Stephen Haffner.25, Kyle Gordon.688, Will Sloan.848

CSE 5473 | Network Security

Final Project Description | P2

2017.04.10

Project Goal

To create a secure and confidential file storage utility that ensures the integrity of the files stored on the server. We plan to encrypt the files on the client side in a way that prohibits a malicious server or a system administrator from leaning about the users' data or modifying them without the users' knowledge.

Preliminary Design

Authentication will use the primary user name and password combined with a freshness token to generate a temporary session key to authenticate all file transfers. Each user device will generate a key-pair used to sign any files created or modified by the device. A secondary password will be used to generate a symmetric key on the client. This key will be used to encrypt the signed files.

Roles and Execution Plan

Our application consists of an Android application and a server written in Golang. Will is taking the primary development position on the server and Kyle and Stephen are taking the primary development roles on the Android app. The app and the server communicate with one another using raw JSON over HTTPS.