Faculty of Information and Communication Technology

DEVELOPING SECURE ANDROID APPLICATION WITH ENCRYPTED DATABASE FILE USING SQLCIPHER

Ardiansa Rachmawan

Master of Computer Science in Security Science

2014

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

DEVELOPING SECURE ANDROID APPLICATION WITH ENCRYPTED DATABASE FILE USING SQLCIPHER

ARDIANSA RACHMAWAN

MASTER OF COMPUTER SCIENCE

2014

DEVELOPING SECURE ANDROID APPLICATION WITH ENCRYPTED DATABASE FILE USING SQLCIPHER

ARDIANSA RACHMAWAN

A thesis submitted
in fulfillment of the requirements for the degree of Master of Computer Science in Security Science

Faculty of Information and Communication Technology

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2014

DEDICATION

I would like to dedicate this work to my parents, thousands thanks is not enough to replace all love that you have given to me.

DECLARATION

I declare that this thesis entitled “Developing Secure Android Application with Encrypted Database File Using SQLCipher” is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : .....

Name : .....

Date : .....

APPROVAL

I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in terms of scope and quality for the award of Master of Science in Security Science.

Signature :…….....

Supervisor Name :…….....

Date :…….....

ABSTRACT

The number of smartphone users is increasing every year. The technology changes the large form of personal computer become portable computer called smartphone. Todays the most popular operating system for smartphones is android, it is recorded that more than 1 billion android devices was activated. With this large number of today's android users, the possibility risk of this device lost or stolen is also high. The problem comes when the users have confidential data or information in database of android application. This secret information inside the phone shouldn't be accessed by other people except the authorized users. The information security lead to protecting information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. To react the problem stated, we propose to develop secure android application with encrypted database file using SQLCipher.

ABSTRAK

Bilangan pengguna telefon pintar semakin meningkat setiap tahun. Teknologi telah mengubah komputer peribadi yang besar menjadi komputer mudah alih yang dikenali sebagai telefon pintar. Hari ini sistem operasi yang paling popular untuk telefon pintar adalah android, ia mencatatkan bahawa lebih daripada 1 bilion peranti android telah diaktifkan. Dengan jumlah pengguna android yang besar pada hari ini, risiko kemungkinan peranti ini hilang atau dicuri juga tinggi. Masalah itu datang apabila pengguna mempunyai data sulit atau maklumat dalam pangkalan data daripada aplikasi android. Maklumat rahsia dalam telefon tidak boleh di akses oleh orang lain kecuali pengguna yang dibenarkan. Peneraju keselamatan maklumat untuk melindungi maklumat dari capaian yang tidak dibenarkan, penggunaan, pendedahan, gangguan, pengubahsuaian, semakan, pemeriksaan, rakaman atau pemusnahan. Untuk bertindak balas masalah yang dinyatakan, kami mencadangkan untuk membangun aplikasi android selamat dengan pangkalan data disulitkan menggunakan SQLCipher.

ACKNOWLEDGEMENTS

First and foremost, I would like to take this opportunity to express my sincere acknowledgement to my supervisor PROFESOR MADYA DR Abd Samad bin Hasan Basari from the Faculty of information and communication technology Universiti Teknikal Malaysia Melaka (UTeM) for his kindness in supervising student like me.

My second acknowledgement goes to my parents, M Salim and Harminah for their support in many aspect of life to me. I am also grateful to all of people around me during my study which has given me positive and negative experience in learning this life to become better person.

Table of Contents

CHAPTER 1

INTRODUCTION

1.1 Research Background

The number of smartphone users is increasing every year. The technology changes the large form of personal computer become portable computer called smartphone. Todays the most popular operating system for smartphones is android, its recorded that more than 1 billion android devices was activated (Yarow, 2013) compare to iOS that reach only 650 million activated devices. Another source from the statistics shared by statista.com about the global market share held by the leading smartphone operating systems from 1st quarter 2009 to 4th quarter 2013 conclude that android is become the most popular operating system by having 77.83% of users followed by iOS in 17.8% of users (Statista, 2014).

The reason behind popularity of smartphones is the large amount of available application to downloads(Avancini, Ceccato, & Kessler, 2013). With this large number of today's android users, the possibility risk of this device lost or stolen is also high. The problem comes when the users have confidential data or information in database of certain application in android. This secret information inside the phone shouldn't be accessed by other people except the authorized users. In facing this issue, we would

like to conduct a research about developing secure android application in order to have a security feature to protect confidential data and information in it.

As stated by (Mattord, 2011)the information security lead to protecting information from unauthorized access, use, disclosure(Manivannan & Sujarani, 2010), disruption, modification, perusal, inspection, recording or destruction. In order to maintain the information security of confidential information inside android device, we need to tackle some possible ways of attack addressed to android application by keeping it from being access by unauthorized users, being used, being modification as stated above.

In developing android application, android has provided database called SQLite. SQLite is an open source database that has supported standard relational database features like SQL syntax. SQLite is embedded inside each android device, not like other SQL databases that has separate server process, SQLite reads and write directly to regular disk files and a complete SQL database with multiple tables, triggers, indices, and views is contained in a single disk file.

When the developer develops an application with the database and in that application will request the user to enter the username and password to access it. As we know, the information such username and password are stored in the database, and this information is very sensitive, means that only the authorized person that can access the application. And the problem is when the information in the database can be accessed by someone that tries to steal the information. This problem occur because of the

developer does not consider the security of the database, the developer store the original data into the database and does not give any extra security features to protect the data.

In this project we would like to develop secure android application with encrypted database file using SQLCipher. This project will be very helpful to increase the security of the information and protect it by encrypting all information inside the database. It is unlike the standard database that only provide database without any security features, and if we want to implement security features usually requires additional extension that can support the database. In fact that most of the additional extension for database that support encryption is usually not an open source, means that we need to subscribe it and pay amount of money.

1.2 Problem Statement

As stated before that android usersare larger than other smartphone OS users. With this phenomenon it comes with the risk that these devices possibility of device lost or stolen is also high. And the problem occurs when we have an application inside that device that contains sensitive information, and android design to afford secure but unrestricted to the users(Jeter & Mishra, 2013). The suspect who found or stole it can do anything with that device as they want, they can get our sensitive information which is not belonging to them and this is need to be supported multiple security objectives(Scarfone, 2013).

To develop android application, android already provide support for the developers to include SQLite database inside their apps, but they doesn't have support for securing data like data encryption and although android security mechanism has ensure through the system and data security mechanism, it doesn't meant that there is no android security risk(Bing, 2012). So when the victims try to look for the database of application, they can find it inside the application directory. The rooted android smartphone allows the users to explore all the systems and directories without any limitation. By opening the database, victims can directly get the original information inside it, because that database is not protected with any security features and it is contain readable information.

1.3 Objective

Refer to the problem statement above the objectives of this project are to:

- Develop android application with secured database file in order to secure and distinguish the sensitive information inside the database.
- Develop android application database implementing SQLCipher to secure and distinguish the information inside database by using 256-bit AES encryption.
- Develop secured android application database using open source extension to SQLite database that provide 256-bit AES encryption.

1.4 Scope

The ACM computing classification system (CCS) categorized several field in computing system, based on the CCS this project is categorized under the security and privacy(Amoroso, 1994). In security and privacy still has several knowledge field, and this project is more specifically to database and storage security field. In this database and storage security still has several knowledge branches, and this project will focus on management and querying of encrypted data.

As mention in the problem statement, the project will be covered in the android application security problem in securing the database by encrypting it using open source extension.

This project will target the user of android OS that use their mobile phone as a device to facilitate them access the information and protect the information, means that only the authorized person can access the information.

1.5 Project Significance

This project aims to provide security for all android application that embed with SQLite database to make the user protect their information inside their mobile phone when their mobile phone move to irresponsible hand that can gain the information illegally because sensitive data handled by mobile users become easily exposed(Barrare & Hurel, 2013).

The project will be different with the normal android application that use standard database to store their information because the normal SQLite database do not provide the security and protection to the information. In database, there is three main function that is insert, retrieve, and delete. In this project the process to secure the data is by encrypting the data before the data is stored into the database(Fahl, Harbach, & Oltrogge, 2013). When the module insert data is executed, the original data that has been inserted by the user is not directly stored to the database, the original data will be encrypted by 256-bit AES encryption that is provided by SQLCipher after that the encrypted data will be stored into database. Instead of storing the original message, this project stored the encrypted data into the database.

1.6 Expected Output

This project is expected to help the android application developers implementing security features in their database application so they can develop secured application without worry about their information being misuse by unauthorized person.

This project also facilitates the developer to develop secured android application by using open source extension to their database application.

1.7 Conclusion

With the growth of android OS users today results the chance of device lost or crime increase. With this condition makes some of users who have application that contains

sensitive information inside their smartphone feel worry when they lose their smartphone. They feel worry because when the information inside the application is misuse by irresponsible person that easily retrieve all the information from that smartphone causes of the database store the information as the original without any security features.

Refer to the case above we propose a project that will develop secured android application with encrypted database using additional open source extension to database called SQLCipher, this project will produce android application with 256-bit AES database encryption. With this project we hope to all android application developers to develop secured application using this open source additional extension to store encrypted information instead of store the original information into database and to distinguish the information so this application can only be accessed by the authorized person.

In the next chapter will be discussing about literature review to support the research part to this project, literature review is very important to make a good research project. By referring to current problems that researcher being faced, we might improve or contribute in that knowledge.

CHAPTER2

LITERATURE REVIEW

2.1 Introduction

In this chapter we will try to elaborate about domain, existing system, technique, and project requirements. These are the important topics in this literature review to support structuring this project. We will explain the domain of the project that we are proposed, the global domain of this project is more to security and privacy and it will be elaborate clearly in this chapter.

The existing system that was already established, we study about the advantage and disadvantage of the existing project as a reference to develop better project. In this chapter also elaborate the technique that we will use in our project. Also all of the requirements needed to develop this project and finally will be closed with conclusion of this chapter.

2.2 Domain

This project is about encrypting database,from the ACM computing classification system (CCS) this project is categorize under the security and privacy domain. In security and privacy domain, this project will go to subdomain called Database and Storage Security. To see the global view of this project domain, we can look at the figure 2.1 below.

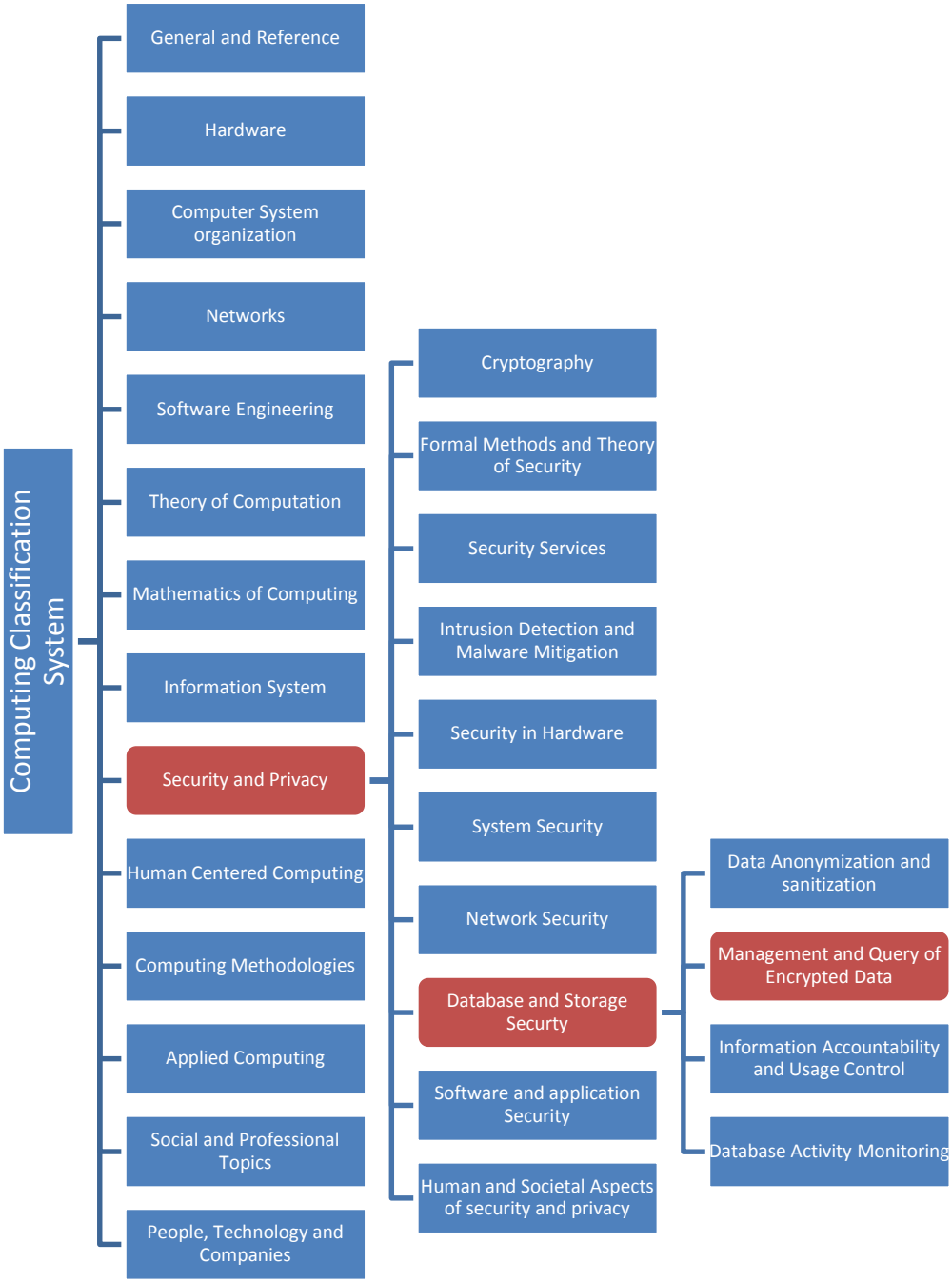

Figure 2.1 : Knowledge domain of project

After understanding the figure 2.1 above, it shows that this project is about management and query of encrypted data the specific knowledge field of security and privacy. And the explanation of this knowledge field is important.

As stated in(Amoroso, 1994) Security and privacy is the new branch that incorporates concept scattered in old classification as well as numerous new terms. Data encryption is now cryptography and is more fully developed with additional concepts.

2.3 Existing System

2.3.1 Attribute-Level Encryption of Data in Public Android Databases.

This is project (Loftis, Chen, & Cirella, 2013) is about software that will encrypt specific attribute of databases residing on the internal secure digital card(SD Card) of android device, here is the discussion about the technology and method used in their android database encryption and decryption implementation and their potential scalability to broader application.

The first discussion is about environment they used to evaluate their attribute level encryption method. The environment in this project consist of an android device running locally installed native android application, they collected data and store into SQLite database located in the internal memory of devices. Another windows based (x86) data transmission program installed on the laptop with the SQLite database via USB connection to android device.

The scenario of testing environment start with SQLite database retrieve from android device using android debug bridge (ADB) pull command. Then the database is stored in laptop hard drive memory for a temporary moment, next x86 data transmission program synchronized to the server database using RESTful web services and HTTPS communication. And finally the x86 data transmission program pushed the temporary SQLite database back to the android device from laptop using ADB push command. Below is the figure 2.2 of their testing environment.

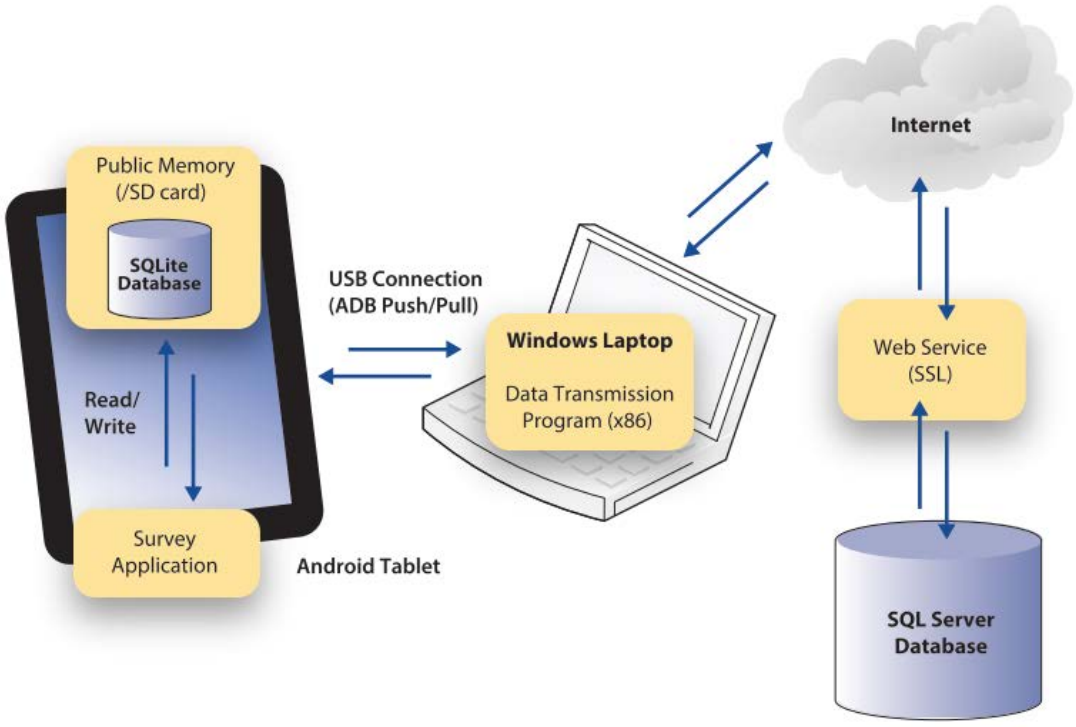

Figure 2.2 : Test environment configuration

To avoid identification of any information related to location or individual that is being surveyed, they decided to encrypt the entire attribute related to personally identifiable information (PPI) such names, addresses, and phone numbers. Their approach required the users to enter a shared symmetric key passphrase and the app to create or recover private key(for each attribute value) that is embed in the final cipher string. The figure 2.3 below is the process of encryption.

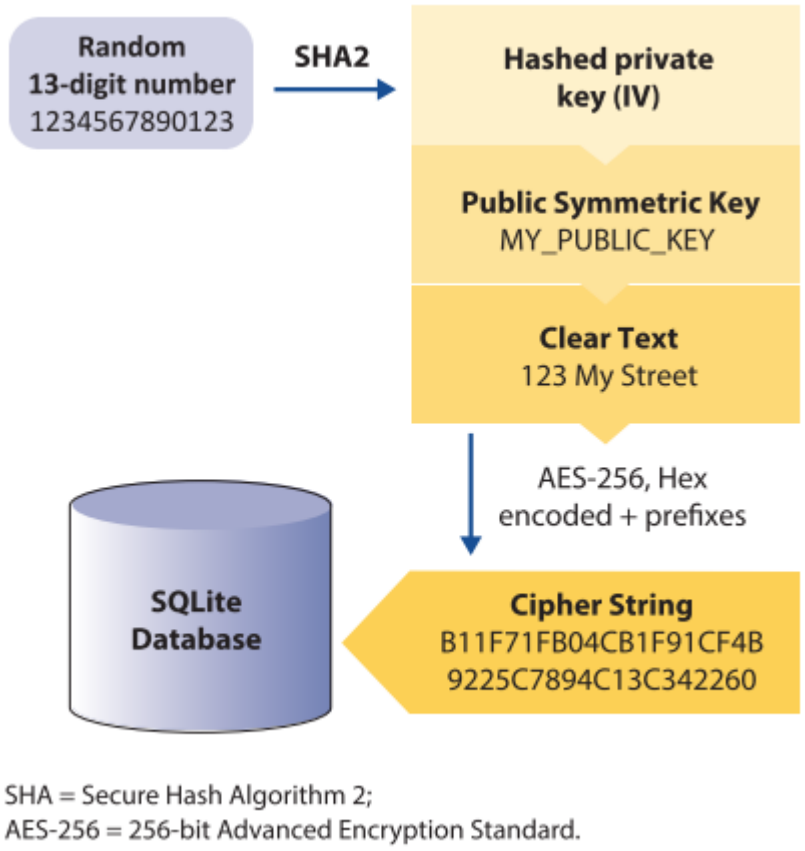

Figure 2.3 : Encryption process