EncryptZip: Compressed, Encrypted Containers on Android
Project Milestone

Alex Shah

4/7/18

1 Abstract

2 Introduction

Encrypting files is a common practice to prevent unauthorized or unintended access to sensitive information. However, encrypting each file is only one facet of security in a system. Encrypting the container which sensitive information is held can prove more robust than encrypting on a per file basis, or in addition to it, in applications where the system cannot be entirely secured or in addition to measures such as disk based encryption. These three levels, file level, container level, and system/disk level encryption ensure that intended access is compartmentalized in nature and can ensure that a system is truly secure. While most desktop systems have applications to accomplish the container level of encryption, such as Veracrypt, Android does not have a native application and third party implementations use proprietary methods. The goal of this project is to use built in features and standard systems to create a container level encryption scheme on the Android mobile platform.

3 Background

4 Methodology

Utilizing the Android SDK and available APIs provided by Google and within Java, it's perfectly feasible to encrypt files, zip them into a container, and encrypt the container itself. This also has an intended side effect of reducing the file size by using compression, as well as ensuring that containers are dynamically sized. It would then be trivial to compute the hash of a zip for an added measure of security, as well as Google drive support to store, share, or keep an encrypted zip container synchronized between two remote parties.

5 Experiments