Journal of Network and Computer Applications 35 (2012) 491–501

Contents lists available at SciVerse ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

A framework for avoiding steganography usage over HTTP

Jorge Blasco [a,*], Julio Cesar Hernandez-Castro [b], José María de Fuentes [a], Benjamín Ramos [a]

[a] Computer Science Department, Carlos III University of Madrid, Av. de la Universidad 30, 28911 Leganés, Spain
[b] School of Computing, University of Portsmouth, Buckingham Building, Lion Terrace, Portsmouth PO1 3HE, UK

ARTICLE INFO

Article history:
Received 24 May 2011
Received in revised form
16 September 2011
Accepted 2 October 2011
Available online 13 October 2011

Keywords:
Steganography
Covert channels
HTTP
Active warden
Sanitization

ABSTRACT

Steganographic techniques allow users to covertly transmit information, hiding the existence of the communication itself. These can be used in several scenarios ranging from evading censorship to discreetly extracting sensitive information from an organization. In this paper, we consider the problem of using steganography through a widely used network protocol (i.e. HTTP). We analyze the steganographic possibilities of HTTP, and propose an active warden model to hinder the usage of covert communication channels. Our framework is meant to be useful in many scenarios. It could be employed to ensure that malicious insiders are not able to use steganography to leak information outside an organization. Furthermore, our model could be used by web servers administrators to ensure that their services are not being abused, for example, as anonymous steganographic mailboxes. Our experiments show that steganographic contents can be successfully eliminated, but that dealing with high payload carriers such as large images may introduce notable delays in the communication process.

1. Introduction

Steganography is the science that studies the techniques to hide the existence of messages (Johnson and Jajodia, 1998). The ability of sending secret messages can be useful for several purposes. On one hand, in a country under a totalitarian government, steganography could be used to circumvent censorship (Feamster et al., 2002), and in a more general setting it could be instrumental for whistleblowers. On the other hand, steganography can also be used to commit malicious or criminal activities. In fact, it could be used by an employee stealing sensitive information from an organization in a case of industrial espionage. Before transferring this valuable information, the employee may hide it into innocuous looking documents. In this way, any security check or network monitoring tool would not detect sensitive information leaving the organization. Steganography can also help exchange illegal content (such as child pornography) using public resources like web servers or P2P networks as repositories, without the knowledge of the owners of those resources.

Recently, the usage of steganography reached public media coverage when a group of spies from Russia were uncovered (McGreal, 2010). As the FBI report describes (Kachhia-Patel, 2010), the spies, who infiltrated into some United States Government agencies, used a steganographic program to conceal their intelligence reports into digital images. Those were later uploaded to public web servers, so the Russian intelligence at Moscow could download them and extract the secret messages (intelligence reports) after the use of a pre-shared key. Another malicious usage of steganography that has risen recently is to command and control botnets (Kartaltepe et al., 2010). By employing steganography, botnet owners can benefit from social network sites and transform them into infrastructures to covertly deliver their commands. In this way, botnet administrators have a centric, fast, reliable and easy method to distribute their commands to multiple bots.

Avoiding such a kind of malicious steganography usage is an important issue for organizations which hold large amounts of sensible information, or by system administrators that do not want their services to be used for unauthorized purposes. Although steganography can be used to create a covert channel through any kind of network protocol, we have focused on the restriction of HTTP for several reasons:

- The restriction of HTTP traffic through firewalls is infeasible as it is essential for Internet communications. HTTP provides access to multiple kinds of services such as news, search engines, web mail, social networks, multimedia, etc. but also provides enterprise services such as Business to Business services, reference, documentation, etc. which are essential for organizations and cannot be simply blocked.
- HTTP allows users to access plenty of information and consumption services (YouTube, Flickr, etc.). These kind of services can be easily used by steganography users as cover repositories and anonymous mailboxes to upload, store and download hidden information (Burnett et al., 2010). In this regard, URL filtering software could be used to restrict the amount of sites a potential steganography user is able to

* Corresponding author. Tel.: +34 916 248 847.
E-mail addresses: jbalis@inf.uc3m.es (J. Blasco), Julio.Hernandez-Castro@port.ac.uk (J.C. Hernandez-Castro), jfuentes@inf.uc3m.es (J.M. de Fuentes), benja1@inf.uc3m.es (B. Ramos).

1084-8045/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2011.10.003

connect. Due to the great amount of these, it is however unlikely that the security administrator will be able to block them all.

- The usage of HTTP provides a higher anonymity level, in comparison with other common organization wide network protocols such as SMTP. Although HTTP communications are not anonymous, only the web server administrator or network nodes between the user and the web server may posses enough information to identify who accessed the server resources. This allows to identify the possible recipients of the hidden messages, but not the actual recipient. Other protocols such as SMTP explicitly specify the recipient of the information when communicating to an intermediary server, so they are easier to trace.
- Finally, the usage of third party web servers as part of the steganographic communication usually involves a violation of these servers' terms of use. This kind of abuse may induce unnecessary overloads that should be actively avoided by system administrators.

The contribution of this paper is a framework, named StegoProxy, which limits the transmission of hidden information through Hyper Text Transfer Protocol (HTTP). The proposed model hinders the usage of steganography on HTTP message body entities such as images, text, etc. Additionally, it avoids the usage of the HTTP protocol structure itself for steganographic purposes (i.e. modifying HTTP headers to hide information as proposed by Dyatlov and Castro, 2003). This is achieved by actively modifying HTTP messages. In order to evaluate the proposed model, an implementation has been developed.

Our proposal enables the normal usage of HTTP connections, while hinders the existence of covert channels through these. This would allow organizations to avoid information theft through HTTP. Additionally, our scheme may allow service providers to ensure clients perform an authorized usage of their services (i.e. they are not used to covertly store unauthorized material). Although our proposal is focused on HTTP it may be easily adapted to other protocols such as SMTP, FTP, etc.

The rest of the paper is structured as follows. We describe the basics of steganography in Section 2. The related work is summarized in Section 3. In Section 4, we describe the steganographic capabilities of HTTP. The proposed framework is explained in Section 5. Section 6 depicts the performed evaluation and summarizes the obtained results. Finally, Section 7 gathers the conclusions and future work lines.

2. Steganography

The first model of steganography was described by Simmons (1998) as the prisoners' problem. Simmons described two prisoners (Alice and Bob) who want to plot an escape plan. As they are not in the same cell, they must communicate through a warden (Wendy), that will analyze any communication between them. If Wendy ever suspects that Alice and Bob are planning to escape he will put them into isolation cells and the escape will be frustrated. In this scenario, Alice and Bob will not be able to just use cryptography, as encrypted messages will raise suspicions on Wendy. In order to achieve their goal, Alice and Bob should hide their secret messages into innocuous looking ones (called covers), so Wendy will only see unremarkable messages exchanged between prisoners.

However, if Wendy is aware of the existence of some kind of steganography she may be able to detect the presence of hidden messages or even further destroy the covert channel between Alice and Bob. On one hand, if Wendy just analyzes the messages and forwards them to their recipients, then Wendy is a *passive warden*. In this case Wendy verifies if the cover contains hidden contents or not. On the other hand, if Wendy has high suspicions of Alice and Bob planning an escape through their messages, but she is not able to obtain proof, she may slightly modify the exchanged messages trying to perturb any hidden information. In this case, Wendy is an *active warden*. Even further, Wendy may be able to insert some information impersonating Alice or Bob, thus performing a man in the middle attack. In this case Wendy is a *malicious warden*. Although steganographic algorithms should be robust to active warden attacks, steganographic researchers have mainly focused on the imperceptibility of hidden information while resistance against active attacks has been mostly addressed in other information hiding areas like watermarking (Cox et al., 2008).

Thanks to the widespread adoption of digital devices and electronic documents, steganography has attracted the interest of researchers in the last years. Fisk et al. (2003) defined the concepts of structured and unstructured carriers. A carrier specifies the features or characteristics used to hide the information in the cover. In this regard, a structured carrier is defined as a carrier which structure is well defined (XML files, PDF files, network protocols, etc.), while unstructured carriers do not have a defined structure (images, video, natural language, etc.). HTTP is a specially interesting and relevant case because it encompasses both carrier types, as information can be hidden into the structure of the HTTP message (see Section 4) or into the content uploaded or downloaded by the user (images, videos, etc.).

2.1. Steganography in unstructured carriers

The increasing concerns about copyright violations of multimedia works motivated the first research efforts on information hiding techniques for unstructured carriers. Least Significant Bit (LSB) techniques are the best known techniques, based on hiding information into the least significant bits of covers (Van Schyndel et al., 1994). Depending on the data representation, least significant bits can be the last bits of the RGB composition, the last significant bits of the DCT transform, etc. The amount of information embedded in the image generally sets the amount of distortion that results in the cover image. Due to the size of image files, image steganography provides high capacity. A comprehensive description of several image steganography techniques can be found in Chandramouli et al. (2004).

Audio steganography techniques allow to hide information in compressed (MP3, etc.) or uncompressed (WAV, etc.) audio files. In this regard, the concept of LSB steganography can be also used in the audio domain. Changing the least significant bit on each audio sample allows to encode information without generally creating an audible difference on the audio file. Depending on its configuration, an audio file may hold up to 44 100 audio samples for every second, making uncompressed audio a very high capacity carrier (Bender et al., 1996). Audio steganography can be performed also in compressed audio files like MP3s (Petitcolas, 1998).

Besides image and audio, another widely used way to represent information is text. The most relevant proposals for text steganography have been based on the concept of mimic functions (Wayner, 1992). Using mimic functions, NICETEXT (Chapman and Davida, 1997) is able to transform a secret message M into a seemingly innocuous text T which contains sentences in natural language. Grothoff et al. (2005) propose to embed information into the noise and errors produced by automatic translation systems. In this way, new errors and noise detected on the steganographic text would be attributed to the automatic translation system. Particular language and