

CovertFS Implementation

Ryne Flores, Kyle Gorak, David Hart, Matthew Sjöholm, LTC Timothy Nix
Department of Electrical Engineering and Computer Science
United States Military Academy

Abstract—In 2007 Arati Baliga, Joe Kilian, and Liviu Iftode of Rutgers University presented the idea of a web based covert file system [2]. The purpose of a web based covert file system is providing confidentiality and plausible deniability regarding the existence of files. The key components of a web based covert file system is hiding files within media using steganographic techniques using online file sharing for the purpose of collaboration [2]. We created such a system, covertFS, as a prototype to develop the idea for a web based covert file system previously mentioned. Our prototype of the web based covert file system implements steganographic techniques to obfuscate an entire file system on a public file share site. By storing data in this manner, rather than within the application or on a users computer, we provide confidentiality and plausible deniability to both the users and the companies that manage these public file sharing sites.



1 INTRODUCTION

TECHNOLOGY continues to integrate itself more and more in our daily lives because of the convenience it provides to users. Users are becoming connected to the internet in multiple ways nearly everywhere they go. Numerous devices are being developed and released to provide more convenience to users and to keep them updated on their various interests. A user will usually have at the very least a cell phone on their person and throughout their routine on any particular day will browse email, social media sites, and various other applications. These applications themselves, regardless of the convenience they provide users, can track and offer the user the option to post their information on the user's social media site profile to share among friends and acquaintances

The majority of people interact with various forms of technology throughout each day. Depending on what type of tech-

nology we interact with there may be some type of data collected from our interaction. Also the use of social media is wide spread and it is easier to find various types of information about people because of this.

The means to store and share information in a covert manner not only serves multiple purposes, but also has various implications depending on how those means are used. There will be innovations designed with the good intentions, yet there will also usually be clever modifications of those designs for malicious intentions.

This project is an application that allows users to share information in a covert manner that can provide plausible deniability to not only the users but also to the file sharing or social media site that is being used as a medium where the information is stored.

2 RELATED WORKS

There are other projects and systems that have been released which offer users covert methods of sharing information. Such examples include Tor and StegFS[4]. The main concepts of this project were obtained from a paper that which involved faculty and students from Rutgers University[2]. There has been no other implementation of the application described in the Rutgers' paper, and this project is our take at creating a working prototype which could later be used to develop a successful application or implementation of the covert file system.

3 DESIGN OVERVIEW

In this section we will explain how we decided to implement a prototype of this project.

3.1 Web Connection

Our application's interface with the internet needs to serve three purposes:

- 1) Retrieve images to use for embedding a message.
- 2) Upload images to a public online forum anonymously without altering the image.
- 3) Retrieve specific images from a public online forum anonymously without altering the image.

After some research, we discovered a site that could satisfy the first purpose. The Cat API is a site that can offer random cat images. This is suitable because they are content neutral images that were big enough to store information inside, and the site is reliable. A downside to this approach is that statistical steg analysis can be done to compare the uploaded images to the originals. The possibility of using local unique images is out of the scope

of our project. The next two requirements are fulfilled by Sendspace.com. This site allowed our application to easily interface with to upload and download images anonymously.

The only significant issue that we encountered while using these online resources was with Sendspace.

The online resources work together as follows:

- 1) The Cat API retrieves a random cat image for a message to be embedded into.
- 2) Embeds message into image.
- 3) This new image is uploaded to Sendspace. Sendspace returns and download and delete URL.
- 4) The new image from step 3 can be retrieved from Sendspace using the download URL.

3.2 FUSE

What FUSE is, what it provides for us, and why we choose it.

3.3 Mounting the File System

Subsection that goes more in-depth of our use of FUSE and our file system.

3.4 MEMFUSE Module

3.5 COVERTFS Module

3.6 Mapping File System Data to Photos

How is the data stored in our file system, and how it is constructed.

3.7 Encoding a File System

The covert file system uses a drop in steganography module that takes in a bytearray object and returns a URL to an image. We used "least significant bit" steganography for this application because of its simplicity and reliability.

3.7.1 Steganography Implementation

Least significant bit (LSB) steganography is a Substitution type of steganography [?] that replaces the least significant bits in the image's pixels. Our steganography module is not true LSB steganography because we replace the least significant bits of each pixel allowing us to encode one byte of data into every pixel. First, we break every byte of the message into three segments. Two segments of the byte will contain three bits, and one segment will contain two bits. Next, we replace the three least significant bits of the red component with the first three bit segment. The green component follows with replacing its least significant bits with the second three bit segment. Lastly, we replace the two least significant bits of the blue component with the remaining two bit segment of data. There are obvious drawbacks to our implementation of LSB steganography, primarily that the image may appear distorted as seen in Figure X. However, with the modularity of the project we used this implementation to increase the amount of data stored while limiting the latency in uploading and downloading images for large file systems.

3.7.2 File System to Images

The first step in encoding a file system into an image is retrieving an image. We use "The Cat API" which retrieves a random cat picture from Tumblr (c). Once we retrieve the image we determine the number of bytes we can encode in the image by multiplying the height and width of the image, in pixels. Since we encode one byte per pixel, this results in the total number of bytes of data we can encode in the image. Next, we take the data we are going to encode and append a special end of file encoding. If the length of the data is less than the amount of data the image can hold, we

encode the data into the image using the steganography method and return the url to the hosted image. Otherwise, we must break the data into multiple segments. In this situation, we must first ... blah blah blah ... encode upload repeat...

3.7.3 Steganography and CovertFS

Based on the requirements of our file system set out in the into steg has obvious risks such as statistical analysis, visible alterations, etc.

Statistical analysis info.

Visible alterations info and pictures.

4 FUTURE IMPLEMENTATION PLANS

One of the things we would like to implement into this project is developing the covertfs into the TAILS operating system and having it run as a bootable program through the a flash drive. The reason for this is because the TAILS operating system in and of itself offers various security measures to ensure a stable and functioning system. We would like to develop a working prototype where our covertfs is integrated in the TAILS operating system to further allow confidentiality and plausible deniability to the users.

The original concept paper[2]

4.1 Encryption and Advanced Steganography Techniques

Another future implementation worth looking into is the use of a more advanced steganographic technique. The purpose of this is to ensure the confidentiality and plausible deniability of the users by:

- 1) Ensuring that pictures being used to hide the information do not give tell-tale signs of modification

- 2) To increase the difficulty of steganalysis tools discovering the encrypted pictures within the sea of publicly shared images within the file sharing site or social media site that the system is using to store the file system.

5 CONCLUSION

6 ACKNOWLEDGMENTS

The original Web-Based Covert File System Paper [2].

REFERENCES

- [1] Ronald E. Anderson, Deborah G. Johnson, Donald Gotterbarn, and Judith Perrolle. ACM code of ethics and professional conduct. *Communications of the ACM*, 36(2):98–107, 1993.
- [2] Arati Baliga, Joe Kilian, and Liviu Iftode. A web based covert file system. *HotOS*, 2007.
- [3] Clement Guitton. A review of the available content on Tor hidden services: The case against further development. *Computers in Human Behavior*, 29(6):2805–2815, 2013.
- [4] Kian-lee Tan. StegFS : A Steganographic File System Laboratories for Information Technology Department of Computer Science. i:657–667, 2003.