Semester Project
MSCS 630

***"Ed's Traveling Barbershop"* Android App**
Jay Modi

1. Abstract

The purpose of this project is to explore the implementation of different security algorithm and protocols in an Android App. While the number of applications on the Google Play Store increases dramatically over time[1], security has lagged behind. Very elementary mistakes such as leaving secret keys or tokens exposed and not encrypting sensitive information may be more common than one thinks.
This project intends to exemplify some of the security measurements that developers may implement during the app development process, and the solutions they provide for ensuring that sensitive information is safe.

2. Introduction

My motivation for pursuing this specific project is that it provide a glimpse into some of Security issues that may arise during app development and how to solve them.
In addition, this project exemplifies that some measures can be very simple to implement while making a significant difference in the app's general security.
Moreover, the specific project topic which is a mock barbershop, indicates how the subject of Cryptography ties-in to real world applications that are used on a daily basis.
My personal ambition to pursue this project was to create a project that I could expand upon later on and perhaps develop it to an extent where I could actually publish it in the Google Play store as well.

3. Methodology

The approach was taken in this project was to build a skeleton (or a "Mock") android App for a friend, who could potentially use it in the real world as a finished product.
To begin, the app would only had very low level and simple functionality such as saving the user's appointment info to a database, without any encryption or security standards.
As the project progresses, AES encryption would be added to protect the user's specific personal/sensitive information.
The application is mainly built in the Main Activity instance, where all the actions are triggered by the OnClickListener.

[1] http://static1.volkskrant.nl/static/asset/2014/playdrone_5524.pdf - 25% increase June - November '13.

Once the user clicks the “Make An Appointment” Button, An alert dialog opens up. This is where most of the development work came into effect. The alert dialog accepts a string (Not many restrictions). If the user clicks on the submit button without inputting anything, the app will not continue. The string that is submitted is then stored in a variable. This variable will be the data that we are encrypting, using our AESHelper class. Afterwords, A date picker opens up, prompting the user to enter a date he wishes to make the appointment on. Then, a Time picker that asks the user for the time slot he wishes to have on the set date. The dialog then closes to complete the action and all the data is stored in a DB in the phone’s internal storage.

4. Experiments

Some of the experiments that were done during the implementation phase were initially inserting information to the database without encryption, and then progressing towards implementing encryption of the user’s name using AES while examining some key mistakes that were made along the way.

5. Conclusions

My key takeaway from this project is how vulnerable apps are. Nowadays, anyone can make an app and put it on the Play store or the App store. While these stores try and verify there is no malicious intent or misuse of information behind the app, they do not really ensure that the data is stored in a safe manner. It is up to the developer to ensure the safe collection and storage of information. It is up to the user’s discretion to select which apps may or may not put his personal information at risk.
In addition, as I mentioned in my YouTube video, a key conclusion that I have made following this project is that encryption of data should be a part of the business requirements that are decided upon even **before** sitting down and writing code, or building the app.