Milestone

EnNotes Encrypted Notes – Android

Balaji Murali

Abstract:

This paper talks about my idea for creating an android application that will allow the user to store confidential information in encrypted format using AES(Advances Encryption Standard). This will use the standard android API and be backward compatible with many versions of android.

Background and/or Related Work:

There are many applications in android play store that provides options to save and organize notes. I am planning to extend this in to creating an application that will not show the notes in plain text, till the user authenticates with a finger print or password. This application also has potential to be a digital locker for storing all kinds of data.

Methodology:

- User will be prompted to set an initial password if it is not set already, and it will be persisted in the database or the preferences file for the application. Password will also be salted and not stored in plain text.
- After an initial password is set or if the password already exists user is redirected to the home screen where the existing notes will be displayed decrypted as cards.
- At the bottom of the screen a simple text box to add a new note will be displayed, possible additional features will be discussed in the experiments section.
- When the user saves the data, it will be encrypted using AES and persisted in a SQLite database.
- An option in hamburger menu will give the user an option to show the notes encrypted or decrypted automatically when the app is open.
- I will be using the crypto api provided by java to handle the encryption and decryption of the user data.

Experiments:

- I will be providing an option for the user to store images encrypted, also possibly letting them take a picture using the camera app.
- Android finger print api will be used to decrypt the notes and images possibly.
- Explore using other sensor api provided by android in the application.
- All of these features will be attempted based on availability of time before the submission date.

Discussion and/or Analysis:

While the experiments mentioned in the above section is still work in progress and have not been tested thoroughly, I am still working on getting the core functionality of the application running.

One of the important point of discussion is how to store the key which allows the user to decrypt the notes, I have not found any other good solution other than storing it in shared preferences or the SQLite database itself. Password can be salted and stored but is this enough for working with an offline app?

If the app can be allowed to communicate with a web server or some cloud based provider, maybe some api can be used to stored the password remotely away from the app providing an additional layer of security.

Finger print can be used to access the password from memory, providing another layer of security offline before decrypting the notes.

Conclusion:

In a world where privacy is a game changer, apps like EnNotes can help prevent should surfing in public. In the uncomfortable times when you lend you phone to some one else, app like EnNotes will provide the additional security and safe guard your information.

I believe EnNotes can be a useful tool for users to confidently save and retrieving data offline and securely.

References:

1. Google keep app design for my design elements
2. Inspiration for the app https://www.nytimes.com/2018/10/10/style/why-you-cant-stop-looking-at-other-peoples-screens.html
3. Snippets of code used in creation of the app and reference for building the app. https://developer.android.com/