SEC 150 Assignment: Disk Encryption with Plausible Deniability

Titus Barik (tbarik@staff.waynecc.edu)

Version 1.0

1 Assignment Description

In class, we used TrueCrypt to create a simple, file-based encrypted disk volume.

In this assignment, you will again create a file-based encrypted disk volume. However, the disk volume that you create will have the property of "plausible deniability" through the hidden volume feature. The TrueCrypt documentation introduces this feature as follows:

> It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.[1]

That is, you will create a volume such that there are effectively two passwords that reveal different sets of data. The first password reveals some data that makes an adversary believe that they have found some secret information. Hopefully, the adversary will be satisfied and leave you alone. But this is just a decoy to fool the adversary. **It is the second password that actually unlocks the confidential data.**

2 Pre-Requisites

Before starting this assignment, watch the lecture video on TrueCrypt and install TrueCrypt.

3 Instructions

1. Extend the example given in class to create an encrypted file container as a hidden TrueCrypt volume.

[1] `http://www.truecrypt.org/hiddenvolume`

2. Name your TrueCrypt volume `lastname.tc`, where `lastname` is your last name in all lowercase.

3. Use the default Encryption Options (AES, and RIPEMD-160), with an outer volume size of 340 KB.

4. Give the outer volume a password of `outer`. In real life, you would use a different password, but this makes it possible for me to grade your assignment.

5. Open the outer volume, and add the file `nuclear_codes.txt` to it. Modify this file so that it contains your name somewhere in the file. Then, create a file called `MD5.txt`, where the name MD5 should be replaced with the actual checksum.

6. Now configure the inner volume, using the maximum recommended hidden volume size. Use a password of `inner`.

7. Mount the hidden volume (remember to use the correct password) and add the file `actual_nuclear_codes.txt`. Modify this file so that it contains your name somewhere in the file. Create a file called `MD5.txt`, where the name MD5 should be replaced with the actual checksum.

8. Verify that a different set of files is shown depending on the password that you use.

Now, under threat, you can pretend to reveal the password to fool the adversary, and the TrueCrypt volume is constructed so that there is no way for an adversary to know whether or not a hidden volume exists in the first place.

4 Milestone

Submit a screen capture demonstrating that TrueCrypt is installed on your system.

5 Submission

Submit the following file: `lastname.tc`. Be sure you use the passwords outlined in the assignment so that your work can be graded. Don't forget to compute the hashes for each of the submitted files and submit them within your TrueCrypt volume.