Data Hiding in the SWF Format and Spreading through Social Network Services

A. Zaharis, A.I. Martini and C. Ilioudis

Department of Computer & Communication Engineering University of Thessaly,
Technological Educational Institute of Thessaloniki, Greece
e-mail: alzahari@inf.uth.gr, admartin@inf.uth.gr, iliou@it.teithe.gr

Abstract

This paper presents a unique way of hiding information inside the SWF Adobe® Flash® Format. SWF has become popular because of its interaction with the end user along with its captive graphics. Furthermore it is massively used by social networks for entertainment reasons (flash games, presentations), as it is easily embedded in web pages. Adobe ® Flash ® Player is used by over 2 million professionals and reaching 99.0% of Internet-enabled desktops. The fact that SWF is so popular and can be found in large scale around the Internet, along with the fact that most SWF applications developed look innocent, make the SWF format a great carrier medium for hidden information to be spread without raising any questions. For the first time, a method consisting of different hiding techniques is presented in order to fully illustrate the potentials of hiding data in the SWF format and spreading them through social network services. This technique can be utilized in order to understand the danger of not thoroughly examining SWF format in a forensics investigation, while allowing the development of a sufficient detection method of possible illegal activity, like child pornography, through Social Networks.

Keywords

SWF format, Data Hiding, Social Network Services, Computer Forensics.

1. Introduction

Data hiding in different file formats has been presented over the last years along with sufficient detection methods. The fact that WEB 2.0 has evolved, led to the large popularity of social network services and the need for less common multimedia medium to become popular. The need of interactive web pages made Flash Technology (SWF) a necessary tool, yet less examined for its possibilities as a hidden information medium. Furthermore, the fact that the majority of internet users nowadays uses social network services, lead to the exchange of large quantities of information some of which is believed to be illegal. In an attempt to present the lack of security and inability of hidden information detection on social network services, we are going to utilize a popular multimedia format SWF, in order to spread hidden information thought social networks such as FaceBook® and MySpace®. Text files, images, video and executable files can be distributed, hidden inside plain SWF files using various hiding techniques some of which can be easily replicated by novice computer users.

The contribution of this paper to the forensics community concentrates on the presentation of an out of the box information hiding and spreading technique that can become easily popular and at the same time dangerous.

2. The SWF format

The SWF file format stands for "ShockWave Flash", a partially open repository for multimedia and especially for vector graphics, originated with FutureWave Software and has come under the control of Adobe. Intended to be small enough for publication on the web, SWF files can contain animations or applets of varying degrees of interactivity and function. Originally limited to presenting vector-based objects and images in a simple sequential manner, the format in its newer versions allows audio, video and many different possible forms of interaction with the end-user. Once created, SWF files can be played by the Adobe Flash Player, working either as a browser plug in or as a standalone player. SWF files can also be encapsulated with the player, creating a self-running SWF movie called a "projector". Based on an independent study conducted by Millward Brown, over 99% of web users now have an SWF plugin installed, with around 90% having the latest version of the Flash Player.

3. Social Network and Illegal Communities

A *social network service* focuses on building online communities of people who share interests and/or activities, or who are interested in exploring the interests and activities of others. Most social network services are web based and provide a variety of ways for users to interact, such as e-mail and instant messaging services.

The social network services selected in order to prove the validity of this work, where chosen due to their popularity and with no intense of harming their credibility in any way. Similar techniques can be used in every social network service supporting SWF file format uploads.

3.1. Illegal Communities

Illegal communities have been reported to perform inappropriate activities utilizing social networks. Such activities include organizing, spreading ideas, exchanging documents and finding new members. Illegal groups are capable of using secret methods of exchanging information through social networks due to the fact that there is access for everyone, anonymity and large amount of legitimate traffic to use as a cover.

While terrorism is certainly one of the more dangerous uses of data hiding that face the world today, there are other groups, both good and bad, who could use social networks and data hiding, to keep their communications secret, including: *Intelligence services, Corporations with trade secrets to protect, Organized crime, Drug traffickers, Money launderers, Child pornographers, Weapons traffickers,*

Criminal gangs, People concerned about government eavesdropping, People who have to circumvent restrictive crypto laws.

4. Proposed Data Hiding Techniques

A number of techniques are going to be introduced, some of which can be performed by an average computer user, while for more elaborate ones, advanced knowledge is needed. To present these techniques an innocent 2D flash game, *("TalkmeInto.swf"),* was developed containing both attacks later discussed.

4.1. Data hiding Technique 1

Type: "Hiding inside unread SWF key frames"

File types hidden: ai, png, bmp, jpeg, emf, gif, wmf, pct, qtif, tga, tiff, wav, mp3, aif, mov, avi, mpeg, flv, wmv.

Description: In order to perform this easily detected technique, one should have basic knowledge of Flash development. This attack can be performed in any version of Adobe Flash. To achieve it a secret file, in our example a picture, can be places in a frame or frames that are not going to be accessible by the gamer or the user of the flash application. This frame can exist in the "main stage" or "Level0" of the flash application or inside a "Movie clip Instance" making it more difficult to be detected.

In an example flash game, a secret image ("papergirl.jpg") is hidden inside Movie Clip Instance "*back*" -> Layer4 -> Frame2, *fig.1*.

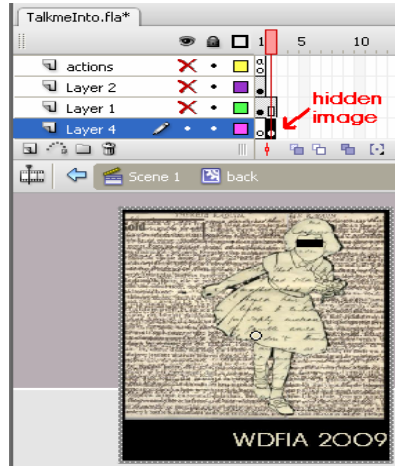

Figure 1: papergirl.jpg hidden inside an inaccessible Movieclip

The flow of the game is deliberately ignoring this frame in every occasion, making it impossible for a user to visually locate the hidden image. This method can be used in order to hide different file formats in more than one place inside the same SWF file. The SWF file size becomes bigger every time a secret file is hidden and may raise suspicions. The receiver must:

Step1: Decompile the SWF file, using a commercial or free SWF decompiler in order to list all the resources embedded. Step2: Browse the graphic resources, locate and save the previously invisible "papergirl.jpg".

This steganalysis attack can be described as *visual attack* and can be performed by investigators unfamiliar with the SWF format.

4.2. Data hiding Technique 2

Type: "Mp3 steganography imported in SWF files"

File types hidden: All file types

Description: In order to perform this data hiding technique the following steps must be made:

Step1: Choose a file (all file types supported) in order to be hidden.

Step2: Choose an mp3 file as your stego-carrier file.

Step3: Use steganography tools to hide information inside the stego-carrier file.

Step4A: Manually import the stego-carrier mp3 file inside an SWF file.

Step4B: Automatically import the stego-carrier mp3 file inside an SWF file using java code presented later (*par. 4.4*).

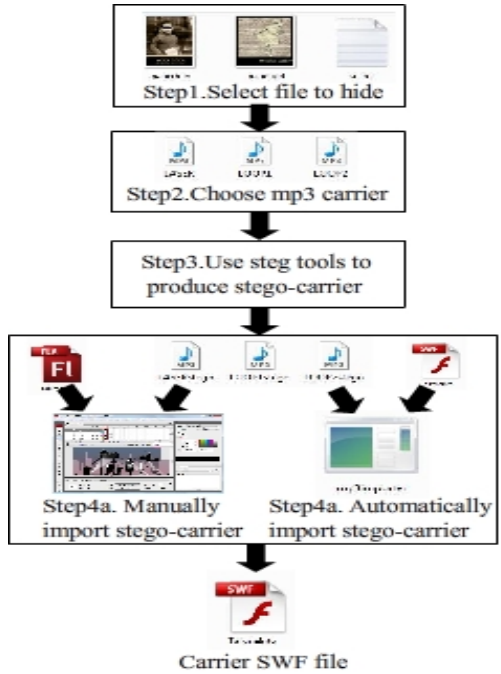

Figure 2: Data hiding Technique 2

The receiver must:

Step1: Decompile the SWF file, using a commercial or free SWF decompiler in order to list all the resources embedded.

Step2: Browse the audio resources, view and save the stego-carrier mp3 file.

Step3: "Tweak" the saved mp3 file in a proper way (optional step).

Step4: Apply inverse steganography (extraction) in order to obtain the secret file.

4.3. Why does Data Hiding Technique 2 work?

Adobe Flash can embed different kinds of file formats inside an SWF file. The formats supported on Adobe Flash CS3 used for testing purposes are: ai, png, bmp, emf, jpeg, gif, wmf, pct, qtif, tga, tiff, wav, mp3, aif, mov, avi, mpeg, flv, wmv.

After exhaustively embedding and retrieving secret information using different steganography algorithms best fitting the given format the following results where extracted (*Table I*).

File Type	Steganography Algorithm	Software Used	Results
ai, emf, wmf, pct, qtif, mpeg, flv, aif, wmv, avi, png, mov	Fuse	Camouflage 2.0	Failed
jpeg	LSB, Fuse	Jsteg , Camouflage	Failed
bmp	LSB, Fuse	Steghide, Camouflage	Failed
gif	LSB, Fuse	S-tools , Camouflage	Failed
Tga, tif	LSB, Fuse	StegoTif , Camouflage	Failed
wav	LSB, Fuse	Steghide, Camouflage	Failed
mp3	LSB, Fuse	Mp3stego , Mp3Stegz , Camouflage	***Success***

Table 1: Results

These results can be explained by the fact that all file formats imported in Flash libraries are automatically compressed in order for the medium to be reduced in size. Even in cases of jpeg or bmp imported files where the Flash developer has the option not to compress files, the embedded files are altered in such a way that retrieval of hidden data from steganography is impossible. The only format not radically altered is the mp3 format. This fact can be exploited in order to use steganography on an mp3 file and then embed it inside an SWF file.

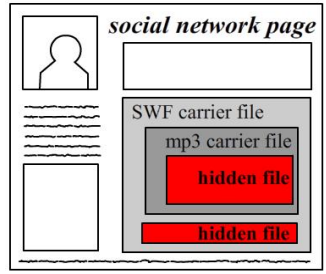

Figure 3: Illustration of both embedding techniques

4.4. Automatic mp3 importing

In order to simplify the process of embedding an mp3 file inside an SWF file, a JAVA program was developed, utilizing an open source flash manipulation library. By developing such a program, a common user can input an SWF file and a stego-carrier mp3 file and the "mp32swfembedder.java" would export a new SWF with the mp3 stego-carrier file used as the background sound of the SWF movie. This way a

user unfamiliar with Flash development could easily embed a stego-carrier file inside any SWF already publicly distributed via the internet.

4.5. Receivers Tweaking

During data hiding technique 2, receivers Step 2, the mp3 stego-carrier file saved, is slightly altered causing the Camouflage 2.0 to fail unveiling the hidden information. This is caused due to a few bytes added at the end of the mp3 file recovered, exactly after the spot where the information hidden by the Camouflage 2.0 steganography tool, reside. This fact does not affect the use of the Mp3stego or Mp3Stegz during reverse steganography. In order to resolve this problem extra bytes added can be removed using any hex editor.

Figure 4: Mp3 file with extra bytes marked

5. Spreading Hidden Data With SWF Files

Hidden data inside SWF files can be easily spread through the internet. The fact that any SWF file can be manipulated in order to contain hidden information along with its great popularity, make the SWF format a great hiding medium. A simple process can be followed by a subject in order to spread hidden information using the above mentioned techniques through social networks.

5.1. Spreading Technique

In order to spread a stego-carrier SWF file <S>, one must perform the following general steps:

Step1: Upload stego-SWF file <S> on an anonymous web-server or a SWF hosting service without unveiling his IP address

Step2: Obtain the URL link directing to the SWF file <S

Step3: Create an anonymous email account <E> in order to use it to register on social network websites

Step4: Register with fake identity to the social networks which are going to be used to spread hidden information

Step5: Use special applications or html code in order to embed SWF file <S> to a profile page or group pages or other user pages

Step6: Invite/inform secretly other users of the hidden information existence.

The above mentioned technique can be more successful if the owner of the fake social network's profile acts as a legitimate user (ex. adding friends, playing games, commenting, chatting). Due to the lack of detection methods and high volume of data exchanged through social networks suspicions are definitely not going to be raised.

5.2. Examples

In order to present a real life application of the above mentioned spreading technique, a stego-carrier SWF game (*"TalkmeInto"*), containing hidden information is going to be uploaded in public view through the two more popular social networks. The game contains two secret JPEG pictures hidden using Hiding Techniques 1 & 2 previously presented. The total size of the hidden files is 127,2 Kb while the total size of the game is 548 Kb.

5.2.1. Facebook

Third party applications exist in order to post SWF files inside a users profile but we are going to present the native Facebook flash player approach. A user can create a page containing a Flash Player box. Using the Flash Player application a user can upload the SWF file on a Facebook hosting server. The SWF file is then previewed inside the page created, along with other information added by the administrator/creator. A basic step in order to make the secret transaction more secure and less suspicious is to attract legitimate users that are going to actually play the uploaded game not being aware of the underlying hidden information. The *TalkmeInto* public page was created as a proof of concept and can be accessed through the following URL: *http://www.facebook.com/home.php#/pages/TalkmeInto/74719738815* or for direct SWF access here: *http://photos-b.ak.fbcdn.net/photos-ak-snc1/genericv2b/284/81/01AwcA9kYVM5kAfakKAAAAE WWku78:.swf*

5.2.2. Myspace

In order to post links to SWF files anywhere inside a Myspace profile simple html embedding code is used. The SWF file must first be uploaded on a third party server. Links to SWF files can also be posted as comments to any users profile during a conversation making hiding information really easy to spread. A fake Myspace profile containing the "*TalkmeInto"* SWF game can be accessed through the following URL: *http://www.myspace.com/458277409*

6. Proposed Detection Methodology

To safely detect hidden information inside SWF files during a forensics investigation, the following process must be followed:

Step1: Locate/download suspicious SWF file

Step2: Calculate SWF files hash value

Step3: Decompile the SWF file, using a commercial or free SWF decompiler in order to list all the resources embedded

Step4: Manually inspect every file resource for suspicious files or evidence. (“visual attack

Step5: Check actionscript used by the SWF, to locate suspicious text messages or textual evidence (ex. URL, passwords

Step6: Collect mp3 files embedded

Step7: Analyze all mp3 files to identify steganography using steganalysis tools

Step8: Extract hidden data / evidence.

The proposed methodology can safely detect both data hiding techniques previously described.

7. Future Work & Conclusions

The contribution of this paper to the Forensics community concentrates on the presentation of a new, less common process of data hiding information, using SWF format as a cover medium while providing a detection technique. Extra effort is made in order to highlight the dangers of not thoroughly examining data uploaded and spread thought popular social networks. Through this paper, SWF format becomes a popular data hiding medium that must be thoroughly examined during any Forensics Investigation.Future work:

- A detection tool must be developed in order to automatically detect steganography contained inside SWF files.
- A specific policy must be described, as far as the content embedded and shared by social networks is concerned.

By both improving the method and the software implementing it, a new powerful detection tool will be produced, that can be used by forensic investigators in order to detect hidden files inside the SWF format and social network administrators in order to prevent illegal activities through their websites.

8. References

Adobe Systems (2008), "Flash Player Penetration: Flash content reaches over 98 percent of Internet viewers", http://www.adobe.com/software/player_census/flashplayer

Adobe Systems (2008), "The History of Flash: The Dawn of Web Animation", http://www.adobe.com/macromedia/events/john_gay/page04.html

Adobe Systems (2008), "SWF File Format Specification Version 10", http://www.adobe.com/devnet/swf/pdf/swf_file_format_spec_v10.pdf

Flagstone Software Ltd. (2008), http://www.flagstonesoftware.com/transform/

Fraser, M. and Dutta, S. (2008), "Throwing Sheep in the Boardroom: How Online Social Networking Will Transform Your Life, Work and World:, *Wiley*, http://books.google.com/books?id=SP92NwAACAAJ

Greek Forensics Community, http://greekforensicscommunity.blogspot.com/2009/04/mp3-2-swfembedder.html http://sites.google.com/site/greekforensicscommunity/Home/talkmeinto.rar

Herald and Weekly Times (2008), "MySpace exposes sex predators", http://www.news.com.au/heraldsun/

Kipper, G. (2004), *"Investigator's Guide to Steganography", ISBN:0849324335, Auerbach Publications © 2004*

Mangu-Ward, K. (May 2009), "Enhancing Child Safety and Online Technologies", Internet Safety Technical Task Force, 2008 (published 31 December 2008), http://cyber.law.harvard.edu/pubrelease/isttf/