Gentjan Gjeci
Final Writeup
Due: 05-09-2017

Because privacy has been one of the fundamental principles of our society it is very important that in our digital age we uphold that principle and protect our privacy by taking appropriate measures to do so. Encryption of our communication through digital media is the foundation upon which we build to protect our privacy. In the digital age, information plays such an important role and it affects our lives in one way or the other. Protecting our information is crucial, and finding better solutions or improving upon the existing ones, motivated me to further investigate how encryption works and how it can be used for our own benefits to keep our communications safe. As more and more mobile devices are used in our everyday lives I wanted to develop an application that sends and receives encrypted messages between users.

As the information in the digital age has become more and more important, keeping our information private and secure has become a necessity. If personal information is compromised it can have dramatic effect on people. With the tremendous increase on the usage of mobile devices and messaging applications to communicate between each other, it has become a challenge to keep our information secure from malicious people. Most mobile users today exchange messages with each other thinking that only them and the intended recipient will see the information. But as the data moves through the digital media encrypted it can compromised and stolen.

Most text messaging application people use in their mobile devices do not encrypt the data . Data traveling from user to user can be collected very easily from hackers or a person with the right skills. The information obtained illegally can be used for anything, which can have a devastating outcome for users. Encrypting the data is a way to protect information from unauthorized entities. Encryption makes it almost impossible for anyone to read the the encrypted data or make sense of the information even if they are able to obtain the data. Using

existing encryption technology enables users to share information securely, and only the intended users can decrypt and read the information. In my research I will show how we can use encryption tools to build a secure messaging application which can be used to share information securely through the digital media.

Before the data is transmitted between parties, it is first encrypted by a strong encryption system built specifically for this application. I am using AES-128 bit encryption, one of the most advanced and secured encryption in existence today. The encryption key will be built before the communication starts and will be shared between users in a secured way. After that the both parties will use the same key to encrypt and decrypt messages sent between them.

The application will be installed among different virtual android devices and a conversation will be started to share messages between them. For experimenting purposes both the encrypted and unencrypted messages will be shown so the messages can be analyzed and compared between them.

My application's is name is UCrypt, and as mentioned it above will be used to encrypt and decrypt text messages and other shared files between two android devices. The AES-128 bit encryption was created following the steps we learned in class. The AES-128 bit program we created step by step during the semester was not created specifically to be used in an Android application. Changes had to be made to it to make it work in my application.

After the changes were made I included it in my application and started to use it to encrypt messages users exchanged with each other. The key used for the encryption is stored in each application. Storing the key in each application as i did for testing purposes does not work in production. The key has to be known only to the parties who established a connection ready to exchange information, and must be kept secret. Once the secured channel is established then the devices can communicate with each other securely. As of right now my application is used to encrypt only plaintext-support for other file types such as pictures needs to

be developed. Decryption also needs to be finished and fully functional before the application is ready to be put into production.

One other important thing I need for this application is the functionality to use public/private encryption to share the key securely between users. And to add more to the security of the application I would like to keep using the same key only for the duration of the session. That means that a new key must be generated, shared, and used after the a session expires and a new one starts.

Furthermore the application needs to have the functionality to check for message integrity. We need to make sure that a message or a file is coming from the device or the person we are expecting it to come. As I mentioned above, in the case of a man in the middle attack it is not enough to just encrypt the information but we also need to make sure that no one has changed it in midway. Encryption prevents unauthorized user from from reading the encrypted message but it does not protect us from some une changing the message before it gets to us. Being able to verify that the integrity of the message is very important as well.

In the process of developing the application I learned a lot about using Android studio and the build in functionality of sending and receiving messages in android. After I built the required java classes for sending and receiving text messages I configured the AESCipher class which implements the AES-128 bit algorithm and the appropriate functions to encrypt those messages.

As I was developing the application I ran into some java runtime errors. The AES algorithm was not working correctly and it crashed my application with a number of different errors. After some time, I figured out that some java regular expressions I was using in AESCipher class were not working in appropriately thus causing the application to crash. I had a really hard time understanding the error because I did not know that java regular expressions don't work the same way in an android environment. I had to come up with my own functions to

do what the regular expressions did previously. Finally after I made all the changes I was able to get the expected answers, and no more errors.

Up to the milestone, my project was able to send and receive messages only from the same device. After the milestone, I was able to create multiple virtual devices and also be able to finish the functionality of sending and receiving messages between multiple devices. In the beginning the default messaging app in android would interfere with my messages. I had to figure out how to send and receive messages within the same application in order to test my project. Doing some research I was able to find out how to create and configure the right activities so the text messages were being processed by my application. All the work from the start to the end was a challenge, and I was able to learn a lot about android app development. Creating the application was not terribly hard, but it was time consuming and a lot of research needed to be done. Adding AES_128 bit encryption to the app made it even more challenging, but it was worth it. More needs to be done with this application besides the main functionalities that have implemented so far before it is ready for production. However I am very proud that the most important key features are implemented and working.

Securing the information by using strong encryption makes it impossible for unauthorized users to read the information illegally. Users can share data between each other without the danger that their information will be compromised, stolen, and used to harm them.

References

Alexander Stanoyevitch. (2013). *Introduction to Cryptography with Mathematical Foundations and Computer Implementation*.

https://developer.android.com

http://www.androidauthority.com

http://stackoverflow.com