Troy Flagg
Project Milestone
4/14/19

StegHide On Encrypted Files.

Abstract

This paper describes the approach taken for encrypting specific text files with AES and then using an open source library called Steghide to hide the encrypted files within images. This will allow for a hidden transmission of files without any reduction in image quality. A second user who also possesses the AES key will be able to scrape the web page the initial user hosts and then extract the encrypted file which they would then be able to de-crypt the file.

Introduction

The motivation behind this is to create a proof of concept for hidden transmission of messages while also encrypting those messages. This allows me to explore three different fields through one project, web hosting and scraping, steganography, and AES.

Background

This project will take very strongly from open source projects such as Steghide. This is a package that facilitates steganography. Also I will be taking very heavily from AES documentation.

Mid-Point summary

Summary

So far I have spent time learning about python system calls as well as hosting images through pythons simple server. I have also spent time experimenting with Steghide and getting familiar with its libraries.

The initial pass at the python simple server was very messy but preformed its basic function of hosting images and then being able to spin up a second user to perform a web scrape of the images from the first user. Similarly the first pass of including the Steghide calls within the server were also messy but functional. In the current state I am transitioning to turning the Steghide calls and web methods into classes to increase readability and maintainability. So in the web-server branch on my github repository the code would need to be rebassed to the initial commits to function.

Completed Work:

Code wise I have created three different python scripts, the main method which determines if the user is a host or a client and will preform actions depending on the decision. I have also created a python script which contains all references to Steghide wrapped up in methods which will make system calls to exploit the libraries and methods provided by Steghide. If the main method is ran through the host path it will call various steganography methods to hide a pain text file within an image then spawn up a simple server to host the image.

Similarly if the main method traverses down the client path, it will inquire for the IP of the web server and then preform a web scrape to download all of the images. Then it will preform various Steghide calls to extract the text file hidden.

Next Steps

As stated in the summary I am in the progress of wrapping the methods into classes. I also have to implement the ability to preform encryption onto the given file by the host, and similarly decryption from the client. With the ability to encrypt and decrypt files I would have accomplished the initial goals set forward.

Stretch Goals

Test hiding files other than text files.

Allow for a form of chat between the two users by having each user host images for the other to download and read rather than a one-way form of communication.

References

Steghide: http://steghide.sourceforge.net/

Python documentation: https://docs.python.org/3/tutorial/

Stack overflow: https://stackoverflow.com/