Modern Applied Science; Vol. 6, No. 11; 2012
ISSN 1913-1844 E-ISSN 1913-1852
Published by Canadian Center of Science and Education

Detection of Steganographic Messages in Email Attachment

Mohd Hazali Mohamed Halip[1], Mohd Afizi Mohd Shukran[1], Omar Zakaria[1] & Syed Nasir Alsagoff Syed Zakaria[1]

[1] Department of Computer Science, Faculty of Defence Science and Technology, Universiti Pertahanan Nasional Malaysia, Kuala Lumpur, Malaysia

Correspondence: Mohd Hazali Mohamed Halip, Department of Computer Science, Faculty of Defence Science and Technology, Universiti Pertahanan Nasional Malaysia, Kem Sungai Besi, Kuala Lumpur 57000, Malaysia. E-mail: hazali@upnm.edu.my

Received: January 12, 2012 Accepted: August 15, 2012 Online Published: October 25, 2012

doi:10.5539/mas.v6n11p29 URL: http://dx.doi.org/10.5539/mas.v6n11p29

Abstract

Steganography is defined as the art and science of hiding message in a communication medium. The ease of use in steganography and the ability to make detecting steganography files difficult have led to the rise in their use in the Internet as one of a secret communication between two parties. There is also a fear that terrorist organisations are using similar technology to secretly communicate with one another. Email that contains the files embedded with hidden information using steganography can be very difficult to detect. One possible way to overcome this problem is by running a detection system that would analyse for any steganographic message which has been sent through email within the network. This paper presents a steganography detection system which captures all the Simple Mail Transfer Protocol (SMTP) transactions that has been established to an email server. It then runs a steganography test in order to detect steganographic message in images files attached to a particular email. Once detected and stored to a database, the system will then extract the hidden message to reveal the message.

Keywords: steganography, steganalysis, information hiding, steganography detection

1. Introduction

Steganography has been an important subject since the rise of Information Technology especially with the introduction of Internet. Steganography is the art and science of hiding communication (Provos & Honeyman, 2003). It is a technique of hiding secret messages inside image and audio files. Steganography derives from Greek's word and it means "concealed writing". It hides the message being exchanged in such a way that is undetectable under traditional packet analysis. The ease of use in steganography and the ability to make detecting steganography files difficult has lead to the rise in their use in the Internet as one of a secret communication between two parties. There is also a fear that terrorist organisations are using similar technology to secretly communicate with one another. Thus, this technology has become a threat to the information security over the Internet.

With steganography, one can send messages without anyone having to know of the existence of the communication. Email that contains the files embedded with hidden messages using steganography can be very difficult to detect. Those with a normal packet sniffer would only see an image or music file go by. In order for someone to detect it, the use of the publicly available tools that can detect the movement and types of traffic on the network may be useful. These detection tools can help network administrators to obtain an understanding of traffic within their network. In doing so, this can assist them in detecting any type of irregularity such as the presence of large images through emails around the network. The network administrator then can further investigate and take action on it.

To counter this new security threat and to assist the administrators, we had developed a system called Steganography Sniffer (Stegasniff) that monitor the email messages for image files that have been steganographically modified by publicly available software (Mohd Hazali Mohamed Halip & Mohd Lazim Abdul Raoh, 2009). Stegasniff (as shown in Figure 1) is a system that would be able to discover hidden messages sent through Internet that may be placed on the email attachment. Once detected over a Local Area Network (LAN) and stored to a database, the system will then extract the hidden message to reveal the message. Our work focuses on image file as it is the most widely used media to transmit hidden messages and also of the popular files to be attached in an email. The focus of our work is also on JPEG images since this image type is commonly used on Internet.

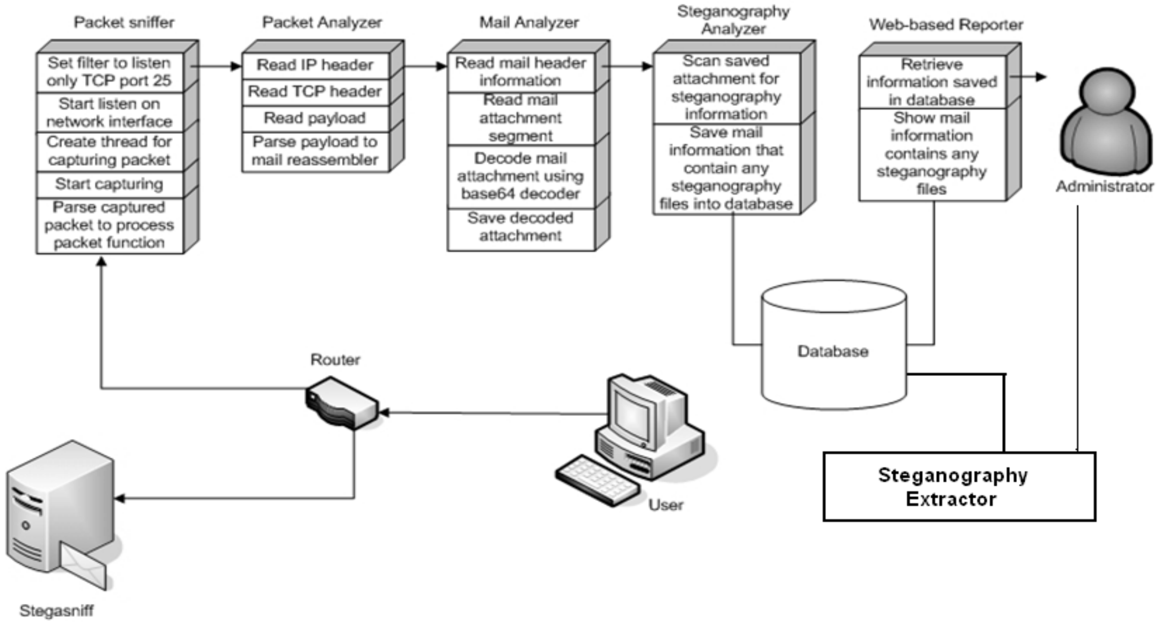

Packet sniffer
Set filter to listen only TCP port 25
Start listen on network interface
Create thread for capturing packet
Start capturing
Parse captured packet to process packet function
Packet Analyzer
Read IP header
Read TCP header
Read payload
Parse payload to mail reassembler
Mail Analyzer
Read mail header information
Read mail attachment segment
Decode mail attachment using base64 decoder
Save decoded attachment
Steganography Analyzer
Scan saved attachment for steganography information
Save mail information that contain any steganography files into database
Web-based Reporter
Retrieve information saved in database
Show mail information contains any steganography files
Administrator
Database
Router
User
Steganography Extractor
Stegasniff

Figure 1. Stegasniff over a Local Area Network (LAN)

The remainder of this paper is organised as follows: the introductions of steganography and steganalysis tools, a brief description of emails' protocol and encoding, the architecture and modules of Stegasniff and finally the conclusion of the paper.

2. Steganography Tools

Presently, there are many steganography tools for hiding data in images files (Johnson & Jajodia, 1998). Some of the tools available on the Internet that can hide messages in JPEG images are:

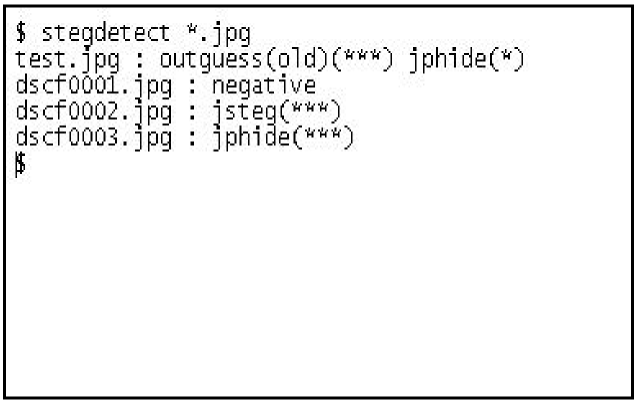
i. Jsteg
ii. JPHide
iii. Invisible Secrets
iv. Outguess 0.13b
v. AppendX
vi. Camouflage

The methods used by the tools to hide information in images includes least significant bit insertion (Lee & Chen, 2000), masking and filtering, algorithms and transformations (Johnson & Jajodia, 1998).

3. Steganalysis

Steganalysis is a process of detecting and extracting steganographic messages. The main objective of steganalysis is to identify the suspicious steganographic files. Currently, there are two extreme techniques used in steganographic detection (Chandramouli & Subbalakshmi, 2004) which are (a) little or no statistical assumptions about the image under investigation. Statistics are learnt using a large database of training images and (b) a parametric model is assumed for the image and its statistics are computed for steganalysis detection. Each of these techniques has pros and cons. Therefore, it is up to the user to choose an appropriate methodology based on the amount of side information that is available earlier.

There are several steganalysis tools that can be used on the Internet to find hidden messages. These tools could determine which steganographic tools were used to embed the messages onto the image. One of the tools is Stegdetect. It is a tool that analyse JPEG images for steganographic message. It is able to detect several different steganographic techniques and methods to embed hidden messages in JPEG images. Stegdetect can detects images that have hidden messages with Jsteg, JPhide and OutGuess. The output from Stegdetect may contains the lists of steganographic images. Stegdetect shows the level of confidence of the detection with one to three asterisks. Figure 2 shows some output from Stegdetect. Stegdetect is used as one of the modules in our Stegasniff.



```
$ stegdetect *.jpg
test.jpg : outguess(old)(***) jphide(*)
dscf0001.jpg : negative
dscf0002.jpg : jsteg(***)
dscf0003.jpg : jphide(***)
$
```

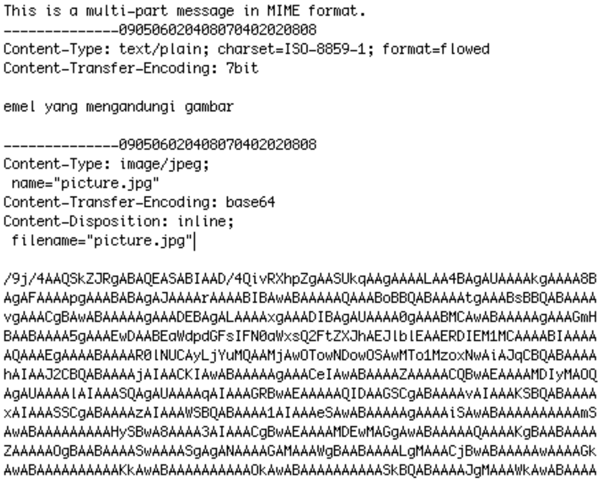
Figure 2. The output of Stegdetect

However, Stegdetect cannot assure the presence of the hidden message. A steganalysis tool called Stegbreak may be used to verify that the detected images have hidden messages. Stegbreak launches a dictionary attack against the JPEG images. JSteg-Shell, JPHide, or Outguess all hide content based on a user-supplied password, so an attacker can try to guess the password by taking a large dictionary and trying to use every single word in it to retrieve the hidden message (Provos & Honeyman, 2003).

4. Simple Mail Transfer Protocol (SMTP)

Simple Mail Transfer Protocol (SMTP) is without doubt the most popular protocol that is widely used since the existence of Internet. SMTP is one of the three primary application layer Internet protocols that support email (Tanenbaum, 2003). It is used for sending emails and it is responsible for establishing the connection between an email client and the email server. By using an email client, user can send messages together with other files types such as image, sound, documents and etc. An important issue in any messaging system is that sender and receiver agree on the format of the message content. Such an agreement is possible by including the description of that format as part of the message header. This is the principle underlying Multipurpose Internet Mail Extensions (MIME) (Tanenbaum, 2003).

In order to send content different from ASCII text, the sending user agent must include additional headers in the message. These extra headers are defined as Multipurpose Internet Mail Extensions (MIME). For example, sender's user agent must encode the message body that contains a JPEG image using base64 encoding. Base64 is one of several encoding techniques standardized in the MIME for conversion of the content of email attachment sent through email. Figure 3 shows an example of the MIME message of a JPEG image encoded in base64.



```
This is a multi-part message in MIME format.
--------------090506020408070402020808
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: 7bit

emel yang mengandungi gambar

--------------090506020408070402020808
Content-Type: image/jpeg;
 name="picture.jpg"
Content-Transfer-Encoding: base64
Content-Disposition: inline;
 filename="picture.jpg"|
```

```
/9j/4AAQSkZJRgABAQEASABIAAD/4QivRXhpZgAASUkqAAgAAAALAA4BAgAUAAAAkgAAAA8B
AgAFAAAApgAAABABAgAJAAAArAAAABIBAwABAAAAAQAAABoBBQABAAAAtgAAABsBBQABAAAA
vgAAACgBAwABAAAAAgAAADEBAgALAAAAxgAAADIBAgAUAAAA0gAAABMCAwABAAAAAgAAAGmH
BAABAAAA5gAAAEwDAABEaWdpdGFsIFN0aWxsQ2FtZXJhAEJlblEAAERDIEM1MCAAAABIAAAA
AQAAAEgAAAABAAAAR0lNUCAyLjYuMQAAMjAwOTowNDowOSAwMTo1MzoxNwAiAJqCBQABAAAA
hAIAAJ2CBQABAAAAjAIAACKIAwABAAAAAgAAACeIAwABAAAAZAAAAACQBwAEAAAAMDIyMAOQ
AgAUAAAAlAIAAASQAgAUAAAAqAIAAAGRBwAEAAAAAQIDAAGSCgABAAAAvAIAAAKSBQABAAAA
xAIAAASSCgABAAAAzAIAAAWSBQABAAAA1AIAAAeSAwABAAAAAgAAAAiSAwABAAAAAAAAAAmS
AwABAAAAAAAAHySBwA8AAAA3AIAAACgBwAEAAAAMDEwMAGgAwABAAAAAQAAAAKgBAABAAAA
ZAAAAAOgBAABAAAASwAAAASgAgANAAAAGAMAAAWgBAABAAAALgMAAACjBwABAAAAAwAAAAGk
AwABAAAAAAAAAAKkAwABAAAAAAAAAAOkAwABAAAAAAAAAASkBQABAAAAJgMAAAWkAwABAAAA
```

Figure 3. MIME encoding

Our work focus on images sent through email. The analysis was performed on the captured Transmission Control Protocol (TCP) packets with destination SMTP port 25.

5. The Architecture of Stegasniff

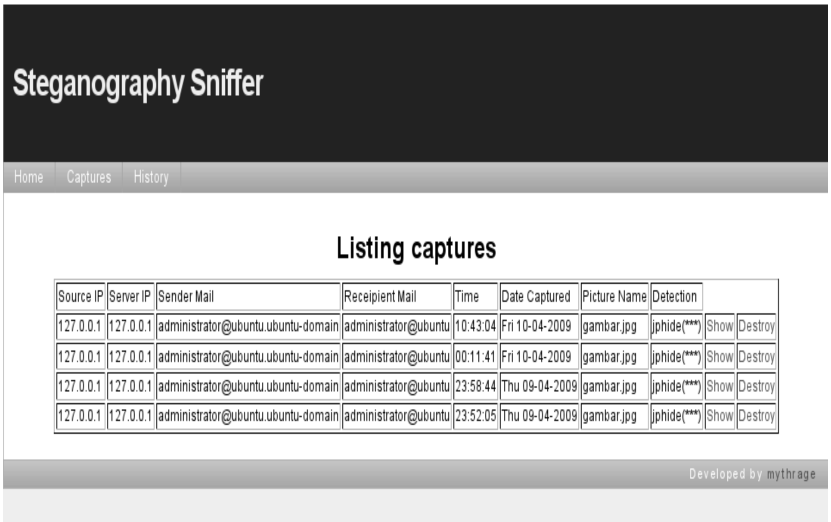
The Stegasniff consists of six modules:

i. Packet Sniffer
ii. Packet Analyzer
iii. Mail Analyzer
iv. Steganography Analyzer
v. Web-based Reporter and
vi. Steganography Extractor

Figure 1 shows how the processes are passed between the modules. These modules have specific functions that enable the detection of steganography during the delivery and the reception of the emails in the local network.

The Stegasniff is the main process that controls all other modules. The system administrator (or network administrator) of Stegasniff will be the key player of the system. Stegasniff then invokes Packet Sniffer module which sets the packet filter in the local network to listen only to SMTP port 25. The system then captures the SMTP packets using pthread function which later are stores temporarily in the system's buffer. The Packet Analyzer will then collects the Internet Protocol (IP) and TCP header plus the payload data of the packet. This module observes and records any traffic that contains email messages. This traffic is then given to Mail Analyzer. The analyzer reads the mail header and attachment segment in order to find and decode any JPEG image attachment to the email using the base64 decoder. The saved JPEG image in the temporary memory is then sent to the Steganography Analyzer module. This module which has Stegdetect as part of it, will detect for any steganographic content in the JPEG image.

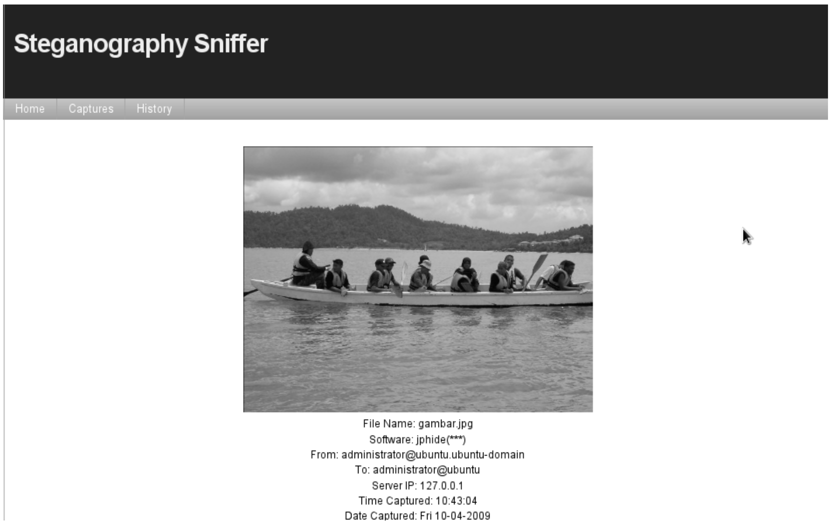
Stegdetect uses the filename of the JPEG image as its input before it can performs different steganalysis methods on the JPEG image. The result of the analysis is then recorded into the Stegasniff database. This database contains information such as the filename, output or results, and confidence level of each analysis. It also includes the email addresses of the sender and the recipient of the email, the timestamp and the IP address of the sender. Only the positive results are stored in the database as this will protect the privacy of the negatives images. The Web-based Reporter module assists the system administrator to check on the lists of the captured images (as shown in Figure 4) and the details of each steganographic image for further actions. Figure 5 shows the detail of steganographic image captured by Stegasniff.


Steganography Sniffer

Listing captures

Source IP	Server IP	Sender Mail	Receipient Mail	Time	Date Captured	Picture Name	Detection		
127.0.0.1	127.0.0.1	administrator@ubuntu.ubuntu-domain	administrator@ubuntu	10:43:04	Fri 10-04-2009	gambar.jpg	jphide(***)	Show	Destroy
127.0.0.1	127.0.0.1	administrator@ubuntu.ubuntu-domain	administrator@ubuntu	00:11:41	Fri 10-04-2009	gambar.jpg	jphide(***)	Show	Destroy
127.0.0.1	127.0.0.1	administrator@ubuntu.ubuntu-domain	administrator@ubuntu	23:58:44	Thu 09-04-2009	gambar.jpg	jphide(***)	Show	Destroy
127.0.0.1	127.0.0.1	administrator@ubuntu.ubuntu-domain	administrator@ubuntu	23:52:05	Thu 09-04-2009	gambar.jpg	jphide(***)	Show	Destroy

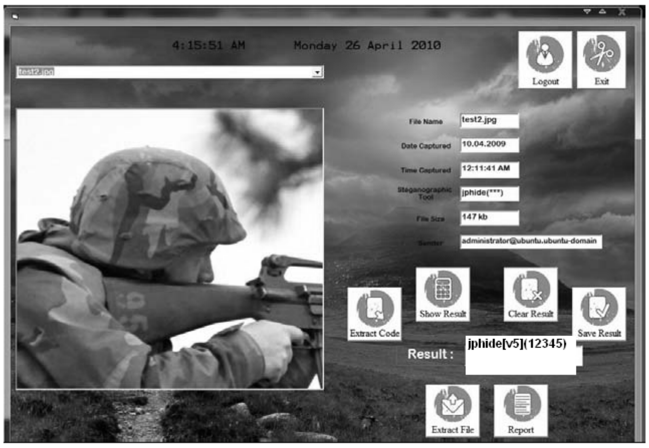
Figure 4. List of the captured JPEG images



File Name: gambar.jpg
Software: jphide(***)
From: administrator@ubuntu.ubuntu-domain
To: administrator@ubuntu
Server IP: 127.0.0.1
Time Captured: 10:43:04
Date Captured: Fri 10-04-2009

Figure 5. The details of a steganographic image

Finally, once stored to the database, the system will then extract the hidden message to reveal the message. This is done by Steganography Extractor module which has Stegbreak tool as part of it. By using Stegbreak, it can extract the messages from the JPEG images that is relevant to a dictionary attack and save it in a separate file. This is shown in Figure 6.



File Name: test2.jpg
Date Captured: 10.04.2009
Time Captured: 12:11:41 AM
Steganographic Tool: jphide(***)
File Size: 147 kb
Sender: administrator@ubuntu.ubuntu-domain
Result : jphide[v5](12345)

Figure 6. Steganography Extractor

6. Conclusions

In this paper, we have presented a system called Stegasniff that can retrieve images from the emails and automatically detects whether they might contain steganographic messages. The hidden message is then revealed to detect its existence in which thwarts the main purpose of steganography. Future enhancements of Stegasniff will include additional support for other types of images and the integration of these tools for capturing steganography contents over the World Wide Web.

References

Chandramouli, R., & Subbalakshmi, K. P. (2004). Current trends in steganalysis: a critical survey. *Control, Automation, Robotics and Vision Conference, 2*, 964-967.

Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: seeing the unseen. *IEEE Computer, 31*(2), 26-34. http://dx.doi.org/10.1109/MC.1998.4655281

Lee, Y. K., & Chen, L. H. (2000). High Capacity Image Steganographic Model. *IEEE Proceedings Vision, Image and Signal Processing, 147*(3), 288-294. http://dx.doi.org/10.1049/ip-vis:20000341

Mohamed Halip, M. H., & Abdul Raoh, M. L. (2009). *Stegasniff: A Packet Sniffer for Steganography Detection.*

Proceedings of the Asia Pacific Conference on Defence & Security Tecnology (DSTC 2009). Kuala Lumpur.

Provos, N., & Honeyman, P. (2003). Hide and Seek: An Introduction to Steganography. *IEEE Security & Privacy, 1*(3), 32- 44. http://dx.doi.org/10.1109/MSECP.2003.1203220

Tanenbaum, A. S. (2003). *Computer Networks* (4th ed.). Pearson Prentice Hall.