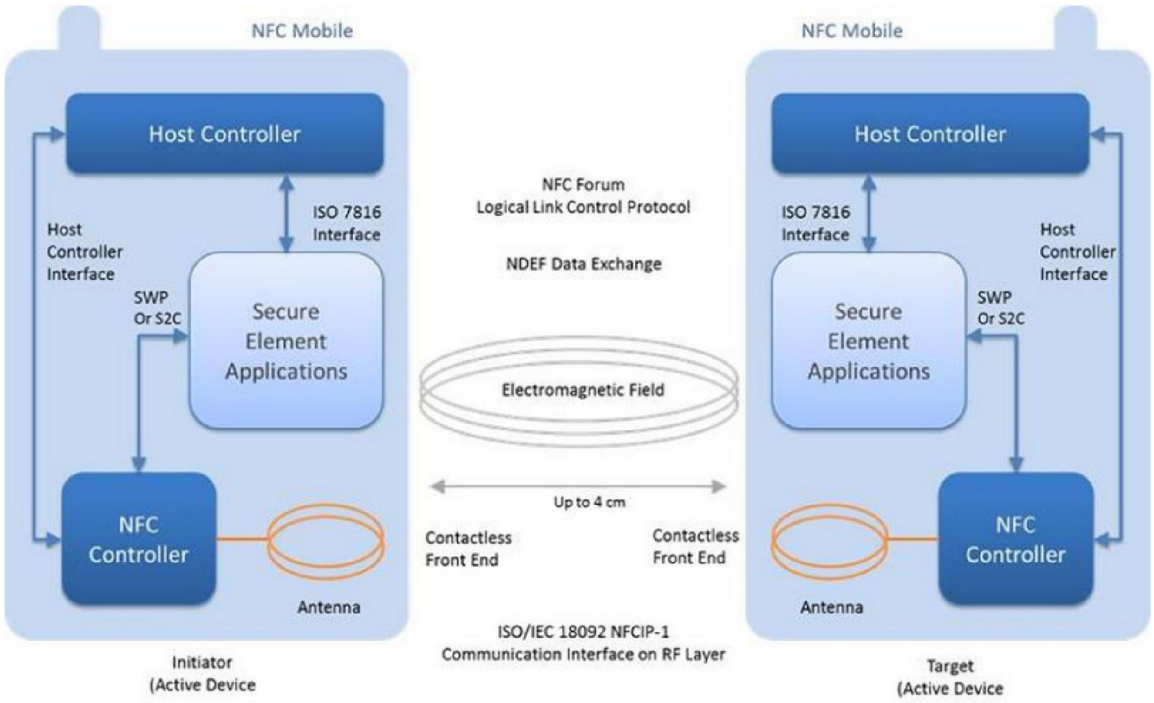

Figure 1.2: Peer-To-Peer Mode in NFC Enabled Mobile Phone

1.3 Architecture

NFC enabled mobile devices consist of integrated circuits, Secure Element (SE) and interface of NFC. The interface consists of a front-end commonly known as NFC Contactless Front-end (NFC CLF), antenna and a controller which controls all the communication over NFC. The SE is considered as an essential part of the architecture and it performs the basic security functions. It provides secure environment to the programs and the communication. It also leverages the security to the storage related with the NFC like credit card data. The SE and NFC controller are connected through a common interface known as Single Wire Protocol (SWP). SWP can used in conjunction with or can be replaced with another protocol known as NFC Wired Interface (NFC-WI). The host controller accesses the SE from within the device and can be accessed externally as well by the RF field. Typical architecture of an NFC enabled mobile phone is as shown in Figure 1.3 [5]:

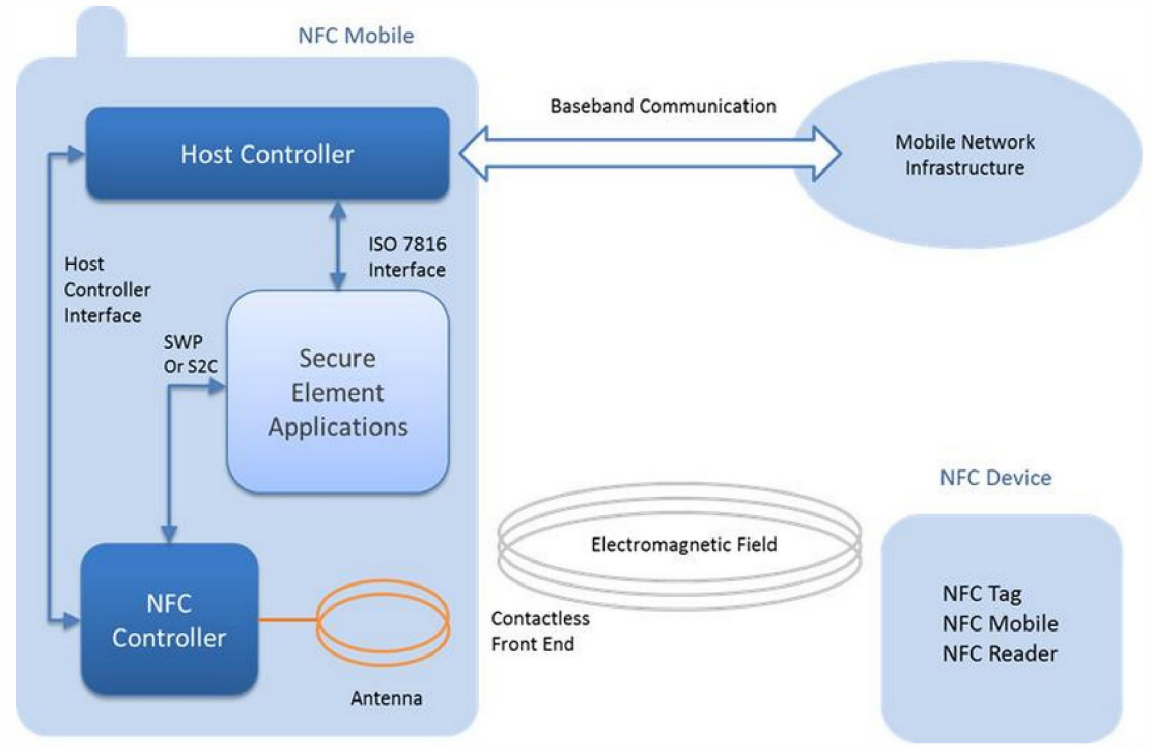

Figure 1.3: Architecture of NFC Enabled Mobile Phone

1.4 Threats

1.4.1 Eavesdropping

NFC communication takes place in wireless mode which is very prone to the chances of eavesdropping. It is a key threat in wireless communication which involves additional resources to stop such incidents. Communicate between two devices over NFC channel can be intercepted or received by an attacker in the vicinity of the devices. The attacker can use bigger and powerful antennas than the mobile devices to receive the communication. This enables the attacker to eavesdrop an NFC communication over greater distances.

1.4.2 Data Corruption

The data transmitted over NFC interface can be modified by an attacker if she can intercept it. The data corruption can be considered as denial of service if the attacker changes the data in an unrecognized format. The communication between the sender and receiver will be disturbed. This disturbance can be temporary if the attacker has focussed on the transmission medium between the devices. If the data stored on the tags or in the storage of the mobile devices is corrupted than it makes that particular tag to be useless and the mobile device would be required to get the data again.

Another way to corrupt the data can be by transmission of the same or valid frequencies at the time when legitimate devices try to communicate with each other. This sort of corruption can be performed by malicious software running on the same smart phone in background. This type of attack does not corrupt the original data but the data received at the receiver end is corrupted. It becomes a Denial of Service attack.

1.4.3 Data Modification

To move forward from data corruption to data modification, where attacker changes the actual data with valid but incorrect data. The receiver in this case receives data manipulated by the attacker during its transmission. The attack requires expertise of the attacker in the field of wireless and radio communication where she can play and handle the amplitude modulations of the transmission

1.4.4 Data Insertion

Rogue and unwanted data can be inserted in the form of messages by an attacker into the data while being exchanged between two devices. The success of attacker in this manipulation depends upon the duration of communication and the response time of the receiving device. The attacker needs to respond to the devices before the legitimate device wants to establish its communication. If both devices, legitimate and the spoofed transmit at the same time then the data received at the receiver end would be corrupted.

1.4.5 Man-in-Middle Attack

In Man-in-the-Middle Attack, third party tricks the two legitimate parties to be the other legitimate party and thus routing the communication between the two parties to go through the third party. Alice and Bob in the following figure are tricked by Eve to undergo a three party communication instead of a one-to-one communication.

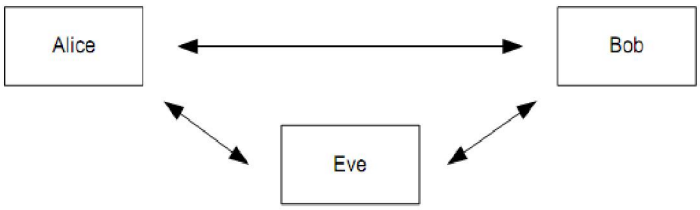

Figure 1.4: Man-in-Middle Attack Setup

Alice and Bob do not know that they are talking to each other through Eve who is listening to their complete conversation without being noticed. If we replace the link between Alice and Bob by NFC then it would be as per our scenario. The communication between Alice and Bob can be easily intercepted by Eve. The data reception by Alice and Bob is at the discretion of Eve who if wants can block the communication between them and alternatively she can send messages of her choice on either side. She can silently store the data being transmitted between the two parties.

1.5 Defense

1.5.1 Eavesdropping

NFC does not have any specific or particular guard against the possibility of eavesdropping. It is pertinent to highlight that passive mode data transmission is

comparatively difficult to be attacked upon than active mode communication. The use of passive mode only cannot be resorted to as many applications transmit data in active mode. Only solution to this type of vulnerability is to use a secure channel. The communication over NFC channel should be authentication based using the authentication and encryption schemes.

1.5.2 Data Corruption

NFC devices are designed to be able to detect RF fields in which they communicate. If the devices can detect the strength of an RF field and the difference when there is some additional RF in the same field then it can effectively counter this type of threat. A higher amount of power than the typical power of the RF field is required to corrupt data being transmitted. The increased power should be easily detected by the NFC devices. These types of attacks are easily detectable and can be countered as well.

1.5.3 Data Modification

Data modifications can be protected in a number of ways. Protection can be achieved by changing the Baud rate. Use of 106k Baud can stop modifications in active mode and make it impossible for an attacker to modify the data. But this implementation would require active mode be used at both ends to stop such vulnerability. This is practical but it increases the chances of eavesdropping manifolds.

NFC devices are capable of checking the RF field before transmitting the data. The sending device needs to continuously monitor the RF field for possibility of such an attack and counter the effects of the attack. The best solution to defend against data modification attacks is to use a secure channel for transmission and reception of data.

1.5.4 Data Insertion

Data insertion by an attacker is possible when the answering device is slow to respond the first device. A possible countermeasure is possible if the answering device responds to the first device without a delay. The attacker does not get the window to insert malicious or manipulated data.

Another countermeasure to data insertion by attacker can be achieved if the second device which is at listening end, continuously listens and monitors the channel

for its open time and start of a communication. The data insertion attempts by the attacker can be detected by the answering machine in this case. The best way to counter data insertion attack is by using a secure channel for the communication.

1.5.5 Man-in-Middle Attack

The distance at which the NFC devices operate is very short i.e. 10 cm. A Man-in-Middle attack is practically impossible to be carried out at such short distance. It is recommended that the communication mode for the NFC should be active-passive. A device should be active and the other device should be in passive mode. The active device should monitor the RF field for any possible disturbance or attack scenario.

1.5.6 Secure Channel for NFC

The best approach to guard against maximum attacks is to use a secure channel between the communicating devices. The secure channel can defend against eavesdropping, all types of attacks on the data during communication and Man-in-Middle attacks.

Diffie-Hellmann key agreement protocol can be used in conjunction with RSA or Elliptic Curves to protect and authenticate the channel between two communicating devices. The arrangement can be augmented with use of symmetric key scheme like 3DES or AES. The arrangement can provide confidentiality, integrity and authentication.

CHAPTER 2: ANALYSIS OF RFID ARCHITECTURE

2.1 Introduction

Remote Frequency Identification (RFID) is an electronic device which stores unique information about a specific item or asset with which it is associated. It is part of an automated process used for automatic identification of a tag containing RFID by a reader and processing of the information at the enterprise database subsystem. It is part of Automatic Identification and Data Capture (AIDC) routines and technology. Radio frequency coupled with magnetic and electric field is used in this technology. Use and implementation prospects of an RFID system are virtually limitless. The technology can be used to locate, identify and track objects of many types including humans, animals and goods. The technology is prune to different privacy, confidentiality, integrity and access control risks. Mitigation and reduction of these risks to minimum level can only be achieved deliberate planning at government, organization, department and individual levels. People are the weakest as well as the strongest link in achieving information security goals. This chapter describes various management, operational and technical controls in detail, which can be employed in an RFID implementation to safeguard against possible threats of any nature. The last part of the chapter enlists privacy related legislations and laws which are available to the government departments, agencies, public organizations, corporations, citizens and immigrants in United States of America. This chapter has been derived from the NIST standards for RFID [7].

2.2 RFID Technology Overview and Adoption in the Market

RFID (Radio Frequency Identity) Tags are rapidly growing in terms of number, quality, technology and utility in our daily life. Their first use dates back to World War II. Usability of RFID tags to identify and authenticate persons, goods, vehicles and electronic devices is increasing rapidly. The reader of RFID tags is linked with Database and network on the backend to store the information related to the tags. It contains an antenna to receive and transmit signals and a circuit to provide processing and storage. RFID tags are similar to smart cards except that no physical contact is required to activate them. Major replacement of bar codes and biometric passports with RFID tags is on the increase. The passive tags can be energized or activated by

magnetic field of the reader. The Active tags have their own battery source to activate them. Semi-passive tags have battery source to support their internal functions and are activated by the reader when required.

RFID systems are implemented in a variety of ways depending upon the requirements of the organization's security and business controls. The custom implementation of the RFID systems makes application of standard security policies ineffective and inapplicable. Security controls described apply to most RFID applications in this section. It does not address the security of smart cards and RFID payment systems. Security controls on systems of information technology, public internet, network communications, databases and/ or web servers are not discussed in this section because they are covered by different safety requirements, needs and guidelines. EPCIS resources can be accessed from the servers through internet by collaborators and these should be protected by the same types of controls that can be used for an online system, the other open (for example, to encrypt confidential communications and control the access to stop illegal and maligned access to data, information and systems) to make sure the security of information derived by the RFID system access. Guidelines and procedures on topics such as information technology, applications, databases and security can be sought from a number of sources and server networks, including the Computer Security Resource Centre (CSRC) of NIST.

RFID technology is emerging as the next generation in asset tag system. It is expected that within next few years every item carrying a price tag of more than one dollar will bear an RFID tag on it. These tags have already replaced bar codes from many items and more are converting to this technology day by day. Widespread use of tags has already raised a lot of privacy and security concerns.

2.3 RFID Security Controls

RFID security is a discipline which is growing at high pace. Although found the most promising research at the appropriate time, this section focuses on the current controls which are commercially practiced, available and used controls. Division of security controls and interacts in three main groups:

2.3.1 Management

It includes controls and management operations of RFID security systems. For example, the management of the institution can update existing policies to address security applications and monitoring interacts, such as the need for RF subsystem. Administrative control usually involves the risk assessment and planning systems and data acquisition systems, safety certification, endorsement and evaluation. The following sections deal with the management and control of the RFID system in detail.

2.3.1.1 RFID Usage Policy

- **Control**: A description of the use of policy and distribution of RFID without a license and regulate authorization to system personnel to work with specific RFID role. Policies should be integrated into the privacy policy of the organization , which involves topics such as how to store and share personal information. The use of RFID policies should describe the format of identification tags and cater for potential privacy issues.

- **Applicability**: The use of RFID technology, or planning to make use of by all the organizations.

- **Benefits**: This policy provides a framework for most other security controls. It provides a way to manage expectations regarding RFID and secure communications systems. It allows managers to make a person or entity legally bound to comply with this policy.

- **Weaknesses**: There is no policy to ensure compliance. Strategies need to be added in appropriate business and implementation of technical controls to enforce effectively.

2.3.1.2 IT Security Policies

- **Control**: IT security approach for achieving the goals of the policy on the use of high-level security. The policies of IT security should cover all subsystems, including security of network, database and application in the enterprise subsystems shared between the institutions. IT security policies to meet the RFID system must:

- Control access to information including the records in system databases,
- Boundary protection , including restrictions on the port and protocol for network traffic between RF subsystems and the company, sub-system of the company and the public or private network,
- Password management, with regard to production, sharing, storage, locking and killing of passwords,
- Safety management system for RFID readers and the hardware in middle, including the application and protection of read and write commands of SNMP community strings.
- Training in the field of RFID safety to administrators and operators of the system, and
- Associated encryption systems management, including the certification authorities and senior administration.

- **Applicability**: All applications of RFID, especially sub-systems of the institution or subsystems shared between the institution.
- **Benefits**: Security policies that govern the well-designed mitigation of business risk associated with using techniques of RFID. Prerequisites and guidelines for the design and implementation and maintenance personnel are provided by the policies.
- **Weaknesses**: There is no policy to ensure compliance. Strategies need to be added in appropriate business and implementation of technical controls to enforce effectively.

2.3.1.3 Agreements with External Organizations

- **Control**: When sharing data linked with the RFID system between organizations, roles and responsibilities can be formally listed in the agreements in the form of Memorandum of Understanding (MOU). These determine communications, authentication and security mechanisms applicable to the data while in transmission or storage. The mechanisms of exchange of passwords

between the organizations should also be mentioned in the memorandum of understanding.

- **Applicability**: If more than one organization is involved in the use of the RFID system.

- **Benefits**: The existence of a memorandum of understanding greatly reduces the risk of security loopholes.

- **Weaknesses**: It is impossible to achieve external monitoring and difficult to handle by the system and staff. Accordingly, conflicts may occur without being detected. A hired third party audit can reduce these risks between the signatories.

2.3.1.4 Minimizing Sensitive Data Stored on Tags

- **Control:** The sensitive data can be stored in a separate subsystem and on requirement can be acquired using the unique identifier of the tag.

- **Applicability**: The use of labels and memory on the chip be deemed sensitive. It can be mixed with other data to gather perceptive information.

- **Benefits**:

  -Random scanning or eavesdropping do not generate enough information for the opponent.

  -It is more economical to carryout encryption of data and access controls in the institution than on RFID system.

- **Weaknesses**:

  -ID can be used by the opponents to get important information about the make, model or type of the tag.

  -Moving the data to a subsystem in company makes it dependant on the network. Network delays for some applications are not acceptable.

2.3.2 Operational

Administrators and users perform daily operations of the control system using these type of controls. For example, RFID systems need to perform checks to ensure the physical security of the system and its proper use. Operational controls can be of several types:

- Restricting the physical access to RFID systems to only authorized staff.
- Careful deployment of the RFID system so that it should be free of electromagnetic radiation and interference.
- Destruction of tags by the organizations after their expiry to restrict adversaries from accessing the data.
- Trained operators can guarantee that employees use the system as per instructions and appropriate policies.
- Labels can bear information for the users to know the proposed RFID system purpose and thus can use simple methods to mitigate risks.

2.3.2.1 Physical Access Control

- **Control**: There are several ways to restrict or control physical access, like security cameras/ guards, turnstiles, walls, fences, door locks and gates. Any material which is relatively opaque to the radio communication can be used to stop physical access of the RFID system.
- **Applicability**: All RFID systems less those installed in the public localities.
- **Benefits**: It can be useful in defense against an adversary's intent to access the system in order to concede, destroy, modify or pilfer components. Security of physical components and RFID system installations is the major concern of the physical access control implementation. Following can be stopped by effective use of physical access controls:
  - Read and write of data on tag without authorization,
  - Tag cloning and rogue usage,

- Mislead readers by spoofing,
- Denial of service attacks caused by interference or commands that are not authorized,
- Targeting,
- Damage to the RFID device, and
- Hazards of Electromagnetic Radiation to Fuel (HERF) / Hazards of Electromagnetic Radiation to Ordnance (HERO) / Hazards of Electromagnetic Radiation to Personnel (HERP).

- **Weaknesses**:
  - Physical access control is not a measure against preventing interference of radio communication from legal discharge of radio communication from equipment in the same area,
  - The range of the RF signal may be longer than the predetermined operating range, allowing the use of directional and customized antennas,
  - No protection against insider attacks,
  - HERF / HERO / HERP still within the physical boundaries of the radiation emitted by the presence of the RFID system,
  - The piping system or other openings can let the radio signals to escape. Physical access control cannot restrict a radio signal as anticipated.

2.3.2.2 Appropriate Placement of Tags and Readers

- **Control**: Electromagnetic radiation caused by RFID systems can be controlled. Following be kept at a distance from the RFID equipment:
  - Petroleum, ammunition and other equipment which can cause damage if it is exposed to electromagnetic radiation,
  - Humans and specific products such as blood and drugs, which may be damaged due to prolonged exposure to radiation,

- Metals and materials which can amplify the signal or can modify to make the radio waves potentially dangerous,

- Interference to other wireless communications apparatus.

- **Applicability**: All locations and environments where the organization decided to deploy RFID equipment (not including numerous consumer and supply chain management applications).

- **Benefits**:

  - Radio interference risk reduction,

  - Remedy against man in the middle attacks and unauthorized transactions of the RF subsystem,

  - Reduction in HERF (Hazards of Electromagnetic Radiation to Fuel) /HERO (Hazards of Electromagnetic Radiation to Ordnance) /HERP (Hazards of Electromagnetic Radiation to Personnel).

- **Weaknesses**:

  - Tags positions and locations change in case of mobile items so they cannot be controlled.

  - Interference with other radios may continue even if the tag is moved in a new position.

2.3.2.3 Secure Disposal of Tags

- **Control**: The process to dispose-off the tags when these have been used should be safe and secure. It may involve the physical destruction and crushing. Destruction of electronics can be achieved using the kill command, or by exposing the tag to a strong electromagnetic field to destroy the circuit permanently.

- **Applicability**: Applications where the existence of a continuous presence of a tag which has completed its life may cause risks to the privacy of people and business intelligence.

- **Benefits**: Destroyed or disabled tags cannot be used later for tracking or accessing data stored on tags by an adversary.

- **Weaknesses**:

  - Although the minimum effort required to destroy but it increases the life cycle cost of the tag.

  - The destruction of a tag can eliminate the possibility of value-added functions in the future, like the products aftermarket support, recalls, follow-up of expiry date and support during recycling.

2.3.2.4 Operator and Administrator Training

- **Control**: Training operators and managers to provide staff with the skills and understanding required to meet the privacy policies and RFID security and agreements with external organizations. The staff may be performing different roles in different RFID applications where different type of training is required. The aspects which can be addressed by training are:

  - What is an unauthorized use

  - Detection techniques of unauthorized use

  - Violations reporting channel

  - Reduction of the HERF/HERO/HERP risks by employing safety distances.

  - Destruction and recycling of tags.

- **Applicability**: All applications of RFID technology.

- **Benefits**: Proper training of operator can help in normal operation and better maintenance of the system. Operators can also identify weaknesses and take necessary measures to stop future occurrences.

- **Weakness**: Only training cannot guarantee the normal operations, or adherence of the policy.

2.3.2.5 Information Labels / Notice

- **Control**: Messages disseminated with tags or pasted near each tag reader. The purpose of the use of RFID systems and notification on how to reduce the privacy related risks.

- **Applicability**: All RFID applications that can be used by simple information messages about how to reduce risks. It is particularly concerned with consumer applications where privacy is an issue.

- **Benefits**: User education/ awareness regarding RFID technology security and privacy mitigation steps.

- **Weaknesses**: The distribution of notifications does not ensure that it will be communicated as desired. Formal training and appropriate ways of communication are required to convey a technical word.

2.3.2.6 Separation of Duties

- **Control**: The division/ separation of responsibilities and duties in RFID systems minimize the damage which can be caused by the behavior of a person by mistake or malice. The possibility of two or more persons engaging in malpractice is less likely than one person.

- **Applicability**: RFID implementations in businesses where change of tag on valuable assets by an insider can render it to be priceless thus causing damage to the organization.

- **Benefits**: Fraud and malice can be reduced by separation of duties, since a user who intends doing such malice would require at least another person as well. It also reduces errors as multiple persons check the items while its transaction is carried out.

- **Weaknesses**: Employees can still make frauds in groups. Institutions with a limited number of staff cannot adhere to separation of duties in true essence.

2.3.2.7 Non-revealing Identifier Formats

- **Control**: RFID tags identifiers can be concealed by using non-revealing formats of the identifiers about the tags by randomizing the identifiers or by use of serially generated identifiers which hide the actual identifiers of the tags. The adversary reading an identifier which is encoded using the EPC code can only gain certain type of information like type of the item its manufacturer. Following shows a 96-bit EPC with the four individual fields which can be parsed.

Figure 2.1: Example 96-bit EPC for RFID Tags

- The control specifies the identifiers to be reprogrammable. The tag information of formats of standard types can also be programmed on requirement. Pre tagged items at the factory cannot be reprogrammed or modified afterwards.

- **Applicability**: An organization which feels that standard identifiers can cause a risk to its business intelligence if revealed.

- **Benefits**: The identifier alone does not reveal any information to the adversary.

- **Weaknesses**:

  - The identifiers which do not reveal identity restrict the organization from gaining the advantages of standard identifiers. Standard identifiers are useful in distributed database system implementations. Searching the items with standard identifiers is easy and can be performed at many locations.

  - Random allocation of ID can result in conflicts when two items are assigned the same ID. The possibility of such an event is very low, but it can cause errors in business process.

  - If the identifier is the distributed using some logic, an adversary can find the method used, this will destroy the order and control.

2.3.2.8 Fall back Identification System

- **Control**: The RFID system unavailability causes the RFID tags useless. Alternative means should be available to identify an object using text labels or the traditional AIDC technology like barcodes. Training of personnel on the standards and operational aspects to ensure that they have the adequate knowledge about the possible scenarios in which the system is to be used.

- **Applicability**: RFID technology for all applications.

- **Benefits**: The available duplicate tag ID serves as the fallback in case and data of the tags has been damaged due to intentional or unintentional reasons or the tag information is unavailable due to network outage or the system unavailability. It can also be used to confirm that data has not been modified incorrectly.

- **Weaknesses**: The possible weaknesses of the control can be:

  - Damage can occur to the data stored in and printed upon simultaneously.

  - Fallback systems will also be affected when the primary system is unavailable.

  - The printed data on the tags can easily be read and interpreted as per desires of the adversaries.

  - Text or barcode label cannot offer the storage capacity like RFID. Two dimensional barcodes can provide basic memory requirements as of RFID tags.

  - The fallback provided by AIDC based technologies cannot be guaranteed where variable tag data applications are used.

2.3.3 Technical

Engineering controls to control or restrict the use of technology, you can perform within the system. Requires RFID system controls several reasons, such as data protection on the label, leading to self-destruct labels to protect wireless communications. Each control provides information as follows:-

- Explanation and working of the control.

- Possible realizations or purposes that can be monitored by this control.

- The control offers advantage such as risk mitigation.

Implementation of control even if the control presents weaknesses, including the possibility of avoiding in some implementations, lasting risks and other remaining issues even if implemented.

RFID systems are under continuous research and review of the technical controls is also undergoing at the same pace. Various industrial organizations and universities are pursuing the research and development in this field. This section of the document focuses on various available commercially available technical controls. Tags are required to compute additional data due to the requirement of different technical controls. A tag performing these additional computations needs additional hardware in the form of memory and computationally more capable processor on the chip. The tag reader may also need to render more power necessary to energize a passive tag to perform these calculations. In addition, the reader may be required to operate at higher power, even though it may not be possible or even permitted in a variety of cases. A passive tag can restrict the use of certain technical controls due to the intrinsic characteristics. Control systems of RFID technology including radio and all the components exist for subsystems of an organization or enterprise. Technical controls are:

- Provision of basic services of authentication and integrity to various RFID mechanisms and operations.

- Effectively guard the communication between a tag and the reader.

- Safeguard the information stored on the RFID tags.

2.3.3.1 Authentication and Data Integrity

RFID systems essentially use typical authentication mechanisms of the IT system techniques. The systems use digital signatures, Hashed Message Authentication Codes and passwords. Primary aim of such techniques is to guard the tags against illegal reading from and writing on them. Integrity is provided by the use of various cryptographic primitives and techniques. This also stops against spoofing attacks on the

tags. A change in the transaction modified by an adversary can be detected at the reader or the tag.

2.3.3.1.1 Password Authentication

- **Control**: The commands which are protected by passwords are not allowed by the reader to be executed unless used with accompanied password. These commands can be executed during reading of data from the tag or when tag is being written. Passwords management systems are used by companies to operate and implement controls of this type. The system deals with password stages, including initiation, transport and subsequent storage. Indiscriminate selection of passwords is the basic requirement to comply with the security requirements. The passwords are written to tags in a protected location to decrease the chances of eavesdropping. Additional security systems are required to be incorporated when the RFID system is deployed in a scenario where it has to be accessed by multiple organizations. Password change policies as practiced in conventional IT systems cannot be afforded in case of RFID systems. The tags will be required to be brought in the controlled environment and accessed to change the passwords which may not be technically feasible.

- **Applicability**: Any RFID implementation which incorporates authorization schemes to execute specific commands which are required by the business process or risks present externally.

- **Benefits**: Unauthorized use of tags is reduced.

- **Weaknesses**:

  - A large deployment of tags makes the management of passwords intricate, especially when the passwords are shared with other organizations as well, as in the scenario of supply chain systems.

  - Interception of passwords by the adversary cannot be ruled out. The same can be used to malice transactions at a later time.

  - Large deployments complemented with multiple organizations involved can force the same password to be used on multiple tags. The loss of single

password can cause a hazard in this case and integrity of the data cannot be promised.

- Brute force techniques can be used to crack passwords stored on RFID tags.

- Passwords of some passive RFID tags can be compromised using attacks on power scrutiny.

2.3.3.1.2 Keyed-Hash Message Authentication Code (HMAC)

- **Control**: Tag and reader use shared secret key in combination with a hashing algorithm to provide authentication which is mutual. Integrity of the information in the messages coded with HMAC is ensured.

- **Applicability**: Applications that use passwords only, authentication mechanism is not sufficient due to the high eavesdropping risks.

- ***Benefits***: HMAC benefits compared with password authentication:-

  - Provides evidence on the validity of the tag ,

  - Protection of integrity, and

  - Plain text data is not transmitted, eavesdropping is handled effectively.

- **Weaknesses**:

  - HMAC has similar challenges of key management like passwords.

  - Duplicating a tag with HMAC keys is a hazard which is prevalent.

  - The tag authentication is invalidated if an attacker gets physical access.

  - Sharing of HMAC keys amongst multiple organizations is dependent on the trust between them.

  - Complex circuitry is required on tags with better computation and memory requirements.

2.3.3.1.3 Digital Signatures

- **Control**: Use of public key cryptography in the RFID systems provides entity authentication as well as non-repudiation for subsequent verifications based on the transaction records. The signatures are generated by the tag readers and stored on the tags. The readers sign the digital certificates. The scheme used for digital certificates is commonly known as asymmetric cryptography. The authenticated RFID working is as follows:

  - Manufacturer embeds identifier in the tag at factory.

  - The tag generates public key in response to a public/private key pair generated by the reader.

  - Message digest is calculated by the reader using a hash algorithm based on the unique identifier of the tag. The message digest is encrypted using public key of the reader. The reader then generates digital signature which is transmitted to a tag and stored on it.

  - The tag when read by any other reader, the reader decrypts the digital signature of the tag and decrypts it using first readers public key. The message digest thus computed is matched with the original one for a possible match. The authenticity of the digital certificate is validated if the message digest matches.

  - The transaction carried out with the new reader is stored on the tag or even on the corporate subsystem.

- **Applicability**: Used where requirement of the applications is more than just authentication provided by HMAC techniques. It can be even useful in scenarios where the system needs to establish authentication without using the network.

- **Benefits**: Advantages provided by digital signatures are as following:

  - The encryption and decryption techniques are on the readers only. The reader is responsible for management and maintenance of the digital signature. Use of public key cryptography means that no secrets are shared between the two devices before start of communication. Tags do not contain any secrets, so the system is more robust as the tags are vulnerable to adversaries.

- Network availability is not strictly required for this system.
- In enterprise system the organizations only need to share the public key.
- Prevalent RFID standards are compatible with the digital certificate scheme.
- The transmission, reception and storage of digital certificates can be performed using existing system commands on the RFID tags.

- **Weaknesses**:
  - A complete infrastructure of PKI is required for this implementation which includes dedicated hardware and software for the authorities like registration and certification. PKI implementation requires deliberated efforts and dedicated management staff.
  - Memory requirements of the system at reader and tag are more in case of systems which incorporate digital signatures.
  - Adversaries can still perform replay attacks using the information acquired from a tag.
  - Tags at present have a very limited computation capacity.

2.3.3.2 RF Interface Protection

Control functions associated with the tag RF interface are as following:

- Cover-coding to hide the message information.
- Encryption of data before transmission.
- Eaves dropping and random scanning can be limited using the various shielding methods.
- Capability to perform in RF populated can be achieved by selecting appropriate frequency which can act against interference and better operations in areas with metal or concrete structures.

- Electromagnetic radiations hazards can be minimized by using active tags. It can be even used for defense against eavesdropping as well.
- Switched tags can be used which transmit only when required.
- The tags can have the operational mode to activate or disable RF interface.
- System health and presence of the tags in an area can be assessed by periodic polling transmissions by the reader.

2.3.3.2.1 Cover Coding

- **Control**: Hiding of information and data from un-intended listeners can be achieved through cover-coding technique. EPC global defines protocol for cover-coding to be used in RFID tags, which is as follows:
  - Reader requests key from the tag.
  - Key in the form of 16-bit random number is transmitted to the reader.
  - XOR operation is used by the reader on the key and plain text to generate cipher text.
  - Tag receives the cipher text from the reader.
  - The tag recovers the plain text by applying XOR operation on the key and the cipher text.
- The following figure depicts working of cover-coding.

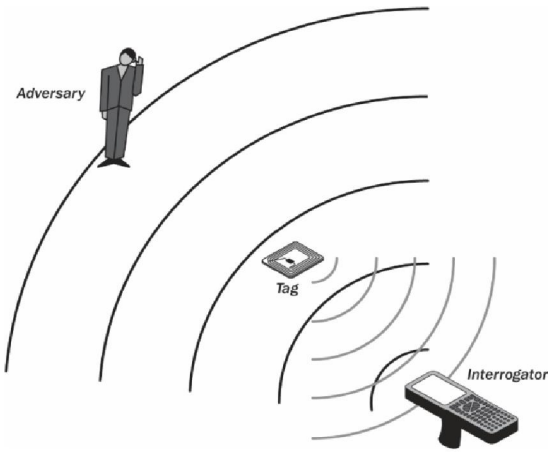

Figure 2.2: Cover-Coding

- **Applicability**: Cover coding is a help against reducing the risk associated with eavesdropping. To receive tags communication on the back channel the adversary has to be in less than four meters distance. Readers signal power is much more than a tag so these can be intercepted over much longer distances.

- **Benefits**: Cover-coding can be helpful in prevention against malicious commands execution which can tamper the data on a tag to make it harmful for the organization or useless at all.

- **Weaknesses**:

  - Interception of a key by an adversary can make her capable to read any message and decrypt it as well.

  - The generation of random number is very critical. If the number can be predicted by an adversary then the system is open to her.

2.3.3.2.2 Encryption of Data in Transit

- **Control**: Encryption of data before transmission in air.

- **Applicability**: Institutions where the applications require guard against man-in-middle attack. The tags have to be capable to process the information and encryption functions.

- **Benefits**: Defense against eavesdropping of RFID transmissions.

- **Weaknesses**:

  - Complex management of keys which are required for encryption of data.

  - RFID communication may be subjected to delays due to inclusion of cryptographic primitives and functions.

  - Requirement of additional power for cryptographic functions. Passive tags lack power capabilities.

  - Cost of the tags can increase by introduction of onboard encryption technology which can make it financially unviable for organizations to adopt.

2.3.3.2.3 Electromagnetic Shielding

- **Control**: Shielding materials surround and limit the wireless signal in the protected area. Shield can be of different size and shape as per the requirement of the application. For example, a metal material protection used for travel documents to restrict the RFID reads. These substances mitigate the reading of the tag from the passport when the cover is closed. Shielding can also be mounted on walls or benches to prevent RF radiation leaving the restricted area. An effective way to shield a tag is by placing it in an aluminum foil package. Following figure shows RFID shields.

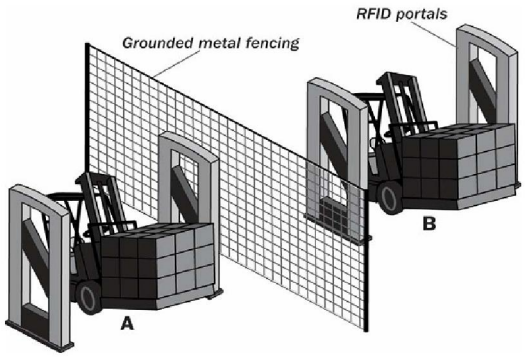

Figure 2.3: Grounded Metal Fencing as Shielding

- **Applicability**: Applicable where chances of eavesdropping or RF radiation exist.
- **Benefits**: RFID information and data is effectively shielded against eavesdroppers and readers which are unauthorized.
- **Weaknesses**:
  - Legal reading of tags can also be limited or disabled due to the use of the shielding in containers or boxes.
  - The possibility of an eavesdropping activity within the restricted or shielded area cannot be ruled out.

2.3.3.2.4 Radio Frequency Selection

- **Control**: Selection of a particular frequency to be used with RFID schemes to mitigate the interference effects. Various frequencies available to be used with RFID systems like microwave, LF, HF and UHF. An RFID system can use multiple frequencies for the frequency hopping to avoid collisions. Frequency allocation by government agencies for the specific purpose is carried out in almost all countries. Site survey to check for frequencies being used in the area of intended deployment of the RFID technology.

- **Applicability**: The locations or system implementations where no limitation enforced by an existing implementation.

- **Benefits**: Useful where the interference, range or penetration power are concerns.

- **Weaknesses**:

  - Interference cannot be traced most of the times. Possible sources which can generate interference should be analyzed before deployment of RFID system in an area or location.

  - Same frequency tags have to be used by all the organizations which are working in an enterprise to keep the notion of interoperability.

2.3.3.2.5 Adjustment of Transmission Characteristics Other than Frequency

- **Control**: Transmission characteristics like direction, range, power, type of antennas, transmitted energy of tag and reader and the duty cycles generated by a reader are to be adjusted as per requirement.

- **Applicability**: Applications which require protection against eavesdropping, interference control and protection against electromagnetic radiation hazards.

- **Benefits**: Reduction in power transmission can:

  - Mitigate interception of traffic by an adversary.

  - Reduce interference of radio waves with other radios operating in vicinity, and

- Electromagnetic radiation reduction

- **Weaknesses**: Performance of the system can degrade if the power of transmission is reduced. Reduction in duty cycles can also result in the same situation. Tags present in the locality can be missed by the reader.

2.3.3.2.6 Temporary Deactivation of Tags

- **Control**: Some tags have the capability to switch off the radio interface. Implementation of the control means that the tags will be enabled or switched on when these are required to read otherwise these are switched off.

- **Applicability**: When the communication between the tag and reader is foreseeable.

- **Benefits**: Temporary deactivation of tags:

  - Helps in prevention and reduction in reading of tags while in storage, and

  - Reduce the battery exhaustion of active tags.

- **Weaknesses**:

  - Transactions can be missed if a tag fails to reactivate.

  - Activation of every tag by a human can add to labor costs.

  - Activation of the tags may take some time thus causing delay in the normal working procedures.

2.3.3.2.7 Tag Press-to-Activate Switch

- **Control**: The tag is activated by pressing a switch present on the tag otherwise the tag remains in deactivated state.

- **Applicability**: When the owner of the tag wants to control the reading of the tag.

- **Benefits**:

  - It provides access control feature.

- Automatic reading of the tag is nullified.
- Privacy control is provided when required by a business application.
- Chances of eavesdropping will be reduced to the occasion when the tag is switched on and being in the close proximity.
- User is in control of the tag operation.

- **Weaknesses**:
  - The process of activation of the tag may cause some delay in the normal operation.
  - Automated process is preference of some users who may discard the switch operated tags considering it inconvenience.

2.3.3.2.8 Tag Polling

- **Control**: To check status of a tag, a reader reads tags on specific periods.
- **Applicability**: Operations where periodic counting of assets is required by the system.
- **Benefits**: Information regarding presence of items/ assets and their condition can be easily verified.
- **Weaknesses**:
  - Life of battery of active tags is reduced.
  - Polling frequency can cause uncertain data collections.
  - An adversary can easily carryout traffic analysis.
  - Eavesdropping is convenient.
  - Theft of items where tags are left behind to keep showing the presence of the item.

2.3.3.3 Tag Data Protection

2.3.3.3.1 Tag Memory Access Control

- **Control**: Read or write operations of the tags are password protected.
- **Applicability**: Applications which use the memory of the tags to store data.
- **Benefits**: Separate operations for the read and write lock commands on the tag ensure authorization control.
- **Weaknesses**:
  - Limited length of passwords being a concern.
  - Management of long passwords.
  - Physical tampering of tags still possible.

2.3.3.3.2 Encryption of Data at Rest

- **Control**: Encryption of data before transfer to tag storage.
- **Applicability**: If the requirement of data by applications is more than the capacity of the tag then additional data is stored on the enterprise system.
- **Benefits**: Authorization of data is ensured by using encryption techniques.
- **Weaknesses**:
  - A key management system is required which may be hard to operate and complex to manage.
  - Use of network for cryptographic functions may add additional delays in the system due to latency in the network.

2.3.3.3.3 Kill Feature

- **Control**: A password protected Kill command to disable a tag permanently.
- **Applicability**: Applications which require privacy of data after a tag has completed its life.

- **Benefits**: A tag cannot be reused after it has been disabled permanently by use of the kill command.

- **Weaknesses**:

  - If the password of the kill command is learnt by an adversary, the tags can be rendered as useless after malicious activity by the attacker. Same password on multiple tags can add the gravity of the situation.

  - Tags which are killed cannot be used again thus losing their further utility.

  - Weak passwords and prolonged password age pose serious threat to the tags.

  - A killed tag can still be used to extract data which is present in its memory.

  - A user may be unaware of the status of the tag which has been killed.

  - Common user cannot initiate kill procedure as it requires knowledge as well as the hardware to perform the task.

2.3.3.3.4 Tamper Resistance

- **Control**: Some RFID tags provide resistance against tamper. A tag can become useless if removed from the item with which attached or someone tries to alter the data stored in it, as the tag design of being sensitive to such activities destroys it.

- **Applicability**: The applications which cannot monitor tags continuously as the tags move away from the system as well. A user may require this type of tags due to some special implementation.

- **Benefits**: It prevents removal of tags from items. Tags can be used to ascertain the limits of the environmental conditions where a tag will be destroyed if subjected to more extreme states than what it has been designed for.

- **Weaknesses**: Adversaries can manipulate the tamper resistance of the tags. These do not prevent the theft or destruction of the tags.

2.4 RFID Privacy Considerations

Primary focus of this chapter is about security of RFID systems. Privacy concerns are always listed when we talk of privacy. Similarly confidentiality is also considered necessary when protection of privacy using technical controls of security in the RFID systems is intended. This section of the document contains explanation of various privacy related concerns involved in the functionality of RFID systems. Implementation of privacy in a system is complicated as it involves the organization's proprietary information in addition to the personal information of the employees serving in it. It has legal impacts as well. The implementation strategy involves the organization's top management, the legal team and chief information security officer.

2.4.1 Types of Personal Information

Rules and procedures regarding access, management and safeguard of personal data and information are explicitly addressed in various Federal privacy laws.

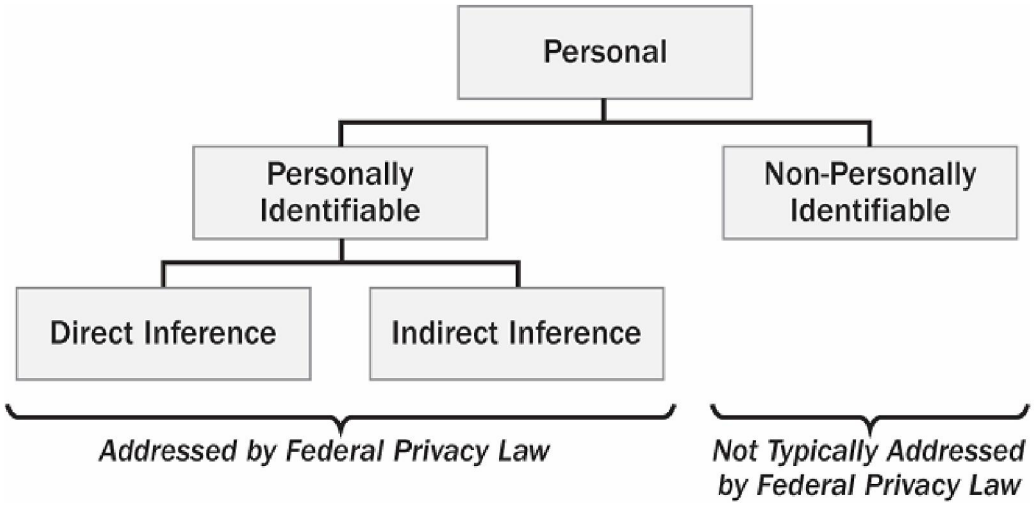

Figure 2.4: Taxonomy of Personal Information

For the current privacy laws, the most important difference in terms of the information being processed is whether personal data and information is in the form of personally identifiable information (PII) or not. A person can be uniquely identified and located by using various aspects of PII like name, gender, age, residential address, social security number and religion. A plurality of information, which is not considered

a separate PII, while still can uniquely identify a person by some combination. Identity of a person can be established by indirect inference using data elements of PII and direct inference using elements of information like license number of a driver. Laws protect privacy of PII which can be acquired through direct and indirect means to inference.

The laws do not involve data elements which as per personal opinion of an individual do not meet the standard definition of e-Government Act of 2002 of the PII. For example, an anonymous person moving on a street might think about loss of privacy, if another person with an RFID reader can judge what books he/ she reads or is taking specific medication by remote scan of the bag or wallet in which the tagged books or medicine is carried. Anonymity of the individual is still intact but it may affect the perception of privacy, because they do not display the control of personal information to others. Institutions may implement RFID systems and may also opt to moderate the risk associated with these conditions.

2.4.2 Applicability of Privacy Considerations to RFID Systems

A large number of businesses and processes which may not have privacy requirements are supported by RFID technology. It may not be a privacy consideration when supporting the industrial production systems, for example RFID and tracking process used for animals and assets management systems. When this system is used to collect, store, or disclose personal information privacy considerations exist. RFID systems can be used in different ways, or disclosure of personal information:

- A tag or database in the enterprise storage subsystems can be used to store PII like name or bank account number.
- Personal items like blood sample, a drug bottle or legal documents folder containing personal attributes can be associated with a tag.
- Description of an item or part of an item which is tagged, in possession of the regular and frequent traveller or individual, e.g., a car or truck, a box or a bag or anything which can significantly be associated with a person.

Although the idea personal identifiable information and privacy are not new, RFID technology has introduced new and complex privacy concerns in a number of

technical reasons. For example, RFID adds to the potential that PII can be generated by some indirect methods. Information related with some commercial transactions can easily be recorded, stored and treated in desired manner due to the RFID technology aids in tracking assets. In our daily life along with an increase in new opportunities on the level of coverage PII details in these systems increases information systems capability and may generate the data elements combined from different sources.

Many of the inherent characteristics of the RFID tags make implementation of privacy related controls extra difficult than conventional IT system implementations.

2.4.3 Privacy Principles

Effectiveness of privacy policy foundations is enhanced when it is based on a careful perception which lists the risks linked with privacy principles. Carefully developed and formulated basic principles of privacy requirements can be further designed to address specific organizations or applications. Main types of privacy objectives perceived are:

- There must be personal information storage systems the existence of which is secret.
- Individuals must have ways to know about his or her files, information stored in it and how it is being used.
- Individuals must have access to correct their information in the records.
- Organization must ensure consistency of the data for its established use while implementing processes of creation, maintenance and distribution, and
- Individuals must have privileges to prevent an object of information to be used for other purposes without the consent of the owner.

2.5 Possible Improvements

Lot of development has been seen in the field of RFID to make it more user friendly by incorporation in different new implementations. Some of the recent developments include:

- Automated toll collection on roads and highways.
- Integration in the smart cards for contactless payments.
- Massive distribution of sensor networks (Stardust).
- Near field communication technology in the smart phones.
- Reportedly RFID cards are being used by Facebook at the live events where guests present in the events can capture/ post photos automatically.
- RFID based smart tickets being used in transport systems.

The above mentioned uses are rapidly growing in number and popularity. As the use of RFID tags is growing, so does the concerns related with it. There have been independent research and development efforts by many individuals and groups in the field of RFID technology. Many schemes and implementations have been developed and tested to help guard against various security and privacy issues being faced by the RFID technology. Following are some of the improvements suggested in different literature and books [8]:

- Use of random pseudonyms so that only authorized readers should be able to determine the real identifier behind a pseudonym.
- Use of blocking technique where identifier/ address of a tag is hidden by incorporating binary tree walking.
- Use of a blocking device to stop eavesdropping and reading by attackers and adversaries.

2.6 Conclusion

The RFID tags have limited computational power, storage and bandwidth to communicate with the reader. For devices with these restrictions the requirement of cryptographic functions is also at a very light scale. Only $1/5^{th}$ of the total computational and storage space is available for the security aspects of the RFID tags, rest all is allocated for signal processing and memory operations. With increase in utility of RFID tags in our daily lives, the data contained in these tags needs to be

protected while it is in the tag or during communication with the reader.

Cryptographers have tried various cryptographic techniques to achieve the secrecy and security of the data contained in the tags. Basic algorithms like DES (with variants like DESL and DESXL) and AES have already been implemented. Privacy issues have gained focus where any attacker can interact with the tag or carryout tracing attacks on the tag or the reader, can tamper the tag to get the info about its communication technique or even the info or data contained in the memory of the tag. Privacy model for the RFID tags suggests that; the secrecy of RFID tags is the inability of the attacker to gain any information while observing the interaction of the system; and, it is system's ability to defeat impersonation attacks. Scientists and researchers could not clearly define the privacy in mathematical terms. Many approaches have been proposed by different researchers.

While different tags have varied privacy levels based on their make and memory capacity. The tags have been categorized as having weak, forward and strong privacy. Weak privacy, achieved by use of pseudorandom function with secure cipher like AES, is for attackers who cannot alter the tags. Forward privacy destroys the tag if it is tampered with and requires use of public key for encryption. Strong privacy is for the adversaries who can access data stored in a tag and be applied to tags with weaker privacy. Strong privacy requires more advanced techniques to achieve privacy, secrecy and security.

Management, operational and technical controls should be used in combination to reduce risks to RFID implementations in business processes. RFID is customized by organizations as per their requirements generated by the businesses. The security controls cannot be ideally mapped to all types of implementations of RFID. Organizations are encouraged to carry out an analysis of their business processes in consideration with the RFID system implementation and various security controls which can be effectively use with some modification or deviation.

Privacy thoughts are closely linked and interconnected with security considerations. An RFID system should be able to identify possible risks and control procedures through use of a security program to safeguard personally identifiable information (PII). An information development lifecycle should be used and privacy

officer of the organization and legal teams should be incorporated while implementing security and privacy plans for RFID systems. Any information which cannot be used to accrue PII is normally not covered under legal considerations. It can still be privacy issue for some personnel who are more considerate about their privacy. Implementation of security controls to protect personal information of employees and corporate data of the organization, in most of the organizations is on voluntary basis. Different controls implemented for privacy concern will also provide security to the system.

CHAPTER 3: ANDROID NFC ARCHITECTURE DEVELOPMENT

Android has emerged as the most popular OS for mobile devices in the recent years. The open source architecture of Android with the inherent flexibility to be adapted to new hardware platform has contributed to the success and popularity of the OS. Today almost 80% of mobile market share is held with the Android. Unfortunately this popularity comes with a cost. Android popularity has also attracted with it the tremendous amount of negative efforts in the form of malware for Android platform. The recent years have seen an un presented explosion of malware growth both in form of quantity and quality. In this chapter, a detailed survey of android security architecture and how this architecture is exploited by malware writers would be presented. In addition different solutions by researchers for combating malware would also be analyzed.

3.1 Introduction

In recent years, an explosive growth for Smartphone sale and usage has been observed. The improved capabilities of smart phones in the form of increased processing, increased memory and availability of different hardware gadgetry such as GPS contribute to their popularity. According to a recent survey, there will be 2.1 billion smart phones by the end of year 2016. The number of devices is growing at an average of 45% a year. Out of 1.4 billion devices currently in use, almost 80% of share is held with Android. The popularity of Android has also given rise to an explosive outburst of malware infection. Android accounts for 79% of all mobile malware according to US Department of Homeland Security.

Given the rampant growth of malware for Android platform, it is of utmost necessity to evaluate security architecture of Android along with different solutions for mitigating the risk of malware. Since Android framework is based on Linux kernel therefore it uses its security architecture at its base for implementing different forms of security implementations specific to the framework. Android uses DAC for allowing access to different system component in the form of API for usage in user applications. We will analyze the Android architecture, Android permission model and component

security and permissions. At the last different solution proposed by the researchers for mitigating the risk of malware would be discussed.

3.2 Android Architecture

Android [15] forms a stack of software with each lower layer providing services to upper layer. Linux kernel forms the lower most layer performing the most basic functions like memory management, resource allocation etc. This layer provides the hardware abstraction function in the form of different drivers managing different parts of hardware. This layer provides some of the basic functionalities for access control. Native Libraries lie above the kernel and consists of native compiled code for use by the system. This layer provides some basic services that are used by other programs. The layer above this layer is Dalvik Virtual Machine and program run time environment. DVM is an optimized virtual machine for executing java byte code in an efficient manner. Android framework libraries lie directly above DVM layer. This layer provides services such as Activity Manager to be used for android applications. Next layer is the layer for applications written in java. These applications run in their own instance of DVM and virtually separated from each other. Application running under DVM use libraries from the layer lying in between DVM and itself.

Linux lies at the base of Android framework. Android uses the Linux access control mechanism to provide some of the very basic access mechanisms for Android applications. Under Linux, each resource has UID which represents the user ID of resource owner. Similarly every resource has GID which is the ID of the group that own the resource. User can only access a certain resource whose UID is the ID of that user or the user is member of the group which is the owner of that resource. In addition to owner and group there is another category that consists of users that does not come under owner or group. Different permissions used under Linux are read, write and execute. Android carries forward the same access control mechanism. Under Android when some new package is installed, a new user ID is generated and allocated to the application. Any data generated by this application in the form of some file, database etc is also allotted the same UID as that of parent application. This model allows the application to access these resources. This default behavior can be overridden by the user application and can assign user defined permission to the resources it owns. Every application installed under Android has different UID and thus practically separating

each application from the other. Any application running under root ID will be able to bypass Linux access control mechanism and can access any application on the system. An exception to Linux permission model is SD memory card. SD card uses file system that is not supported by the Linux and therefore all data needing protection on SD card must be encrypted.

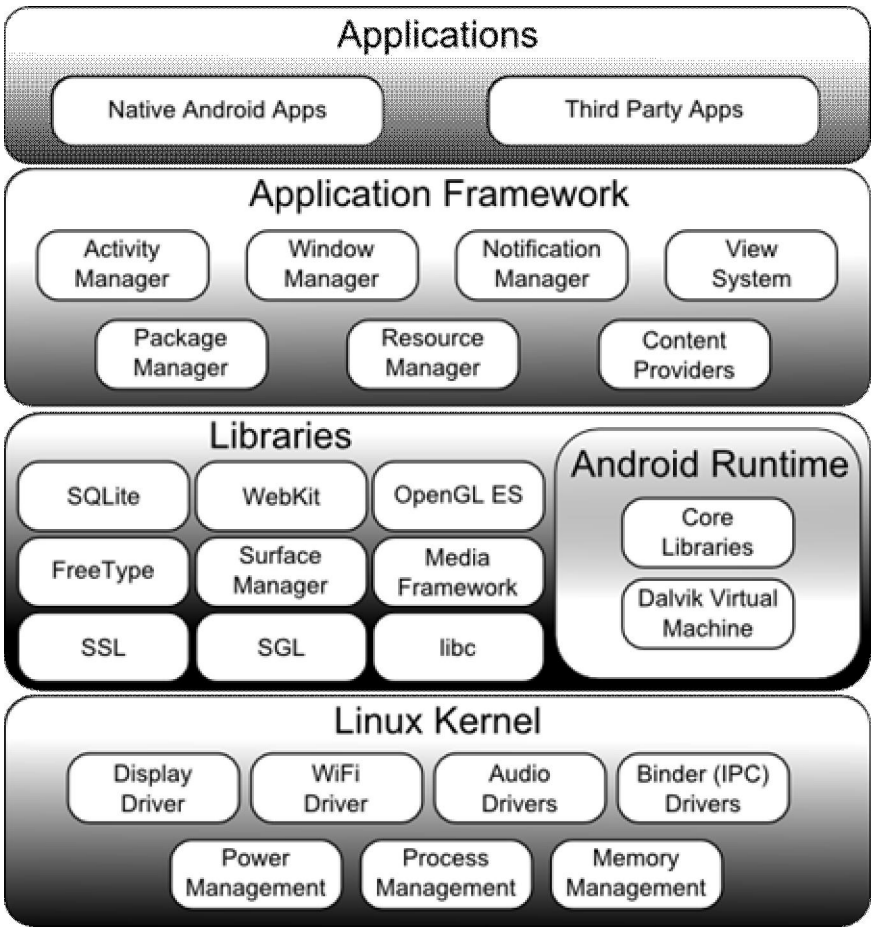

Figure 3.1: Android Architecture

Under Android application can only be installed if it is signed. Updates for some particular application signed by private key KA must also be signed by the same key in order for updating to succeed. It is possible that two different applications share the same user ID. Under such condition both applications will also share their data with each other. For sharing of user ID and data both the applications should be signed with the same private key. In addition the string associated with shared UserId attribute in manifest file of both applications must be same. All the components that are part of the same package run under one process by default. But it is possible to run different components of the same package to run under different processes.

3.3 Android Permission Model

Under traditional desktop environment, applications run with the privileges of user who have started it [15]. If a browser is compromised by injecting malicious code in it, that malicious code will run with the privileges of user starting the browser. Under Android, each application runs with its own user ID and therefore can only access its own data and files. Android has implemented the mechanism of asking user for the permissions of the application at the install time. All the services and API in Android is protected by certain permissions. Only that application can access certain API or service whom the user has granted permissions required for that application. Thus malicious code in some compromised application will only be limited to areas for which user has granted access permissions. The objective of the permission system is to allow user to make an informed decision as to whether install certain application or not. The real benefit of this strategy can only be realized once user carefully analyzes the requested permission by the application. An example of permission is INTERNET which is required by all applications to communicate on the network connections. All the permissions that the application require in order to fulfill its design goals will be listed in the manifest file of the application and would be presented to user at install time for acceptance or rejection. There are four categories of permissions. Normal permissions are harmless permissions e.g. permission to change background of Android phone. These would not be asked explicitly from user but will be installed automatically once the application is installed. However user has the flexibility to query these types of permissions. Second category is Dangerous permissions. These types of permissions can harm the user e.g. impairing user of his account balance. These types of permissions would be explicitly asked from user. Third category of permissions is Signature. This permission is automatically granted to the application if that application is signed by the same signature as that of requesting application. Fourth category SignatureOrSystem follows the same rule as that of Signature except that system image also gets the same permission in addition to requesting application.

3.4 Android Component Security

An Android application consists of four types of components [15]. One type is activity which is basically the user interface of the application or in simple words what you see on the screen. Second type of component is content provider. The objective of

this type is to share data across applications. Third type is broadcast receiver that is used for receiving system messages called intents. Service is the fourth type of component that is used for background processing. Intents are the primary means for the components to communicate with each other.

Components can be public or private. Public components allow components from other application to interact with them. In case of private components the only components that can communicate with it are those from the same application. Whether the component is private or public depends upon the *exported* attribute in the manifest file. The default behavior depends upon how the component is used. If there has been some intent filter specified by the component, it means that component want other application components to use it and therefore default value of *exported* will be set to true. If there are no intent filters specified, *exported* attribute will default to false.

In addition each component can create permissions so as to limit access to only those applications which have declared the required permissions. In this case the required permissions can be mentioned in the manifest file of the component. In case of content provider separate permission for reading and writing the database would be required. A write permission does not necessarily imply read permission as well. For reading and writing, both the permission to read and write would be required. Under certain situation, a component that has read/write permission to a content provider would be required to delegate that permission to another application for performing some specialized task through the process of URI permissions. It is possible to configure a content provider in such a way that would allow the application having read write access to it to delegate temporary URI permission to another application.

3.5 Characterization of Mobile Malware

Broadly speaking Android malware can be categorized in four broad categories [12]. First and the most common type is Mobile Device Data Stealer. They try to acquire different information such as OS version, product ID, IMEI number and IMSI number. This information can be used for future attacks. Second type is Rooting Capable Malware. Rooting is performed in order to get root access of the infected mobile. Attacker with root access can have unrestricted access to the mobile resources. Third category is Premium Service abusers. These type of malware send text messages

to premium numbers and make mobile owners to pay for services which they have not used. Last category is Mobile Device Spies. This category monitor different kind of private information such as GPS location, text and email messages and send them to attacker over the network.

Yajin [16] has analyzed 1260 malware samples and characterized them in 49 different categories basing on their functionality, behavior and other characteristics. The author discovered 36% of all these malware were using root exploits, 90% converted mobile phone into part of botnet, 45% can send premium based SMS and 51% were stealing user information and credentials. From malware installation point of view almost 83% of all malwares were using repackaging. Repackaging is the process whereby an attacker disassembles a popular application, encloses malicious payload, assembles it again and publish it on mobile market. Another technique is to repackage an update component that would download and run malicious payload at runtime thereby making static analysis of the malicious code impossible. Third technique of malicious application uses drive by download by exploiting some vulnerability in the mobile browser. This category also includes enticing users to download new feature rich and interesting applications. Android registers for the reception of system wide events to kick off their activation. Among all the events BOOT_COMPLETED is the most popular. This event is triggered when the system has completed its boot process. The second most widely used event is SMS_RECEIVED. Another popular event used by mobile malware is ACTION_MAIN to hijack the entry activity. This event is triggered once the user presses the application icon to launch it. Naturally many malwares would be interested to do some pre launching events before the application starts its activity. Another feature used by author to characterize the malware is the carried payload. One type of payload is privilege escalation exploits. Due to complexity of Android framework, there may exist many a vulnerabilities which are exploited by exploit writers merely for raising the privileges of the application. Among different types, payload remote control that turned mobile phone into botnet was the most common. Almost 93% of all malware under consideration used this type of payload. Payloads used for financial benefits and information collection are also very common.

Adrienne [10] investigated 46 pieces of malware for different mobile OSs and investigated behavior of current malware and incentives behind malware development.

The author also evaluated the effectiveness of different security features present on the mobile platform. The author categorized malware in three different types namely malware, spyware and grayware. Grayware are the legal and benign application but with some data collection functionality that may offend the users. The main thrust of iOS in fight against malware is the review process of the application before making it part of Apple Store. In case of Android focus lies mainly on the permission model to assist users from installing malicious application. That is why Android permission model is more comprehensive than iOS. The main incentives behind mobile malware development are selling of user information, stealing of user credentials, premium rate call and SMS, SMS spam, search engine optimization, ransom, invasive advertisement, weapon of monitoring and spying for governments, DDOS, NFC and credit card frauds. The author proposed permission anomaly analysis for classification of malicious applications. In addition application may not request special permissions to execute their malicious functionality rather a root exploit can effectively raise the privileges of the application to bypass restrictions imposed by Android framework. Root exploits for any version of Android is available within 5.2 days of the release of that version.

3.6 Detection of Mobile Malware

Detection techniques are generally categorized in static and dynamic detection. In this section, malware detection techniques which have been suggested by different researchers will be presented. These techniques have been selected basing on the most common threat vectors being employed by attackers.

3.6.1 Static Detection Techniques

This is the malware analysis technique where malware is analyzed without executing the code. The most basic type of static detection is to study the source code and try to analyze its scope and objectives. The advantage of this technique is that it can uncover those behavior patterns of the malware which are near impossible to uncover through dynamic analysis. The common tools used for static analysis are disassemblers, decompilers and source code analyzers.

3.6.2 Repackaged Application Detection

Repackaged applications constitute 90% of all malicious applications. Repackaging involves getting popular applications from official Android market,

inserting malicious code and finally publishing them on third party application market. Zhou [11] devised a mechanism to detect repackaged applications in third party Android market places. The mechanism is based on measuring the similarity between two applications through DroidMOSS system. First step was to create finger prints of large number of applications present on the Android market. Fuzzy hashing was performed on the applications for fingerprint creation. Normal hashing was not useful in present scenario since a change of single character could change the hash of an application to a totally different value. Finger print creation is a two stage process. First step is the feature extraction under which instruction and author information will be extracted from application after disassembling .dex file. Second step involves the finger print creation using the extracted information of first phase. DroidMOSS creates the signatures by dividing the application instruction in small groups. Hash is calculated on each group of instructions and contributes to the overall hash of the application. If repackaging inserts some instructions in certain piece, hash of only that piece would be affected thus effectively localizing the change. The similarity between fingerprints would then be measured for categorizing the application as repackaged or benign.

3.6.3 Over Privileged Application Detection

Android application framework security is crucially dependent on the privileges granted to an application. Due to lack of proper Android API per-mission documentation and poor understanding of permission system by application developers a large number of applications requests permissions that are not required by them in order to function correctly. An over privileged Android application can be exploited by an attacker to gain restricted privileges. Malicious code inserted by an attacker in an over privileged application will have the same level of access and privileges as that of compromised application.

In one of the effort [14] the author tried to build a permission map necessary for detecting over privileged applications with the help of automated tools and then judged around 940 applications on the basis of this permission map. He concluded that almost one third of judged applications were over privileged. Author utilizes the Android API framework for finding the permissions associated with the system API. The Android API consists of two parts. One is that runs in the virtual machine instance of the application. The other is the actual implementation that runs as a part

of system process. The virtual machine part of API is RPC stub. This stub requests the system process to deliver the services requested by the RPC stub. The java reflection has been used to access all the private and public classes, methods and properties. After listing the methods, all these methods were tried to be invoked by using all possible inputs from the input pool. This technique explored the permissions associated with all the invoked methods. In the second step all the detected methods along with their permissions also underwent the manual verification.

The Android API consists of 1665 classes with 16732 public and private methods. With the technique adopted by the author he was able to cover 85% of the API. This knowledge is then used by a tool, Stowaway to find the over privileged applications

3.6.4 Content Provider Vulnerabilities Detection

In the first technique discussed under static detection, application as whole was analyzed and checked whether it is repackaged or not. Second technique narrow down the focus to the privileges granted to the application which are over and above the required level. In third detection method we further go down and focus on one component of the application i.e. Content Provider. A Content provider is an application component that is meant to maintain application specific data using SQLite database. As was discussed previously in section II-E, a component can be public or private. Content providers are by default public unless otherwise configured.

Yajin [16] tried to analyze two application vulnerabilities with regards to content providers. One is content leak and the other is content pollution. When content provider is public and custom permissions created on it are normal, it is very likely that another application installed on same mobile may be able to access data like SMS messages, browser history. This is called content leak. Content pollution is the ability of an application to change the data present in the content provider. The author first short listed the application from the Android Google Play by inspecting the manifest file of applications. All applications where exported attribute of content provider is true and custom permission level is normal are selected for further analysis. Function call graph of selected applications were built from start function to terminal functions. Start functions are the interface functions of the content provider while terminal functions are all those functions which implements insert(), query() and

openFile() API of SQLite database. After the construction of all paths from start to query functions, necessary inputs are generated. These inputs are generated by constraint resolver after satisfying all constraints which arise due to CFG and data flow analysis. These inputs were used to check reach ability from start to the end functions. Where there was a path from start function to end function due to some particular input, it was characterized as malicious. After analysis there were 2.0% applications which suffered from these two vulnerabilities.

3.7 Dynamic Detection Techniques

The most common form of dynamic detection is the behavior analysis. Static detection, owing to its effort and time consuming nature is not very practical for analysis of large applications. Dynamic analysis techniques are characterized by observing the run time behavior of the application. The disadvantage of this technique is that it may not be able to explore the complete behavior of the application. Tools for performance of this technique includes debuggers, function call tracers, machine emulators, logic analyzers and network sniffers.

3.7.1 Remote Detection

Smart phones are characterized by their low processing power, low memory and energy restraints. Malware detection algorithms are often very processing intensive and consumes large amount of platform energy. The malware detection techniques that can be effectively employed on a desktop PCs may notfit into the constraints offered by mobile platform owing to the reasons defined previously. There have been ideas to detect mobile malwares away from mobile platform on remote servers.

One such approach was discussed by Mark Guido [13]. The researcher has proposed an approach to detect malicious applications of the Android mobile phones remotely. The major constraint of his work is that this approach can only be applied on those mobiles which are associated with the enterprise. The idea is to move computation intensive malware detecting operation away from the mobile device to the remote server. In this approach, the only application installed on mobile phone would be a service that would take note of changed bit stream from the previous scan and send them to remote server via Wi-Fi for analysis purpose. Prerequisite would be that the server is provided with the complete image of all the applications running on the

mobile phone in advance. When server will receive the changed bit stream along with the start and end offsets, it would replace the received bit stream at the reported offsets and complete the image for analysis purpose. The image would then be compared with the base image already held with the server for detecting malicious artifacts. The main components of this framework would be tractor beam, which is a mobile side daemon that would be started with init to have proper privileges, the enterprise server that would be running analysis plus detection framework and database that would store sent updates at server end.

The limitation of this work was the compulsion of mobile to be part of some enterprise network. Although theoretically it may seem to be an effective system but practically this is in contrast to the very basic fundamental of mobile computing i.e. the mobility.

3.7.2 System Call Centric Detection

Behavior Analysis has always been the corner stone for detecting malicious behavior. There have been much work in this area of research. In one of the work Alessandro Reina [9] has evolved a system that analyzes the behavior of underlying Linux kernel through system call monitoring approach and Android framework through Binder analysis. Android emulator *CopperDroid* was built to support malware behavior analysis through binder analysis. This emulator executes on QEMU hypervisor. VMI introspection was used for the monitoring of system calls. ARM architecture uses swi instruction to switch from user mode to kernel mode for implementing system calls. QEMU was modified to track system calls by intercepting swi instruction. Android framework is dependent on IPC and RPC mechanism for inter process communication. Android implements binder protocol for communication to services. Binder mechanism is implemented through AIDL files. Stub of AIDL is extended by callee to implement the services where as the proxy classes are used by caller to call the remote object methods. The communication that takes over this channel is mainly used for the discovery of behavior of malware on Android framework. BINDERWRITEREAD ioctls used by the binder implementation are of main interest to behavior analysis since it is used for the transfer of data between the processes. CopperDroid focuses on transactions for the behavior discovery. It dynamically parses all the structured data and retrieves all transaction related information. For discovery of all possible behavior of a

malware CopperDroid provides stimulus to the malware artificially with number of events.

3.8 NFC Devices and Applications

NFC encompasses smartphones which can act as reader as well as writer. Other devices include the NFC based smart tags and NFC reader terminals. NFC tags are passive devices which are activated by the NFC reader terminals. NFC tags are basically RFID chips [24]. Contactless smart cards may store additional data in a secure manner. Security is required when these cards/ tags are used in ticketing and payments today may include additional technology for storing secure data.

Apart from the smartphones, other NFC enabled devices are also available in the market to perform electronic transactions. Point of sale (POS) terminals are used for operations related to contactless payments. The most important applications of NFC are [25]:

- E-commerce; for payments involving contactless cards and devices
- Trivial data sharing over smaller distances; android beam is a typical application of the same.
- Identification tokens; NFC tags and devices can be identified on the basis of unique identifiers.
- Reading tags; NFC tags are replacing QR codes to share identification data or even web URLs/ addresses.
- Writing tags; custom NFC tags can be written as per user requirements.
- Bluetooth and WiFi connection management and initial parameters through NFC for subsequent data transfers. Bluetooth and Wifi both have higher data transfer rates [26]. Figure: 3.2 depicts typical data transfer and effective distances of various wireless technologies.

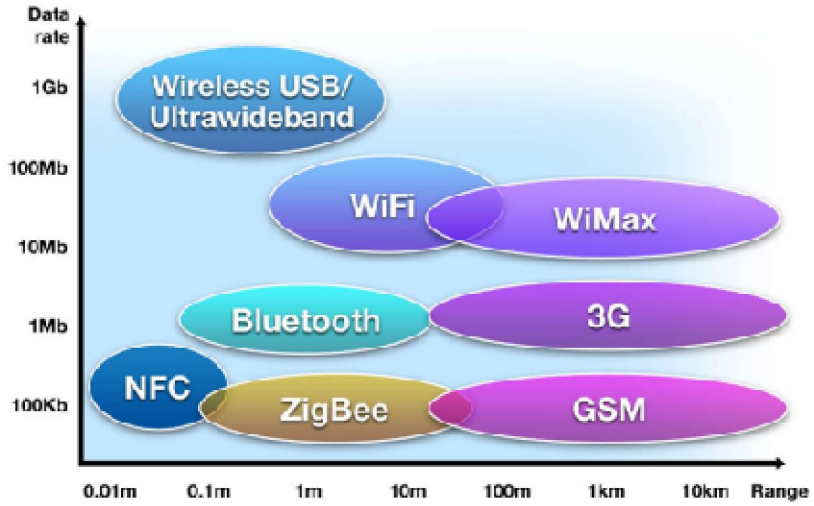

Figure 3.2: NFC and other Contactless Technologies

3.9 Operating Principle

NFC devices can be divided into two main classes like RFID devices. A device capable of generating a magnetic field and generate its identification using its integral power source is an active device. Whereas a passive device is dependent on other devices to generate RF field to energize their internal circuit. The RF field generates enough power to activate the passive NFC/ RFID device. Almost all of the NFC tags are passive devices which are dependent on RF energy to energize their internal circuit. Smartphones capable of NFC can act as active and passive on either requirement.

NFC interface can act as an initiator as well as a target device. Initiator device acts as the master device and starts the communication. The target device, also known as slave device responds to the requests initiated by the master device [27].

3.9.1 Modes of Operation

An active mode of communication involves two active devices and passive mode involves an active and a passive device communicating with each other. No communication is possible between two passive devices [27].

3.9.1.1 Active Mode

The initiator device generates RF to induce voltage in the antenna loop of the respondent device by activating its transmitter. The target device on detection of the RF

induced voltage, acts as slave/ target device and responds to the requests initiated by the initiator device. The slave device responds to the initiator by generating its own RF and transfer the response to the initiator. Both devices alternatively act as initiator as well as target to send and receive data to each other [27].

3.9.1.2 Passive Mode

Like passive RFID tags described in chapter 2, the target is activated by high frequency RF generated by the initiator to send and receive data to and from the target device. Initiator transfers the data by modulating the signal amplitude. After transmission of initial data request, the initiator keeps the RF signal emission on but in an un-modulated mode [26]. The target responds by generating load modulation.

3.10 General Architecture of NFC Enabled Device

This section describes hardware components of NFC devices and their working mechanism to communicate with smartphones etc. Books [24] and [27] have been referenced to compile this section of the thesis.

3.10.1 NFC Interface

NFC interface communicates directly with other NFC/ RFID devices using short range wireless communication. NFC interface can act as RFID reader and RFID transponder to transfer data. The interface has a controller and an antenna to carryout NFC. The controller interface is based on analogue RF interface to transmit and receive data signals. Card emulation mode is achieved by RF interface which has a load modulator. It generates responses to active NFC devices by generating modulated loads.

A contactless UART (Universal Asynchronous Receiver Transmitter) encodes and decodes data into corresponding signal forms required for the transmission. A microprocessor is the core of the controller which processes the messages as per the protocol. The controller connects the host controller with the secure element using multiple interfaces. The connection can be through SWP (Single Wire Protocol) and NFC-WI interfaces. Figure 3.3 illustrates basic components and block layout of NXP PN544 NFC controller [28].

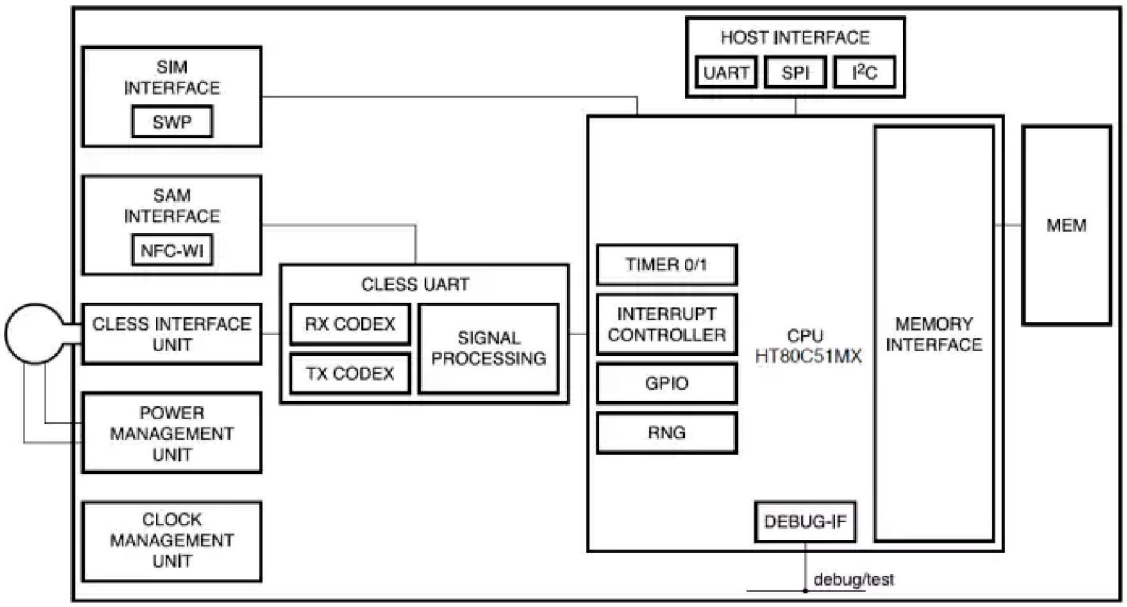

Figure 3.3: NXP PN544 Controller Block Diagram

3.10.2 Secure Element (SE)

Security is a major concern in many NFC applications which involve transaction of money like payment and ticketing applications. The secure element provides secure storage and safe execution environment to the critical applications. SE typically have MULTOS (Multi Application Card Operating System) or Java Card OS. The applications are in the form of small java applets. SE is a hardware module with software in the form of OS on it. SE is available in the form of [27]:

- Embedded hardware
- UICC (Universal integrated circuit card)
- Secure memory card (SMC)

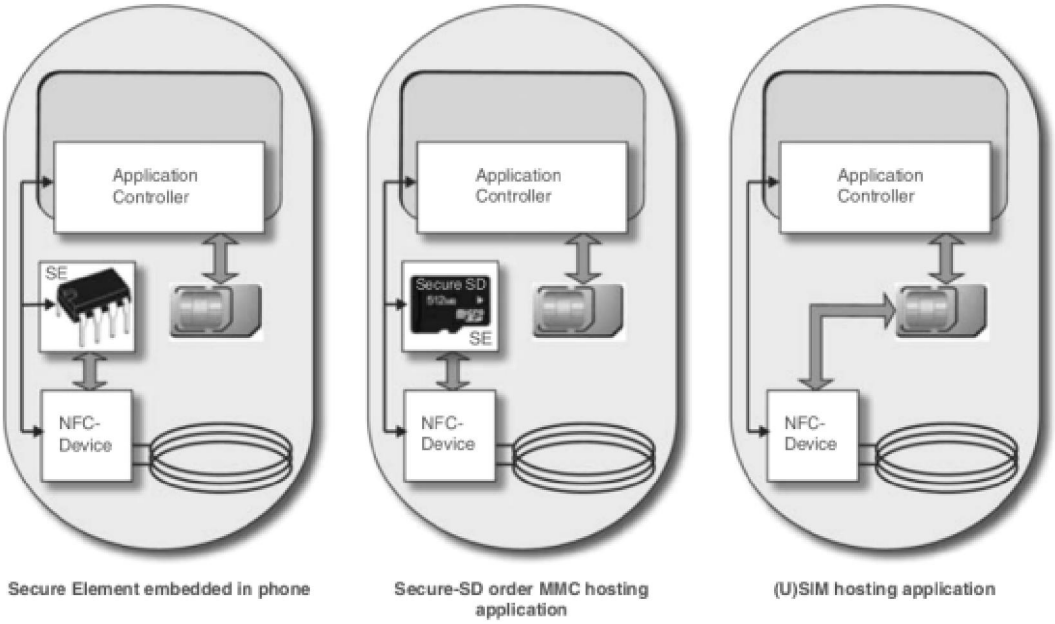

Figure 3.4: SE Options in Smartphones

3.10.3 Application Management on SE

Brief description of Application management on SE has been covered here. It is a very complex task. Protocols developed for smart cards apply to SE also because it is basically a smart card [29]. The native OS of the device hosts the SE which has an operating system. Multiple applications in the form of applets run in this operating system in a virtual machine.

JavaCard OS is the most commonly used OS in SE. A separate framework developed for application s executing on SE has been developed. This framework is called Java Card runtime environment (JCRE). JCRE supports Java language applications developed for the framework. Java Card virtual machine, API classes and supported service are the main components of JCRE.

Global Platform developed Global Platform Card Specification (GPCS) which define loading, initialization and deletion of applets on the smart card [30]. A unified card management standard which is independent of the card make, type and internal architecture has been specified. Global Platform compliant cards have essential components like an Issuer Security Domain, mostly known as Card manager. The Card manager is an application which provides necessary interface for addition or removal of

applications on the card. It manages application life cycle. Card manager keys are used to authenticate the management operations as the use of SE can be critical when it hosts payment applications. The authentication keys provided by a card issuer are saved in the SE. The keys are not available to the host operating system like Android. So operating system vulnerabilities do not affect security of these keys. Secure communication protocols haven specified by GPCS. These protocols ensure that communication with the card is confidential and message integrity is maintained [31]. Detailed and extensive specifications have been provided by Global Platform Card to secure every aspect of the application running on SE [30].

3.11 NFC - Standards and Protocols

3.11.1 Base Standards

Basic NFC specification protocols used in different hardware can be one or combination of more than one. Following basic protocols are specified [32]:-

- **ISO/IEC 18902 or ECMA-340 (NFCIP-1)**: NFCIP stands for Near Field Communication interface and protocol. This standard specifies communication between two NFC devices using over physical layer.

- **ISO/IEC 21481 or ECMA 352 (NFCIP-2)**: Communication mode selection mechanism for communication between different contactless technologies that operate on the 13.56 Mhz frequency.

- **ISO/IEC 14443 (Proximity-Coupling Smart Cards)**: This standard describes communication between card and the reader device. It covers transmission protocols, methods of operation and proximity cards with communication range of 7-15 cm [27].

- **ISO/IEC 15693 (Vicinity-Coupling Smart Cards)**: Vicinity-coupling smart cards functioning and operations are defined by this standard. Vicinity cards can be read from the greater distance (up to 1-1.5m) than proximity cards [27].

3.11.2 High Level NFC Standards

It is a group of standards specified by NFC Forum organization. These standards are built using ISO/IEC standards [1]. These standards provide detailed functionality and new possible methods of operation.

- **NDEF**: NFC Data Exchange Format defines a data format between NFC tags and NFC enabled devices.
- **RTD**: Record Type Definition defines the types of record in various NDEF messages.
- **Connection Handover:** It defines the protocols and procedure to establish a connection between NFC and other wireless technologies like Bluetooth and WiFi.
- **LLCP**: Logical Link Control Protocol is used to support pier to pier communication between two devices, used on top of NFCIP-1.
- **Digital Protocol**: It provides an implementation specification on top of the ISO/IEC 18092 and ISO/IEC 14443 standards.
- **SNEP**: Simple NDEF Exchange Protocol is used on the top of LLCP to allow exchange of NDEF messages.

3.12 NFC Forum Tags Specifications

NFC Forum has specified four types of tags which can be used with NFC-enabled devices. Each tag has different technology [2]. The tag types are as following

- **Type 1 Tag**: Type 1 tag is based on the ISO/IEC 14443 Type A standard. These tags are readable as well as writable. Tag can be configured by users to become read-only. Small memory, only 96 bytes, is available which can be expanded up to 2 kB. Due to limited memory capacity it can be used to store short text like URLs.
- **Type 2 Tag**: It is based on the ISO/IEC 14443 Type A standard. Tags are both readable and writable and can be configured to be read-only. Default memory

capacity is 48 bytes expandable to 2 kB.

- **Type 3 Tag**: These tags are based on JIS X 6319-4, also known as FeliCa. Memory size of these tags is variable, 1 MB per service (multiple services can be run on these tags). These tags have been designed so as to support complex applications. These are expensive than other types of tags.

- **Type 4 Tag**: Type 4 tags are fully compatible with the ISO/IEC 14443 standard. These tags have Type A or Type B compliant communication interface. Read and re-writable, or read-only mode is preconfigured on these tags. Up to 32 kB of memory is available per service.

CHAPTER 4: POLICIES, REGULATIONS AND LAWS

4.1 Introduction

Most of the policies regarding use of electronic devices originate from the US departments. Here we list some of the regulations and guidelines available in NIST documentations. Initial part of the chapter enumerates requirements related to use of RFID based technology in US. Guidelines for Securing Radio Frequency Identification, NIST publication number SP800-98 [18] has been consulted for first part of this chapter.

Subsequent parts cover various cyber/ electronic security laws of Pakistan published from time to time. Around the globe, about forty nations reacted to the need of creation or improvement in the laws and legislation related to information technology by extensively ordering devoted efforts to establish laws. These laws and regulations generally cover following aspects:

- Existing laws and their derivation to suite the information technology regime.
- Revisions in the existing laws so as to cover the technology where gaps were observed.
- Recognizing the requirement for specialized learning and capacity enhancement of the personnel who deal with the laws to enable them to understand legal requirements in the field of information technology.
- Legal advices for all electronic transactions and records.
- Legal and official identification of different forensic tools and technological equipment required for assessment of information technology breaches of laws.
- Declaration of acts which are criminal in nature and are derived from use of information technology apparatus or internet.

4.2 Privacy Requirements for US Federal Agencies

The section deals and lists various guidelines and instructions for the federal agencies of the USA. Being particular to US agencies the statutes have not been discussed in this review. List of these policy guidelines are:

- Privacy Act of 1974
- E-Government Act of 2002
- Consolidated Appropriations Act of 2005
- Federal Information Security Management Act (FISMA)
- Federal Chief Information Officers (CIO) Council Privacy Control Families.

4.2.1 Privacy Act of 1974

The provisions of the Privacy Act are used for the compilation, use, preservation and distribution of personal data and information of U.S. people or foreigners who are legal immigrants for permanent residence. This Act concerns with the data maintained by executive branch through the records relevant to government departments. It is concerned with the files to provide information which:

- Contain names of individuals and social security number along with an additional piece of information like birth date, and
- These can be recovered by person's name and Social Security number or PIN.

4.2.2 E-Government Act of 2002

It contains several information types which can be related to RFID technology such as:

- Impact assessment on privacy be performed.
- Compliance with the requirements of the tracking technologies used in web pages.
- Development and implementation of planned policy for machine readable privacies.

4.2.3 Federal Information Security Management Act (FISMA)

FISMA offers a framework for the administration of information security at federal level. It includes steps to protect information by establishing controls required at different levels.

4.2.4 Consolidated Appropriations Act of 2005

The rules which apply to privacy issues related with the Departments of Treasury and Transportation and Independent Agencies. The requirements of the act want that:-

- The technologies used should not reveal private information while storage and use of the data.
- Compliance to the auditing procedures and rules.
- Compliance to Privacy Act of 1974 for fair information practices as defined in the law.
- Evaluate legislation related to privacy and offer suggestions.
- The proposed rules of a department be tested against privacy impact assessment.
- Annual report on the issues affecting privacy be submitted to Congress.
- Protection of information of the department against possible disclosure, alteration and destruction.
- Training and education of the employees.
- Establishment of policies and procedure related to data privacy and protection.
- Compliance with the department policies related to privacy.
- Written report in consultation with the Inspector General of each agency about its practices for security of information and privacy.
- Ensure compliance of internal audit procedures by the agencies.

4.2.5 Federal Chief Information Officers (CIO) Council Privacy Control Families

It may be necessary to organize the implementation of privacy controls to fulfill and abide by the federal laws and regulations. The implementation of RFID system and controls will differ in different business implementations supported by RFID systems. An RFID technology which delivers health care will be considerably different to support transportation projects and will contain different privacy controls.

4.3 Cyber/ Electronic Security Laws of Pakistan

4.3.1 The Electronic Transaction Ordinance - 2002

The Electronic Transaction Ordinance, 2002 [19] was published in the gazette on September 11, 2002. General summary of the sections of the ordinance is as following:

- Section 2: This section contains definitions of the terms used in the ordinance.
- Section 3: Electronic forms and their legal value has been acknowledged and recognized.
- Sections 4, 5 and 6:These sections deal with the use of electronic media.
- Section 9: This section defines offences related to electric signatures.
- Sections 13, 14, 15 and 16: These sections describe and explain legal value of electronic documents.
- Section 18: This section contains instructions for government to form and establish a council which would be responsible for certification related issues.
- Sections 19, 20 and 21: These sections contain guidelines for the selection of members for the certification council. It even defines the requirement of qualification and procedure for selection. The council thus formed will be responsible for issuance rights to certification service providers.
- Section 32: It deals with the crimes or incidents which are done outside Pakistan.
- Sections 34, 35, 36 and 37: Offences are enlisted.
- Section 38: Punishment for the offences is described in this section. Further details of the offences which are non-bailable or of grave nature are described.
- Section 39:This section describes that at least a Session Court will try an offence under this ordinance.

4.3.2 Prevention of Electronic Crimes Ordinance – 2007

This ordinance [20] provides procedures and guidelines for investigation, case prosecution and offences which can be tried. Summarized chapters are as following;

- Chapter I: It covers the general terms, definitions and the authority of this ordinance.
- Chapter II: It contains details about Offences and Punishments

- Chapter III: This chapter contains information about prosecution and trial of offences.
- Chapter IV: This chapter describes the powers of the investigating officers and detailed procedures for establishment of investigation and different prosecution agencies which are authorized to carryout necessary actions for investigation.
- Chapter V: This chapter defines the rules and guidelines for the government to establish contact with international organizations, agencies or other governments where deemed necessary.
- Chapter VI: This chapter describes and provides guidelines for establishment of information and communication technologies tribunals.
- Chapter VII: This chapter contains miscellaneous provisions like; Ordinance to override other rules, power to amend rules, power to make rules and removal of difficulties.

4.3.3 Payment Systems and Electronic Fund Transfers Act, 2007 (State Bank of Pakistan)

This Act [21] provides procedures and guidelines involved in carrying out financial transactions. It provides description of all possible types of payment scenarios and the legal restrictions involved in it. Summary of chapters is as following;

- Chapter I: This chapter is the preliminary and contains definitions and jurisdiction and powers of the State Bank as provided by this act.
- Chapter II: This chapter contains definition and explanation of payment systems and their designation, revocation status, gross settlement system, electronic record retention guidelines and operational arrangements.
- Chapter III: This chapter defines different payment instruments and rules related with their issuance and discontinuation.
- Chapter IV: This chapter contains information regarding clearing houses, audit and inspection rules.
- Chapter V: This chapter deals with the supervisory role and powers of state bank.
- Chapter VI: This chapter rules regarding documentation of transfers.
- Chapter VII: This chapter describes various types of errors and their notifications.

- Chapter VIII: This chapter lists rules related to liabilities to parties, burden of proof, force majeure, intent, exceptions and waiver of rights.
- Chapter IX: This chapter describes the legal outcomes of the actions performed in front of the court and violations affecting electronic commerce. It also provides explanation if someone cheats by use of electronic device.
- Chapter X: This chapter contains miscellaneous rules regarding electronic acts and crimes. It also describes the implication of these rules for the employees of the state bank.

4.3.4 Prevention of Electronic Crime Act-2015

Prevention of Electronic Crime Act-2015 [22] lists offences and punishments in details. The act contains scenarios with examples for assimilation of general public as the acts pertaining to electronic crimes become ambiguous and confusing. List of offences is as:

- **Illegal access to information system;** the offence is liable for a period of six months imprisonment and one hundred thousand rupees as fine or both at the same time as per the gravity of the offence.
- **Illegal access to program or data**; the offence is liable for a period of nine months imprisonment and two hundred thousand rupees as fine or both at the same time as per the gravity of the offence.
- **Illegal interference with program or data**; the offence is liable for a period of three years imprisonment and five hundred thousand rupees as fine or both at the same time as per the gravity of the offence.
- **Illegal interference with information system**; the offence is liable for a period of three years imprisonment and five hundred thousand rupees as fine or both at the same time as per the gravity of the offence.
- **Cyber Terrorism**; Unauthorized act in relation to information system, circumventing or infringing security measures with respect to an information system and act against government controlled critical information system is liable to be tried under Cyber Terrorism Act which is punishable with imprisonment of fourteen years or/and fifty million rupees fine.
- **Electronic Forgery**; the crime is punishable with imprisonment up to two years or/and a fine of two hundred and fifty thousand rupees.

- **Electronic Fraud**; the crime is punishable with imprisonment up to five years or/and a fine of ten million rupees but not less the extent of the damage caused.
- **Making, supplying or obtaining devices for use in offence**; the crime is punishable with imprisonment up to one year or/and a fine of one hundred thousand rupees.
- **Identity Crime**; the crime is punishable with imprisonment up to six months or/and a fine of one hundred thousand rupees.
- **Unauthorized Interception**
- **Special protection of women**

4.3.5 Prevention of Electronic Crime Act-2016

Prevention of Electronic Crime Act-2016[23] contains the majority of rules from Prevention of Electronic Crime Act-2015 with some additions. The additional crimes are as under:

- Hate Speech
- Recruitment, Funding and planning of Terrorism
- Unauthorized issuance of SIM cards
- Offences against dignity of a natural person
- Offences against modesty of a natural person and minor
- Child pornography
- Cyber stalking
- Spamming
- Spoofing

CHAPTER 5: NFC BASED TRANSACTIONS, COMMUNICATION AND APPLICATIONS

5.1 Introduction

In recent years, our wallets have slowly been growing thicker by number of electronic cards that we have to carry around with us. Such an electronic card typically serves one or very few purposes only. We have a card as a key to our office, a card as a bank card, another bank card from our second bank, a student card, an ID as well as several discount cards (one discount card per one shop, in the worst case). Basically, each institution we are involved in provides us, with high probability, with another contact or contactless card.

The main goal of this chapter is to explore if and to what extent it is possible to implement a given payment protocol in a mobile phone equipped with NFC. The payment protocol we talk about is a new protocol, designed mainly for use on contactless smart cards (meaning that customer's device is the smart card). The protocol description is given later in this chapter. We focus on mobile phones with Android operating system, since it is the most widespread OS used in smart-phones today.

5.2 Smartphones as Alternative to Plastic Contactless Cards

One idea that may help to reduce the number of contactless cards is to use another electronic device that we carry with us every day - a mobile phone. Mobile phones have already become more than just devices for making calls and sending messages. Today, they are commonly well equipped and equal in power to personal computers being widespread only few years ago. They offer many different connectivity options, the one we want to talk about is the near field communication (NFC). The key thing that NFC allows is to communicate in the same way as contactless cards do. With a special chip inside the phone called secure element, the phone offers the same functionality as a contactless card. This is one of the main objectives of NFC in mobile phones. We might one day, eventually, replace all our contactless cards with a single NFC phone, containing all those cards under one hood. A user will be able to select the card he would like to use and then just tap his phone to the reader.

Innovation in NFC tools is being incorporated into bank cards, cell phones and point of sale terminals, all together towards quick execution of payment exchanges with no physical contact. EMV is the standard planned to operate both contact based (traditional) and contactless-NFC payments securely. As of late some security vulnerabilities in this EMV convention have been reported by researchers. We present the dangers and risks involved in application of EMV protocol due to the vulnerabilities and especially those in question on account payment transactions using NFC. Consequently, so as to overcome EMV shortcomings, we propose a security convention where an online correspondence and verification system is used for establishment of trust. The proposition is bound to secure NFC payment utilizing bank cards that use NFC technology.

We will scrutinize practical resolutions for realization of the specified payment procedure on the NFC based smart-phone containing Android operating system. Significant part of this chapter is the explanation of mobile payment system.

5.3 Mobile Transaction Security Requirements

In any payment systems, following transaction security properties must be satisfied:-

- **Authentication of Stakeholders**: The parties engaged in the transaction carried out using payment system must be able to authenticate other parties and system involved. It may include the communication system as well.
- **Privacy of Transactions**: Only intended parties should have visibility of the transactions and these should not be revealed to any third party. Transactional messages should be received only by the parties engaged in the transaction.
- **Integrity of Transactions**: Mechanism to ensure that integrity of messages generated and received by the parties is ensured. Alteration of messages during transmission can be checked and verified by the recipients.
- **Non-repudiation of Transactions**: The party engaged in the transaction cannot deny the performance of transactions.
- **Accountability**: E-commerce activities involve funds transfer and goods exchange between the participating parties in a payment system. The parties engaged in a transaction must produce and prove the transaction messages being

sent as originator or recipient. The accountability covers validity of above listed all security properties.

5.4 General Implementation of NFC at Point of Sale (POS)

NFC-enabled smartphones will change and improve the transactional experience at point of sale terminals at various businesses. Mobile payments, mobile based ticketing, on-site payment, mutual funds transfer and an unlimited list of loyalty programs will be enabled by use of NFC technology. It will change the way we live, work and pay in our daily lives.

Pre-requisites of NFC payments at any point of sale include:-

- NFC-capable POS device; and
- an NFC-equipped phone running a payment application.

Here are the basic steps to establish payment through an NFC based payment system:-

- A customer sets up his or her smartcard credentials and subscriptions in the application running on an NFC enabled smartphone.
- A consumer can enable a smartcard on previously held or newly bought smartphone in one of the following two ways:
  - Smartcard credentials for payment are stored in SIM/ internal storage of phone using cryptographic aids.
  - A payment application authorized by a bank or published by a phone manufacturer is enabled in the smartphone to use Host Card Emulation.
- Customer makes payment by tapping his/her NFC enabled smartphone on an NFC-capable POS device through NFC.
- The payment transaction is routed through the goods vendor, an acquirer, a smartcard issuer (bank/ loyalty company) and a service provider who may be authorized to provide loyalty rewards, commission and/ or discounts.

5.5 Proposed Payment System

The payment system has five elementary characters: Customer, Vendor, Issuer, Acquirer and Broker. The current description has a unique broker, quantity of vendors, customer, issuer and acquirer can be more than one and is unlimited. Broker has

established trust with all other entities participating in the arrangement of the payment scheme being used in the system. The system has the capability to process payment transfer requests from one to another user of the system. Usually the customer transfers money to the vendor through trust relationship established by the broker. The customer can process the payment transaction through his contactless smart card or NFC enabled smartphone. The smart card/ smartphone with NFC application is authenticated and registered by the broker. The vendor offers services and goods to the customer and charges the customer using a terminal device. Broker is responsible for transfer of payment from customer account maintained by issuer to the broker account maintained by acquirer. The payment is like payment through electronic cheque being offered to the vendor in return for his services and goods. Authenticity of the electronic cheques is carried out by the broker who performs digital signatures verification of the customer and the electronic cheque being offered. The service can be availed by credit/ debit card or smartphone with user credentials/ data.

5.5.1 Customer

A customer in this arrangement is considered a payment device which can be an active device (smartphone) with its integral battery source or can be a passive device (smart card) which is activated by the magnetic field generated by the terminal device held by the vendor. The computation capability of the customer device is very limited where it can perform basic operations required by the payment system. A smart card has very limited storage and computation capability. The same is considered for a smartphone although it can perform very complex calculations. Communication between the customer device and vendor terminal is through wireless/ contactless medium. Number of customers is not limited and has many interfaces and device types. A customer requests to purchase goods or services from a vendor who is offering these to all customers.

5.5.2 Vendor

The vendor is a terminal capable of reading customer credentials and exchange of instructions and data with the broker. Number of vendor devices can be one or many. Vendor communicates with the customer through contactless/ wireless arrangement. Connectivity of vendor with the broker is not necessary. The vendor-broker communication can transfer required data at any time before or after transactions.

5.5.3 Issuer

An issuer is the financial institution/ guarantor of a customer. It has an account associated with a customer. It manages customer's account and all funds transactions authorized by the customer.

5.5.4 Acquirer

An acquirer is the financial institution of a vendor. It manages vendors account including various fund transfers which are authorized by the vendor.

5.5.5 Broker

The broker does not actively participate in purchase of goods/ services. It is an entity in the system which is located on a central server. It acts as a payment gateway between Customer, Vendor, Issuer and Acquirer. It is connected with the Customer and vendor through a public network/ internet. Issuer and Acquirer are connected with the broker through a network which may be a private banking network.

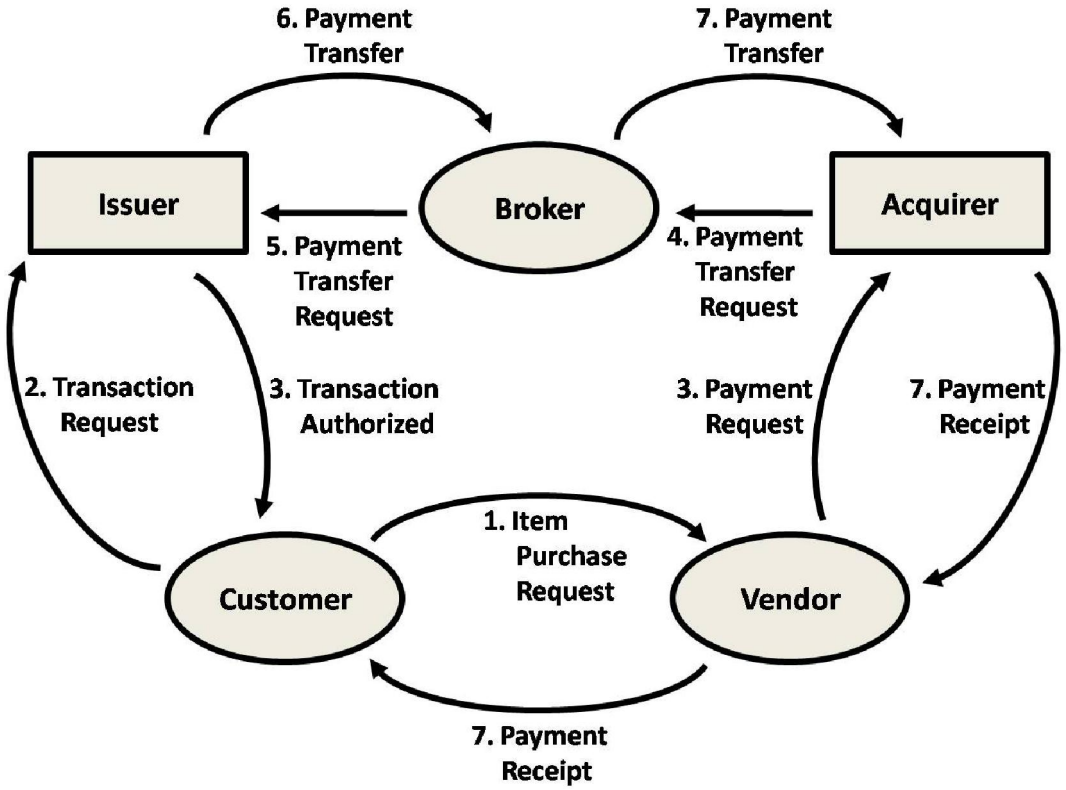

Figure 5.1: Payment Process

5.5.6 Other Operations

Other parts involving various operations in the payment may include the updates regarding customer registration with the broker, account balance sheet update operations and transfer of payments from the client device to the vendor through broker. It may also have other banking operations like data synchronization between the device and broker, settlement of payments and revocation lists. These operations are not discussed here.

5.6 Safety Measures for Making Secure Transactions

In comparison to desktop computers and laptops, smartphones have only been with us in last five years or so but these devices have gained popularity due to their portable nature.

Mobile payment systems are emerging and smartphones are active candidate to replace other devices presently being used for financial transactions to purchase goods and services. While carrying out financial transactions over smartphones we have to be cautious to save us from fraudulent software applications and other security risks. Smartphones due to their mass adaptation and utility are target of hackers. These devices may become less secure at times due to the software applications running on them.

Mobile phones have gained attention of security researchers due to which security of mobile phones has improved manifolds. Improvements in the security domain of smartphones has gained tremendous momentum as more dependency on practical utility of smartphones has been felt.

5.6.1 Trustworthy Apps Download Sources

Applications downloaded from sources other than official App Store are very risky. 3rd party application available on multiple sources is an extremely unsafe choice. Android Play Store provides authentic applications which are checked by different analysis tools before uploading for customers.

Best approach for a common user who is more conscious about security of smartphone is to restrict download of applications from the official app store and further developed by the authentic software company.

It is recommended that a payment application should preferably be downloaded from App Store which is a native application. Native applications are tested to be more secure as these are developed the same team which develops the operating system.

5.6.2 App Reviews

It is highly recommended that before downloading any applications from official App Store or other app sources, a user must go through the reviews provided by other users who downloaded and installed the same app earlier. The user reviews provide visibility about application performance and usability.

App ratings available on the official source locations provide choice to customer where they can opt for an App providing same functionality but having better user feedback in the form App rating.

5.6.3 Password/ Biometric Authentication on Mobile Devices

Passwords provide privacy protection and security of data available on smartphones. Setting up and using passwords to unlock and use smartphones may be nuisance for some people. Leaving smartphone without a lock protection is not advisable at all. Newer hardware of smartphones come with embedded biometric readers which can be used to secure mobile phones.

Unprotected smartphone can provide access to all applications installed on it. The applications range from simple calling/ sms application to banking application. The passwords and/ or biometric authentication provide basic phone security to advanced application security. Individual applications can also be locked to further enhance the security.

We carry mobile phone with us everywhere, chance of misplacing or losing a phone is more likely. In such case, an unsecured phone will compromise private and confidential data.

5.6.4 Data Transmission Over Secure Internet Connection

Public Wi-Fi networks are susceptible to data stealth as the communication medium between the mobile and the internet terminal device is not secure. To use a payment

transaction application, one must ensure that the internet link which he/ she is using has requisite security.

5.6.5 HTTPS Websites

There are always situations when a user has to use web explorer to access certain websites. One must be cautious to and must look for the website address bar to ensure that the link address is using HTTPS instead of HTTP protocol. Information shared over HTTP websites is not secure and may jeopardize the security and leakage of sensitive information.

Data transferred using secure HTTPS connection ensures that the information passed between the server and the end user device is shared between the two intended machines only. One must check for the padlock icon on the website address bar before sharing sensitive credit card or bank account information.

Applications created for mobile devices or smartphones cater for secure data transmission medium and ensure use of secure protocols. Preference should always be given to authentic applications over web browsers.

5.6.6 Transaction Statement Validity and Suspicious Activity

Tracking of financial transactions and personal audit of account statements must be carried out on regular basis. Any suspicious activity must not go without a proper action and reporting of the incident to concerned authorities. Changing of passwords without any possible activity will always be in benefit of the user. A gut feeling of any activity should be responded immediately even if it does not bear any wrong response.

Online bank and account statements should be carefully scrutinized. Money transfers and electronic purchases should be reconciled with own receipts. It does not take really much time to check the online account details.

CONCLUSION AND FUTURE WORK

NFC does not address the notion of security in entirety and it requires the inclusion of standard cryptographic practices to protect its communication channel and the data while being at rest or during transit. Secure channel implementations in NFC can protect against maximum attacks. Communication over NFC channel is protected against Man-in-Middle attack due to the small distance of communication involved.

NFC has huge avenues and applications in our daily lives where it can provide ease in many routine tasks like mobile payments, ticketing system in transportation and access control procedures. NFC utilities are emerging as the standard is getting older and stable.

This thesis focuses on the NFC technology and its application in payment system on an Android device. The first chapter provides an introduction about the NFC technology with brief description of threats posed and possible defensive measure against the vulnerabilities reported so far.

Second chapter describes the basic RFID architecture with focus on different controls, their advantages and disadvantages. RFID is at the core of NFC technology. To understand basic working principle and possible difficulties in operations of NFC technology, one has to be conversant with the RFID basics. There is huge potential of RFID utility in our daily lives for identification and tracking of common user items. The same tags can be read by a smartphone which has NFC hardware and software available on it. Application based RFID tag reader using smartphone may be tested to evaluate difference and operational requirements.

Chapter three of this thesis focuses on Android application architecture with focus on the weaknesses which can be exploited to breach the security of an NFC application. There is a lot of room to define specific parameters for an NFC application in a smartphone. Restrictions and limitations which may be catered for during design phase of such application may be pondered upon.

Chapter four gives a brief list of NFC related technology laws in the US government. State laws of Pakistan which affect electronic transactions and use of information technology have also been briefly covered. There is a need to explicitly

enlist and modify laws which may regulate use of smart devices and vendor side equipment which is capable to address NFC technology.

Chapter five provides information about a basic flow of application design to perform payment transaction using NFC technology. Detailed specifications and components of NFC technology to be incorporated in any payment application may be researched.

There are a number of ideas which can be implemented to test on ground performance of the NFC architecture in payment and traffic ticketing system using smartphone capable of NFC technology based on card emulation procedures. The basic design for payment procedure can be expanded by incorporating a commercial Bank from the private sector to test possibilities of such services to the customers.

Storage of sensitive data on android devices is vulnerable to threats. Future studies may be carried out to analyze the security parameters being used to store important and sensitive data. Transactional security of the NFC based payments needs to be explored to offer design improvements.

REFERENCES

[1] NFC-Forum, [Online], Available: http://www.nfc-forum.org.

[2] International Organisation for Standardisation (2004). "Near Field Communication - Interface and Protocol ISO/IEC 18092".

[3] Ecma International, "Near Field Communication - White Paper", 2005, Ecma/TC32-TG19/2005/012, Available: http://www.ecma international.org/

[4] N. A. Chattha, NFC - Vulnerabilities and Defense, Conference on Information Assurance and Cyber Security (CIACS), 2014, no. 1, pp. 35–38.

[5] NFC-Near Field Communication, Reader/Writer Operating Mode, [Online], Available:http://mp-nfc.org/nfc_near_field_communication_operating_mode _.html#.U24BBIGSzng

[6] NDEF, NFC Forum "NFC Data Exchange Format - Technical specification", Version 1.0 [Online]. Available: http://www.nfc-forum.org/specs/spec_list/

[7] Tom Karygiannis, Bernard Eydt, Greg Barber, Lynn Bunn and Ted Phillips; Guidelines for Securing Radio Frequency Identification (RFID) Systems, Recommendations of the National Institute of Standards and Technology, April 2007

[8] Levente Buttyan, Jean-Pierre Hubaux, Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing, Cambridge University Press.

[9] Alessandro R. Aristide F. and Lorenzo Cavallaro, A system call centric analysis and stimulation technique, European Workshop on Systems Security (2013).

[10] Adrienne P. Matthew F. Erika C. Steven H. and David Wagner, A survey of mobile malware in the wild, ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (2011).

[11] Wu Z. Yajin Z. Xuxian J and Peng Ning, Detecting repackaged smartphone applications in third-party android market places, ACM Conference on Data and Application Security and Privacy (2012).

[12] Noah Gamer, The android Malware Problem, [Online], Available: http://blog.trendmicro.com/the-android-malware-problem/

[13] Mark G. Jared O. Justin G. David W. Thanh N. and Andrew Hunt, Automated identification of installed malicious android applications, Digital Forensics Research Conference (2013).

[14] Adrienne P. Erika C. Steve H. Dawn S. and David Wagner, Android permissions demystified, Conference on Computer and Communications Security (2011).

[15] Je Six, Application security for android platform, O'Reilly, 2012.

[16] Yajin Zhou and Xuxian Jiang, Dissecting android malware: Characterization and evolution, IEEE Symposium on Security and Privacy (2012).

[17] Yajin Zhou and Xuxian Jiang, Detecting passive content leaks and pollution in android applications, 20th Network and Distributed System Security Symposium (2013).

[18] Guidelines for Securing Radio Frequency Identification (RFID), [Online] Available: csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf

[19] Electronic transactions ordinance, 2002, Ordinance LI. of 2002. [Online] Available: http://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Fta5Y%3D-sg-jjjjjjjjjjjj

[20] Prevention of Electronic Crimes Ordinance, 2007, Ordinance LXXII of 2007. [Online], Available: http://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2FuZ5s%3D-sg-jjjjjjjjjjjj

[21] Payment Systems and Electronic Fund Transfer Act, 2007. [Online] Available: www.sbp.org.pk/psd/2007/EFT_ACT_2007.pdf

[22] Prevention of Electronic Crime Act-2015, [Online], Available: www.na.gov.pk/uploads/documents/1421399434_340.pdf

[23] Prevention of Electronic Crime Act-2016, [Online], Available: www.digitalrightsfoundation.pk/wp-content/uploads/2016/08/PECB2016.pdf

[24] COSKUN, Vedat, Kerem OK and Busra OZDENIZCI. Near field communication: from theory to practice. Hoboken, NJ: Wiley, 2012, xxviii, 361 p. ISBN 978-1-119-97109-2.

[25] Near field communication. Wikipedia: the free encyclopedia [online]. Available: https://en.wikipedia.org/wiki/Near_field_communication

[26] NFC and contactless technologies [Online] Available: http://members.nfc-forum.org/aboutnfc/nfc_and_contactless/

[27] FINKENZELLER, Klaus. RFID handbook: Fundamentals and applications in contactless smart cards, radio frequency identification and near field

communication. 3rd ed. Chichester: Wiley, 2010, xvi, 462s. ISBN978-0-470-69506-7.

[28] NXP PN544 NFC Controller. [Online] Available: http://eu.mouser.com/new/NXP-Semiconductors/nxppn544/

[29] Emulating a PKI smart card with CyanogenMod 9.1. ELENKOV, Nikolay. Android Explorations [online], Available: http://nelenkov.blogspot.com/2012/10/emulating-pki-smart-card-with-cm91.html

[30] GlobalPlatform Card Specification. v2.2.1. Global Platform, 2011. [Online], Available: http://www.globalplatform.org/specificationscard.asp

[31] Android secure element execution environment. ELENKOV, Nikolay. Android Explorations, [online], Available: http://nelenkov.blogspot.nl/2012/08/android-secure-element-execution.html

[32] Warakagoda, Narada. Telenor. Presentation: Near Field Communication (NFC): Opportunities & Standards. Available: https://www.scribd.com/document/59812368/ 081028-Nfc-Standards-Payments-Narada