ARTICLE:

HIDING ILLEGAL CONTENT IN THE SWF FORMAT AND SPREADING THROUGH SOCIAL NETWORK SERVICES: A LEGAL APPROACH

By **Alexandros Zaharis, Adamantini I. Martini, Christos Ilioudis** and **Michael Rachavelias**[1]

Introduction

It is possible to hide data or illegal content in different file formats. The evolution of web 2.0 has led to the popularity of social network services, and the exchange of large quantities of information. Web pages would not be as interactive without flash technology. However, flash technology has not been examined widely for its possibilities as a medium for the transmission of hidden information. This article will illustrate how flash technology can be used to disseminate hidden information through the most popular social networks. Text files, images, video and executable files can be distributed, hidden inside plain flash files using various techniques to hide a message, some of which can be easily replicated by novice computer users. This article focuses on cases concerning abusive images of children that are exchanged through publicly accessible social networking web sites by hiding the images, and the legal issues and ramifications of this act.

There are a number of techniques that can be used to hide data that are discussed below.

Data hiding technique 1

Data can be hidden inside SWF key frames that are not read by the computer's software. (SWF is the 'Shockwave Flash' format that enables the use of vector graphics in multi-media applications (vector graphics is a terms used to denote the use of geometrical shapes and points, lines and curves, all of which are based on mathematical equations, to represent images in computer graphics)). SWF files are intended to be small enough to allow ease of publication on the web, and they can contain animations or applets that vary in respect of their interactivity and function, such as enabling the use of audio, video and other forms of interaction with the end-user. Once a SWF file had been created, they can be played by the Adobe Flash Player. The file types that can be hidden include: ai, png, bmp, jpeg, emf, gif, wmf, pct, qtif, tga, tiff, wav, mp3, aif, mov, avi, mpeg, flv, wmv.

This method of hiding data can be performed in any version of Adobe Flash. To hide the data in a game (a secret file – for instance, a picture), can be placed in a frame or a number of frames that are not going to be available to the user of the flash application. This frame can exist in the "main stage" or "Levelo" of the flash application, or inside a "Movie clip Instance", thus making it more difficult to be detected. In an example flash game, a secret image ("papergirl.jpg") is hidden inside a Movie Clip *"back"* ⇢ Layer4 ⇢ Frame2, as in figure 1.

[1] *This article is partly taken from a previous work by Alexandros Zaharis, Adamantini I. Martini and Christos Ilioudis, 'Data Hiding in the SWF Format and Spreading through Social Network Services', presented at WDFIA 2009 (Workshop on Digital Forensics & Incident Analysis).*

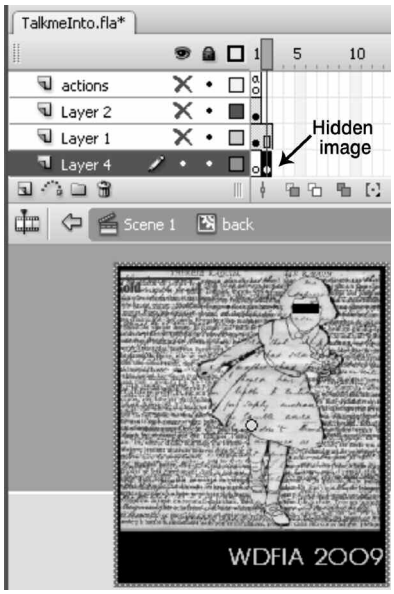

Figure 1: 'papergirl.jpg' is hidden inside a Movie clip

The flow of the game deliberately ignores this frame on every occasion, making it impossible for a user to visually locate the hidden image. To oversimplify this process through an every day example, if a flash application was a movie film with a hidden image on its last frame, then it would end one frame before the full length. The hidden frame is present in the hard copy of the film but is never transmitted to the audience. This method can be used in order to hide different file formats in more than one place inside the same SWF file. However, the SWF file size becomes bigger every time a secret file is hidden, and may raise suspicions.

Data hiding technique 2

The second technique that can be used to hide data is known as "Mp3 steganography imported in SWF files". In this instance, the file types that can be hidden cover all file types.

In order to perform this data hiding technique, an experienced user has to choose a file to hide (in our case abusive images of a child). They then choose an mp3 file as a "stego-carrier" file (that is, a file that will be used to hide the image). In turn, a steganography tool must be used to hide the data comprising the image inside the stego-carrier file. Once this operation is complete, the user has two options: either to manually import the stego-carrier mp3 file inside an SWF file, or automatically import the stego-carrier mp3 file inside an SWF file using java code (which is discussed later in the article).

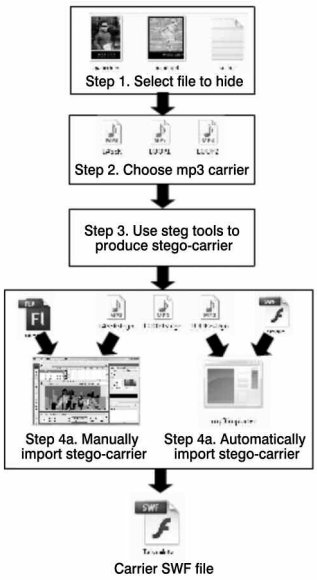

Figure 2: Data hiding technique 2

When the receiver receives the file knowing an image is hidden, they must first decompile the SWF file, using a commercial or free SWF decompiler in order to list all the resources set into the file, then browse the audio resources, then view and save the stego-carrier mp3 file. They then have the option to "tweak" the mp3 file they have saved in a proper way, before applying inverse steganography (extraction) in order to obtain the secret file.

Tweaking

During data hiding technique 2, when the mp3 stego-carrier file saved, it 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 that is recovered, exactly after the spot where the information, hidden by the Camouflage 2.0 steganography tool, resides. This fact does not affect the use of the Mp3stego or Mp3Stegz during reverse steganography. In order to resolve this problem, any extra bytes that have been added can be removed using

any hex editor.

Figure 3: Mp3 file with extra bytes marked

This particular data hiding technique works with an mp3 file because Adobe Flash can enclose different kinds of file formats inside an SWF file. The formats supported on Adobe Flash CS3 used for testing purposes are as follows: ai, png, bmp, emf, jpeg, gif, wmf, pct, qtif, tga, tiff, wav, mp3, aif, mov, avi, mpeg, flv, wmv. In preparing the paper presented at WDFIA 2009, the authors exhaustively tested the embedding and retrieving of secret information using different steganography algorithms that best fitted the given format. Only the mp3 file format could be used successfully. This result 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.

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, an ordinary user can place an stego-carrier mp3 file into an SWF file. In this way, a user who is not familiar with Flash development could easily inset a stego-carrier file inside any SWF already publicly distributed via the internet after downloading it. The automation of this process can lead to an increase of its use by every day users.

Distributing 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, together with its great popularity and innocent content, make the SWF format a useful medium for hiding data. Furthermore, while playing a Flash game, the browser automatically downloads the SWF file and stores it. This automatically causes every person downloading a flash game that includes such hidden files to become a possible recipient of abusive images of children while being unaware of the existence of the hidden content inside the SWF game. This fact can, if the prosecution fails to consider this carefully, be exploited by an accused person, in order to claim ignorance of the existence of the hidden content, thus making difficult to validate such evidence.

It is simple process to spread hidden information using the techniques mentioned above through social networks. A false e-mail address, together with a sham social network profile acting as a legitimate user are all the ingredients needed in order to start spreading illegal content. Because of the lack of detection methods and high volume of data exchanged through social networks, suspicions are rarely raised.

Distribution technique

In order to spread a stego-carrier SWF file 'S', it is necessary to perform the following general steps:

Step 1: Upload stego-SWF file 'S' on an anonymous web-server or a SWF hosting service without unveiling the IP address.

Step 2: Obtain the URL link directing to the SWF file 'S'.

Step 3: Create an anonymous e-mail account 'E' in order to use it to register on social network websites.

Step 4: Register with the social networks using a sham identity which will be used to spread the hidden information.

Step 5: Use special applications or html code in order to embed SWF file 'S' to a profile page or group pages or other user pages.

Step 6: Secretly invite or inform other users of the existence of the hidden information.

The above mentioned technique can be more successful if the owner of the fake profile acts as a legitimate user (for example, by adding friends, playing games, commenting, chatting and such like). Due to the lack of detection methods and high volume of data exchanged through social networks, it is not likely that suspicions will be raised.

An example: a publicly available profile

The distribution technique set out above is illustrated by indicating how a stego-carrier SWF game ("TalkmeInto"), containing hidden information is to be uploaded, in public view on popular social networks. The game contains two secret JPEG pictures containing Fake Child Pornography, hidden using the two hiding techniques described above. The total size of the hidden files is 127,2 Kb while the total size of the game is 548 Kb.

Facebook

Third party applications exist in order to post SWF files inside a users profile, but this article will illustrate how to includea file in the native Facebook flash player. 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, together with other information added by the administrator or 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, who are not aware of the underlying hidden information

Myspace

In order to post links to SWF files anywhere inside a Myspace profile, simple html embedding code can be used. The SWF file must first be uploaded on to a third party server. Links to SWF files can also be posted as comments to any users profile during a conversation, thus making hiding information really easy to disseminate.

Third party applications exist in order to post SWF files inside a users profile along with a native flash player. A user can create a page containing a Flash Player box. Using the Flash Player application, a user can upload the SWF file on the social networks hosting server. The SWF file is then previewed inside the page created, together with other information added by the administrator or 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 or distribute the game that is uploaded, and who are not aware of the underlying hidden information.

Legal issues

It is possible for an ignorant or innocent user to unknowingly install a seemingly innocent game on their computer, yet the data might contain illegal content (such as abusive images of children) that has been installed without their knowledge in the hard drive – content that can be easily found by a digital evidence specialist if conducting a forensics investigation. The legal issues raised in such a case are relatively easy to understand, but can be difficult to deal with. For example, in the case of distributing child pornography, Greek law requires intention for the accused to be convicted, as set out under article 348A of the Greek Penal Code:

Article 348A Penal Code: Child Pornography

1. Whoever intentionally produces, distributes, publishes, demonstrates, imports or exports, transports, offers, sells or by any other means disposes, buys, acquires or possesses child pornography material or disseminates or transports information relevant to the conduct of the above mentioned actions, faces the penalty of at least 1 year imprisonment and a financial penalty of up to 100,000 Euros.

2. Whoever intentionally produces, offers, sells or by any other means disposes, buys, acquires or possesses child pornography material or disseminates or transports information relevant to the conduct of the above mentioned actions with the use of a personal computer or by the use of Internet, faces the penalty of at least 2 years imprisonment and a financial penalty of between 50,000 Euros to 300,000 Euros.

3. Child pornography content, for the meaning of previous paragraphs, is the reproduction or the real or virtual impression in electronic or other material of an underage person's body or part of his body, in such a way that self-evidently causes sexual stimulation, and any other real or virtual indecent (licentious) action by or with an underage child.

4. The penalty of incarceration for up to 10 years is imposed for the actions of paragraphs 1 and 2,

a) if they were conducted by profession and repetitious, b) if the production of the child pornography is connected to the exploitation of a minor's need or his mental or psychic disease or corporeal illness or with the exercising of violence

or threat of exercising violence or with the exploitation of a minor that is under 14 ears of age.

If the actions of paragraph b1 have inflicted heavy damage to health, the sanction imposed is incarceration of at least 10 years and a financial penalty of between 100,000 Euros to 500,000 Euros; if the outcome is death, life imprisonment is imposed.

In Greek law, premeditation is a prerequisite, and it has been held[2] that eventual fraud is also enough for a conviction, providing the eventual fraud covers[3] the knowledge and the will to create, circulate and distribute the illegal content. Proof of intention is always difficult, and the burden of proof lies with the prosecutor, so technical evidence that the accused is aware of the images, for instance, must be shown if the prosecutor is going to demonstrate intent.

Furthermore, the prosecution also needs to demonstrate the procedural problem of integrity and authentication, both of the evidence and the process of obtaining the evidence. This is illustrated by Mason (excluding footnotes):[4]

'Issues that may need to be covered and tested include demonstrating the provenance of the source of the data, how it is authenticated, indicating the process by which the data were acquired, and proving the continuity and reliability of the evidence. In essence, the requirements for authentication can be reduced to the following:

(a) The data (both the content and associated metadata) that a party rely upon have not changed (or if the data have changed, there is an accurate and reliable method of recording the changes, including the reasons for any such changes) from the moment they were created to the moment they were submitted as evidence.

(b) As a corollary to (a) above, it is necessary to demonstrate a continuity of the data not being altered between the moment the data were obtained for legal purposes and their submission as an exhibit.

(c) As a corollary to (b) above, it should be possible to test any techniques that were used to obtain and process the data.

(d) The data can be proven to be from the purported source.

(e) The technical and organisational evidence demonstrates the integrity of the data is trustworthy, and is therefore considered to be reliable.'

Unless the authorities have good reason for suspecting a person has actually committed a crime, an investigation (and possible prosecution) cannot take place.

Future work and conclusions

From a technician's point of view, it will be useful to develop a detection tool in order to automatically detect steganography contained inside SWF files. In addition, consideration should be given by social networks to drafting a specific policy relating to this issue. 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 web sites. This will protect not only web sites and social networks in preventing the hosting of illegal content in their servers (content that they might not be aware that they are hosting) but will also protect their legitimate users.

The main legal issues relating to data hiding, as described above, have to deal with: identifying the intention of the user, the differences in jurisdictions, the handling of digital evidence and, in some jurisdictions, the privacy of the data. A significant problem relates to the fact that data might be located in various jurisdictions, and this poses practical difficulties for those investigating crimes, as well as deciding where legal action should be commenced. There is, arguably, a need for countries to follow a common direction and adopt similar cyber crime laws. It is true that a number of local and global initiatives have been taken, but the road to a universal consensus is still very far away. The

[2] *1145/2008 Supreme Penal Court, 628/2006 Supreme Penal Court.*

[3] *The definition of fraud has various classifications in the Greek legal system. The term 'eventual fraud' [dolus eventualis] exists when the offender predicts that his actions can produce the delinquent result and, nevertheless, he still continues his actions, and by so doing he accepts the production of the criminal result.*

[4] *Stephen Mason, general editor, Electronic Evidence (LexisNexis Butterworths, 2nd edn, 2010), 4.25.*

problem is, that criminal activities over the internet can be conducted in countries where no cyber criminal laws apply, and the problem is not only the differences between different legal systems. Cyber crime law is not a static law; it evolves every day and this makes developing and implementing laws difficult. In Greece, for example, a unified law that applies to cyber crimes does not exist. At present, acts that concern activities conducted in the physical world also apply to crimes committed over the internet crimes by analogy with laws already in place.

Furthermore, the procedural problem of integrity and authenticity, both of the evidence and the process itself remains relevant. The quest for such evidence is in the hands of law enforcement authorities, and such evidence should be handled appropriately.

Alexandros Zaharis
Alexandros Zaharis holds a Bachelor (2007) in Computer Engineering and Telecommunications and an MSc (2010), in Computer Science, from the Computer Engineering, Telecommunication and Networks Department, University of Thessaly, Greece. His interests include Computer Forensics, Network Security and RFID technology.

alzahari@uth.gr

Adamantini I. Martini
Adamantini I. Martini holds a Bachelor (2007) in Computer Engineering and Telecommunications and an MSc (2010), in Computer Science from the Computer Engineering, Telecommunication and Networks Department, University of Thessaly, Greece. She joined the Centre for Research and Technology, Thessaly in 2007 as a researcher on RFID technology.

dimart@uth.gr

Christos Ilioudis
Christos Ilioudis BSc, PhD is an Assistant professor in the Informatics Department, ATEI Thessaloniki. He teaches information systems security in the ATEI of Thessaloniki. His research interests include Internet security, information systems security, and digital forensics. He is a member of the Hellenic Computer Society, the IEEE and ACM.

iliou@it.teithe.gr

Michael G. Rachavelias is a member of the editorial board