

# Literature Review

Daniel Jones

University of Birmingham

`dgj470@student.bham.ac.uk`

November 12, 2017

## Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Main Body</b>	<b>2</b>
2.1	Image steganography . . . . .	2
2.2	DNS steganography . . . . .	2
2.3	HTTP protocol . . . . .	3
2.4	Detecting tunneled DNS traffic . . . . .	3
<b>3</b>	<b>Conclusion</b>	<b>3</b>
<b>4</b>	<b>References</b>	<b>3</b>

# 1 Introduction

In this literature review, I am going to look at some literature surrounding steganography, HTTP, DNS tunneling and detecting tunneled traffic. This review will not explore more that required to do with encryption or standard VPNs.

There has been a lot of work done on the study of steganography, and using different protocols to hide data. The most work has been done on DNS, as it is often below the radar for firewalls and checking if data is being exfiltrated.

## 2 Main Body

### 2.1 Image steganography

Steganography is most commonly used for hiding data in unused or unimportant areas of data[1], and the most common form of data for this is images. This is because all of the colour data in an image is not required for a human to see it, and the human eye is very good at filtering out noise[1].

More advanced approaches to steganography can involve identifying redundant data in images[2] which can be better than changing the least significant bit in an image which can be detected by steganalysis[2].

Steganography that is hidden from computers and is hidden from people are quite different things, and can require quite different approaches. The real challenge is to hide data from both.[2].

### 2.2 DNS steganography

It is possible to hide data very easily in DNS requests, and this is called DNS Tunneling, and it is often used to get around firewalls and hide which websites are being accessed.[3] This paper highlights the point raised in the previous section, that it is very easy for a human to look at the data and see it's not normal, but non-trivial for a computer. The paper describes how the data is detected, and in doing so describes in depth how the data is encoded and tunneled. DNS tunneling as described in the aforementioned paper has a few advantages and disadvantages. The key advantage is that it can be used in locked down networks, as DNS traffic is often let out, but the main disadvantage is that data transfer is very slow with a lot of overhead.

## 2.3 HTTP protocol

The HTTP 1.1 Protocol[4] is a protocol that describes how data is sent to and from a client, and it describes many areas where data could be included. HTTP traffic can include: Images, HTML, CSS, Javascript, Binary files, and more.

## 2.4 Detecting tunneled DNS traffic

There are a variety of ways to detect tunneled traffic, from entropy analysis to performing DNS requests[3]. Another way of performing the lookup is to do character frequency analysis[5]. Frequency analysis looks at the difference in frequency of letters in domain names/english words and in random data. It is similar to but not quite the same as entropy analysis, and it is also more effective[5].

## 3 Conclusion

In conclusion, I think that using HTTP/HTML could be more effective than using DNS to tunnel data, because there would be less overhead (more places to put data), and it would be harder to detect, as HTTP data can be more structured. The disadvantage would be that HTTP traffic is often monitored in depth, but using steganography to hide data in images and text on websites could go under the radar.

## 4 References

### References

- [1] Johnson Neil F and Jajodia Sushil. Exploring steganography: Seeing the unseen. *Computer*, 31(2):26–34, Feb 1998.
- [2] Provos N and Honeyman P. Hide and seek: an introduction to steganography. *IEEE Security & Privacy*, 99:32–44, June 2003.
- [3] Greg Farnham. Detecting dns tunneling. *SANS Institute Reading Room*, Feb 2013.

- [4] Fielding R, Irvine UC, Gettys J, Compaq/W3C, Mogul J, Compaq, Frystyk H, W3C/MIT, Masinter L, Xerox, Leach P, Microsoft, and Berners-Lee T. Hypertext Transfer Protocol – HTTP/1.1. RFC 2616, RFC Editor, June 1999.
- [5] Born Kenton and Gustafson Dr. David. Detecting dns tunnels using character frequency analysis. *CoRR*, abs,1004.4358, 2010.