Chapter 1 Introduction

Introduction

With the advent of technology, information exchange techniques have grown in leaps and bounds in the last 10-15 years. Internet and wireless technology spreading and introduction of new mobile communication devices such as mobile phones, tablets, and laptops have created new ways to generate, share, and gather information. Numerous apps have been introduced by developers for various purposes, from banking and finance management to calorie intake management and from dating apps to healthcare and fitness. The user uses all these apps and many more that collect large amounts of data that is personal in nature. This data is sometimes stored on the user’s mobile device locally, but most of the time, the data is uploaded onto the developer’s server for further analysis. This transfer of data from user’s device to developer’s server is done using an Internet. Internet is an insecure network which means that any data shared over it can be intercepted and read by anyone with means to intercept [1].

To prevent this from happening, a technique of data hiding is used. This technique is called cryptography.

Cryptography is a technique to hide the text under plain sight. The cryptography technique has two main functions, i.e., to encrypt and decrypt. Encryption function is used to hide the text. It takes in a meaningful message in text format and converts it into meaningless text message. Now, even if the message is intercepted by a malicious user, the user will not be able to make meaning from the message. The only way to make it meaningful again is to decrypt the message using the decrypt function. This function takes input of a meaningless text message that has previously been encrypted by encryption function and does exactly the reverse of it. It converts a meaningless message into a meaningful message.

This solves the first problem of sending the sensitive data securely over an insecure network.

The second problem comes when the data has been successfully sent across the network and received by the intended recipient. The data that the recipient has received is encrypted and it is of no use to the recipient in its current state. To use the data for intended purposes, the data should make sense to the recipient. This is where another process related to cryptography needs to be performed. In this
process the earlier encrypted data is converted back to its original meaningful format. This operation is known as decryption. Decryption operation converts cipher text into plain text.

Both encryption and decryption operations are essential for any cryptographic algorithm to succeed. The encryption operation is performed with help of a key which is used to convert the plain meaningful message into ineligible and meaningless message. This key can be any number or an alphabet or a string. The same key is required on receiver’s side when decryption operation needs to be done. The key needs to be sent from sender's side to receiver's side. There are two types of keys, public key and shared secret key. The discussion here is related to a shared secret key.

A key exchange protocol is set of rules that both sender and receiver need to follow in order to securely exchange the shared secret key. This problem of secure key exchange between two devices is one of the prominent issues in the field of cryptography.

1.1 Problem Statement

Authors of this thesis define problem statement as “Designing a universally composable key exchange protocol for mobile computers”. Subsequent description explains it in more detail.

As the world is transiting from a wired world to a wireless world, it is important to remember that it is easier to eavesdrop on a wireless signal than a wired connection. This is because of property of wireless signal that it is transmitted in all directions equally. The signal can be easily intercepted and decoded to data from using packet capturing tools and decoded for information. This information can then be used to harm or harass a user in different ways. The solution is to use encryption. We need to have a key for encryption and the key exchange protocols enable us to have that key.

A key exchange protocol is used to exchange a secret key between two computers. The computers can use this secret key to encrypt their messages before sending them over insecure network such as Internet. Since the message cannot be decrypted back to its meaningful state without key and only two computers, sender and receiver, have the key, only these two computers can transform encrypted message into a meaningful message. However, the prerequisite is that the key is not available to the adversary. Thus the key exchange process is critically important for security of the process. However, exchange of the secret key is not without problems. There are many challenges such as authentication, staleness of the key, etc.
Challenge of authentication deals with ability to authenticate incoming request for key exchange. The challenge is to make sure that the request is coming from a genuine source and not a malicious source. Stale key refers to usage of an old key which was generated before a certain period of time. This stale key can be used in replay type of attacks to exploit vulnerability of device. The device is vulnerable to this type of attack if it is unable to distinguish between stale and fresh key.

A key exchange protocol is required to deal with all these challenges and make the key exchange process secure such that it fulfils all the requirements by the particular application.

The authors of this thesis aim to design a key exchange protocol that can be used by all mobile applications that manage sensitive personal information. The information of such nature can include information regarding user’s finances, health, family, etc. The key exchange protocol should primarily be designed with mobile devices in mind. The authors have kept in mind limitations faced by mobile devices with challenges that come in designing an optimal key exchange protocol that is time efficient. The protocol is also designed with keeping in mind the network infrastructure and other limitations of developing countries.

1.2 Problem Description

The mobile and wireless computing devices have met with a huge success and have replaced traditional computers in many fields. As these devices are getting popular, they are becoming a target for hackers and other users who want to get personal data of users and use it for their advantage in one way or the other. This can happen by monitoring the traffic of incoming or outgoing packets from a particular device on an insecure network or by application installed on the device.

Due to this situation, security analysts and researchers have been exploring techniques that can aide in establishing a secure communication channel between source and destination over insecure network. Here the basic idea is to make communication secure such that malicious user cannot figure out what information is being transferred. Solution to this problem lies in the field of cryptography.

Both encryption and decryption functions utilize a key that is used to both encrypt and decrypt a message. Like a key of a lock this key is used for encryption and decryption of a message. It is
not possible to decrypt a message with different key than the one that was used to encrypt it. If it is tried, message will not go back to earlier meaningful state fully. This key needs to be common between both sender and receiver. This key is like a key of a lock where the same key needs to be used to both lock and unlock the door.

The idea of key has been around as long as the idea of cryptography. But with development of networks and rise of Internet, the distance between computers increased. Also a new possibility emerges where the computers are not part of the same network and do not recognize each other. It was due to this that the trust level between them becomes low. During this time the questions regarding security of sensitive data transmission over insecure network such as Internet were also raised. It was due to this reason the computers needed to be provided with a method of securely communicating over insecure network. This is where the key exchange protocol is required.

A key exchange protocol is used to securely transfer a shared secret key from one device to the other over insecure network. This secret key can then be used to encrypt and decrypt information, making secure exchange of sensitive information possible over insecure network. In this thesis one such secure key exchange protocol is proposed by authors.

The key exchange protocols use various types of cryptographic techniques such as hashing, encryption, signature in order to provide security. Using individual or combination of techniques mentioned above, parties interested in secure communication form a set of rules for communication that would let them exchange a common secret key. Later, this common secret key is used to encrypt messages between two parties.

The idea of key exchange protocol was first coined by Whitman Diffie and Martin Hellman in their 1974 paper [2] “New Direction in Cryptography”. In this paper they present a new technique to exchange a key by using mathematical characteristics. Another significant work in the field of key exchange protocols was done by Needham and Schroeder [3]. Both these works mark the beginning of modern day cryptography. In their work, Diffie & Hellman introduced what is now known as public key cryptography system. Since these papers, many other authors have proposed protocols till now. These protocols can roughly be divided into two categories - symmetric key cryptography systems and public key cryptography systems.
Symmetric key cryptography or shared key cryptography involves two parties using the same private key to both encrypt and decrypt the message. Hence it has better performance than public key cryptography. Symmetric key cryptography systems are also easy to understand, implement and maintain. Symmetric key cryptography can work on slower processors since it requires much less processing power when compared to public key cryptography systems. However, the problem with symmetric key cryptography is that in case if one host is compromised, whole network’s security will be compromised.

There is also a potential disadvantage in case the two parties do not trust each other. It is possible that two parties are not part of same network and do not recognize each other. It is also possible that the two parties are on different sides of the world and are communicating for first time. This is where they need a secure way to authenticate and share the key between them. If there exists a secure way to share the secret key between two parties, then application of cryptography is not required, however it is not the case. The distance between two communicating parties may be too large for one single network and connection may have to be routed through a number of different networks. These intermediate networks may or may not have secure connection or malicious users eavesdropping on the conversation. The cryptography overcomes this problem and provides a secure channel in insecure network for communication between two parties.

In a public key cryptography system two different keys are used, one for encryption and other for decryption. The public key cryptography works on two keys system: public key and private key. A public key is the key that belongs to a device attached to the network and is known by all other computers on the network, this key is freely shared with anyone who wants to communicate with the device.

In case of a private key, as the name suggests, it is private to the device and is never shared with anyone except with the trusted third party. The private key and public key are mathematically related and a message encrypted by a public key can be decrypted by a private key.

In a public key cryptography system there are three parties involved when a secure communication channel needs to be established over insecure network. These are sender, receiver and the trusted third party. The trusted third party is a neutral entity that both sender and receiver trust with their private keys. When a sender wants to establish a channel with a receiver, it does it through a trusted third party. The trusted third party generates and distributes the secret
key to both parties which can then be used to create a secure channel to communicate over insecure network. The trusted third party securely sends secret key to both sender and receiver by encrypting the secret key with their own unique public keys which both sender and receiver share with it. Once encrypted, this information can only be decrypted by using a private key by each of the parties. Thus the trusted third party makes sure that no one else but the intended recipient receives the message. However, the public key cryptography is very difficult to implement and maintain.

There are key exchange protocols proposed for both symmetric and public key cryptography techniques. Both symmetric and public key techniques are vulnerable to replay type of attacks, man-in-middle attacks, etc. Symmetric key cryptography has a set of predefined keys or a mathematical function. This means that the key is as secure as the mathematical function that is used to exchange it. In public key cryptography system, there is a third party that the other two parties trust. If the trusted third party is compromised, then it is possible to know each and every key that is generated and exchanged between the two hosts.

Designing a key exchange protocols poses its own unique set of challenges. Two of the major challenges that should be addressed are security and efficiency of key exchange protocol. The security of protocol can be achieved by considering following factors:

1. The concepts on which protocol is built must be secure on their own.
2. The way different cryptography techniques are used must be secure as well.

To address the first factor, it is assumed that the fundamental concepts that form the basis of key exchange protocols are secure. This leaves the second issue where different permutations and combinations of cryptography techniques such as public key cryptography and hashing, symmetric key cryptography with digital signatures must be secure as well. This means that the protocol must behave in a secure way when interacting with both parties. If the history of designing key exchange protocols is any proof, the second point is very challenging. Historically, key exchange protocols have been developed with significant vulnerabilities. Many protocols proposed by researchers were proved to be vulnerable to one attacking technique or the other in their later analysis by fellow researchers.

Performance of key exchange protocol is another point of concern in designing key exchange protocols for mobile computers. A key exchange protocol for mobile computers needs to be
integrated into practical applications. The efficiency of a key exchange protocol can be measured by the number of operations and overhead of messages. Therefore, in an application where user has constrained resources of processor, memory and battery power, it is extremely important that a protocol is designed so that it can perform operations with low processor and memory usage and does not significantly drain the battery. In recent times as people are becoming more and more aware about cyber security and extent of effects of loss of privacy, the demand for secure applications is growing and is expected to grow substantially in future [4] [5].

This thesis is focused on design and implementation of key establishment protocols for communication between two parties. The particular focus of this thesis is on designing a secure as well as resource efficient key exchange protocol for mobile based applications of new era of mobile based communication with heterogeneous hardware environment.

The next section provides brief description of background in the field of key exchange protocol. The authors also discuss major challenges in the field of key exchange protocol which motivate this thesis. Then, objectives of the research and brief organization of thesis are presented.

1.3 Background and Motivation for Research

As mobile wireless networks are gaining popularity and diversity of applications available for these mobile platforms increases, especially android being an open source system where an application can be installed by user without being first screened by a third party, users being victim of malwares is one of the major concerns for security researchers. It is specified in standards of mobile communication for authentication and key agreement to be used before any critical communication takes place. However, the security standards that have been specified are now old. These standards were specified for earlier generation of devices and mobile communication. Thus, they are not relevant any more for current/future generation of mobile devices where newer applications are being introduced on which people share their personal information. Hence, increased security standards are required. It has also been observed that a large number of key exchange protocols that are proposed by security researchers are found to be vulnerable to one attack or the other due to them being not tested properly before being proposed. Thus there is a large number of faulty key exchange algorithms also available which needs to be fixed. It is due to above reasoning that designing and developing a key exchange protocol for mobile computer is an interesting area for research.
In recent times in India e-commerce applications for mobile computers have become highly popular. E-commerce companies are offering significant discounts, cashback and a number of other offers to encourage users to install and use their mobile application in their devices. Security in these applications is crucial as they deal with financial information of users over insecure networks like Internet. This has also increased demand for secure key exchange protocols specially designed for applications in this category. We can take a multi-party key exchange protocol and modify its functionality to produce a three party key exchange protocol.

A large research material is present that shows efforts of researchers in using variation of Diffie-Hellman protocol to make secure communication possible. However, there has been very little success in this effort so far. Introduction of new low powered devices that come with a wide variety of hardware implementation has stipulated that a resource efficient key exchange protocol must be designed for mobile applications. Such environment favors less computing and less overhead which is a major advantage for a user with mobile device with low resources. It is due to this reason that computationally intensive protocols with multiple rounds of encryption are not suitable for them. Also peer-to-peer protocols which stipulate that all computers are similar in power are not applicable here due to sheer number of users and a wide variety of hardware available for implementation of system. Hence, design of key exchange protocols for a variety of hardware configurations and resource efficiency is another challenging research area.

The designing of key establishment protocols for two party mobile computers also involves a number of issues that are unique. One such issue is proper testing. Many two party key exchange protocols have been proposed by security researchers, however, most of these protocols are found be vulnerable to one attack or the other. This puts a question on testing methodology of a key exchange protocol. Also this can be seen as a sign to amend existing vulnerabilities in already proposed protocols that will strengthen them instead of proposing new protocols that are not properly tested and may have been vulnerable. Not many security researchers are focusing on this issue.

Keeping computing environment and methods on side, another import issue in designing of key exchange algorithm is analysis of its efficiency. In most protocols proposed in literature, efficiency analysis is not performed. An important parameter of analysis of efficiency of key exchange protocol is a number of operations it takes to exchange the key between two parties.
with the help of a trusted third party. The other parameters to measure efficiency of protocol are execution time and battery power used to process different tasks related to the protocol.

Based on above discussion several issues have been identified that are not addressed by researchers properly. This research aims to work on these issues. Following issues have been studied in key exchange protocol that needs to be addressed:

- It is observed during literature review that many protocols are designed for traditional desktop computers or server systems. This draws attention to designing protocols for mobile and other wireless computing devices. Therefore, it is very essential to produce a protocol specifically designed to meet the needs of mobile and other wireless computing devices.

- Principle concepts of symmetric key cryptography are as strong as mathematical formula they are based on. Therefore, for low powered devices it will be computationally intensive. A public key cryptography system with a trusted third party could be used for low powered devices reducing computation load on them significantly.

- A three party protocol has a lot of potential for future applications such as E-Commerce, E-Healthcare, E-Voting, etc. Thus designing a key exchange protocol that is resource efficient and fast is an important area of research.

- During literature survey it was found that many researchers developed new key exchange protocols without proper testing and hence the protocols were later found vulnerable. Another option is to analyze existing key exchange protocols and try to address existing vulnerabilities in them.

- As we transition into mobile based applications, security of such applications will be more in focus for software designers. This research can help software designers to better understand the parameters that affect the choice of using key exchange protocol in an application.

The next section briefly discusses work done during this thesis to address above mentioned points.
1.4 Summary of Contributions

This thesis aims at investigating and addressing issues in key establishment protocol design mentioned previously. The thesis contributes in following three parts. Each part addresses more than one concern that is mentioned earlier.

- **Review of existing key exchange protocols**
  This part contains study of existing key exchange protocols. We have divided key exchange protocols into two types, classic key exchange protocols that were proposed soon after Diffie and Hellman proposed their ground breaking key exchange protocol, and modern key exchange protocols that include multi-party key exchange protocols and card or other device based key exchange protocols. In first part of literature study various vulnerabilities were highlighted and compared with other protocols during same time line. Many variations of classic protocols were proposed and they were also included in the study of classic key exchange protocols and comparison of classic protocol vulnerabilities. In second part of literature study modern key exchange protocols were studied. These protocols included key exchange protocols that are used in group and protocols that use hardware such as a microchip or a magnetic strip to authenticate the computer. Many potential problems were identified and highlighted for these protocols. The review of existing key exchange protocols of different types is carried out in chapter two of this thesis.

- **Simulation of key exchange protocols to check their efficiency**
  This part of thesis highlights different parameters that affect execution of a key exchange protocol. The concentration is on following parameters: time it takes to generate and send key exchange message from a trusted third party, processor utilization to process the key exchange message and battery power required for the execution of the protocol. Later an important parameter, i.e. a number of operations is added to the list. The simulation begins with classic key exchange protocols on different systems. These systems include a laptop computer and two mobile phones with different configurations. Results of simulations are analyzed and the most efficient protocol is selected based on performance during the simulation. Later during research another simulation study was undertaken, during which the efficiency of the proposed protocol was checked against modern key exchange protocols. It was evident from the result that bar one modern key exchange protocol, the proposed protocol was performing better than all of the
proposed protocols tested against it. Details of various simulation experiments that were carried out during this research are discussed in chapter six of this thesis.

- Review for potential future application of proposed key exchange protocol

In this part of thesis, review of security requirements for some of the potential applications of the proposed protocol is carried out. These applications were selected based on their potential of users using them in their phones. These applications include an e-commerce application, an e-voting application and an e-healthcare record management application. All these apps were reviewed and different security requirements were selected. Some of the security requirements such as integrity or authentication were common in all applications. However, each application had its own unique set of requirements. For example, in e-healthcare record management system privacy of information is considered extremely important. In e-voting application auditing of user votes was found to be equally important factor of security. After determination of security requirements of each application, it was found that an e-commerce type of application has requirements that can be fulfilled by the proposed protocol. Hence, a sample e-commerce system was developed integrating the proposed protocol to check its performance against other industry standard protocols. Details of these simulations are discussed in chapter six and chapter seven of this thesis.

1.6 Chapter wise Organization of Thesis

The rest of the thesis is organized in following chapters:

**Chapter 2 – Review of existing key exchange protocols**

This chapter will discuss various key exchange protocols reviewed during the research and their functioning. In this chapter various vulnerabilities affecting the key exchange protocols and the solutions provided by researchers to address them are also described. The chapter will also include a discussion on setting up a simulation environment and selecting various key parameters such as key generation and control overhead time, as well as battery consumption to measure performance of the key exchange protocol.

**Chapter 3 – Research methodology**

This chapter explores different types of existing research methodologies. The chapter then goes on to compare different research methodologies based on its advantages and disadvantages when
utilizing them in research work. Lastly it describes research methodologies used in the proposed research work.

Chapter 4 – Testing and implementation strategy for the proposed protocol

This chapter gives testing and implementation details of the proposed protocol. The chapter begins with argument on why testing for the proposed protocol is necessary. It then goes on to give details on setup used for testing, various components of the setup and selection of suit of protocols to test and implement along with the proposed protocol. In the end of the chapter the authors justify their choice of a mobile based payment system for implementation and testing of the proposed protocol.

Chapter 5 – Testing and performance parameters for the proposed protocol

This chapter begins by giving details needed for experimenting and evaluating the proposed protocol. It begins by describing need for simulation and benefits of simulation method. The authors then discuss why it is required for the proposed protocol. Lastly, the authors discuss and justify their choice of various parameters considered under this experiment for measuring performance of the proposed protocol against other similar protocols.

Chapter 6 – Result of the experiment and performance comparison

This chapter begins by presenting results of the experiment under previously discussed model. The authors present parameter wise results of the experiment and give conclusions.

Chapter 7 – Summary and future directions

In this chapter authors summarize their research work. Guidelines for future implementation of protocol are also presented. The chapter is concluded with future directions for research work.