OpenPuff

Overview

- Introduction To OpenPuff
- What Does OpenPuff Do ?
- Major Functionalities
- Carrier Chaining
- Unique Features
- Lab Exercise
- References

Introduction To OpenPuff

- **OpenPuff Steganography and Watermarking**, sometimes abbreviated **OpenPuff** or **Puff**, is a freeware steganography tool for Microsoft Windows

- Created by Cosimo Oliboni and still maintained as independent software.

- The program is notable for being the first steganography tool (version 1.01 released on December

- It can provide more discretion than a conventional file encryption program by hiding the data into regular files rather them using a specific extension

What Does OpenPuff Do ?

- Allows you to hide data into encrypted files in order to send it to other users.

- Uses principles of steganography in order to hide the information into regular files such as images, audio or video files

- The carrier files can be transmitted by using emails, removable devices or other storage devices without arousing suspicion about the concealed message.

- This method aims to protect both the message and the persons that are exchanging the messages.

Major Functionalities

- lets users hide data in more than a single carrier file.

- When hidden data are split among a set of carrier files you get a carrier chain, with no enforced hidden data theoretical size limit.

- Implements 3 layers of hidden data obfuscation (cryptography, whitening and e ncoding)

- extends deniable cryptography into deniable steganography

Carrier Chains

Data is split among many carriers. Only the correct carrier sequence enables unhiding. Moreover, up to 256Mb can be hidden, if you have enough carriers at disposal. Last carrier will be filled with random bits in order to make it undistinguishable from others.

Carrier Formats Supported:

- Images (BMP, JPG, PCX, PNG, TGA)
- Audio support (AIFF, MP3, NEXT/SUN, WAV)
- Video support (3GP, MP4, MPG, VOB)
- Flash-Adobe support (FLV, SWF, PDF)

Unique Features

- (HW seeded random number generator (CSPRNG)
- Carrier bits selection level
- Modern multi-cryptography (16 algorithms)
- Multi-layered data obfuscation (3 passwords)
- X-squared steganalysis resistance
- Adaptive non-linear carrier bit encoding
- Multithread support (up to 16 CPUs)
- OpenSource core crypto-library (libObfuscate)

Lab Exercise

1. Install Openpuff in your System
2. Run Openpuff
3. Insert three separate passwords. Each password has to be different (at bit level) and at least 8 characters long
4. Add 3 different carrier files and shuffle those
5. Reset all bit selection level to normal
6. Hide a message and a decoy message into any carrier file

Lab Exercise

7. Now Unhide those hided
   - Typing twice the same password
   - Adding all the carriers in the right order
   - Setting all bit selection levels to the original value
   - Start the unhiding task.

8. Also show that Openpuff support **plausibly deniable encryption** by entering decoy password and extracting decoy message out of image

Output required

Create a ROLLNUMBER_Op.zip from a ROLLNUMBER_Op directory. The directory should contain files including

- Screen shots of
  - Openpuff window after steps 1 to 8
  - Task Reports
    - Hiding Secret and Decoy Messages
    - Unhiding Secret Message
    - Unhiding Decoy Message
- A readme.txt file specifying what each of these files are

References

- Wikipedia
- http://en.wikipedia.org/wiki/OpenPuff

- User guide-
http://embeddedsw.net/doc/OpenPuff_Help_EN.pdf

- Download
embeddedsw.net/OpenPuff_Steganography_Home.html

- Review
http://www.pcworld.com/article/2026357/review-openpuff-steganography-tool-hides-confidential-data-in-plain-sight.html