

## **Table of Contents**

- 1. Overview**
- 2. Anonymity and You**
  - 2.1 Implications of being Anonymous Online
  - 2.2 Legal Considerations
  - 2.3 Ethical Considerations
  - 2.4 Evaluation of Future Policy
- 3. Encryption**
  - 3.1. Asymmetric Encryption
  - 3.2. Public/Private Key Implementation of Asymmetric Encryption
- 4. Anonymous Access Models**
  - 4.1. Traditional Anonymous Access
  - 4.2. Employing Encryption for Anonymous Communication
  - 4.3. Onion Routing
  - 4.4. Tor
- 5. Distributed File Storage**
  - 5.1. Introduction
  - 5.2. Current Distributed File Storage Systems
  - 5.3. Problems with Distributed File Storage
- 6. Anonymous Distributed File Storage**
  - 6.1. Introduction
  - 6.2. Anonymous Peer-to-Peer
  - 6.3. Free Haven
    - 6.3.1. Concept
    - 6.3.2. Problems
    - 6.3.3. Proposed Solutions
- 7. Ghost Writer**
  - 7.1. An Anonymous Distribute File Storage System for the Masses
  - 7.2. Clients
  - 7.3. Files
  - 7.4. Directory Server
  - 7.5. Communication
  - 7.6. Problems
  - 7.7. Future Work
- 8. Conclusion**

## **Executive Summary**

The need for anonymity on the internet is large and shared by many individuals. Anonymous communication is necessary to preserve safety, to protect sensitive content and to give individuals the sense of satisfaction that comes with knowing one's interactions are secure. Unfortunately, the average user has a limited number of choices available when it comes to anonymity tools. Many tools exist in concept, but not in practice. Recognizing this need, our project attempts to put the concept delineated in Free Haven into practice, to provide users with an anonymous distributed file storage tool. This paper will start out by considering the advantages and repercussions of having the ability to be anyone and say anything online without having it linked to one's identity. We will take ethical and legal considerations into account as they pertain to pornography and free speech, and will discuss the extent to which an individual's online privacy should be regulated in the future. We will then explore the various tools enabling anonymous Internet access that already exist, such as re-mailers, onion routing, and Tor. This analysis will concentrate heavily on Tor, which will be fundamental to later parts of the paper. Next, we will present a brief analysis of the work that has already been done in the field of distributed file storage, and discuss the motivations behind the investigation undergone in this paper. We will then outline our implementation of the Free Haven project called Ghost Writer and present the code that makes this program run. To conclude we will explore the problems with our system, discuss potential solutions, and suggest ideas for future research that can be conducted in this area.

## Bibliography

- Acquisti, A., Dingledine, R., & Syverson, P. On the Economics of Anonymity.
- Back, A., Möler, U., & Stiglic, A. (2001). Traffic analysis attacks and trade-offs in anonymity providing systems. In Ira S. Mokowitz, editor, *Information Hiding (IH 2001)* pages 245-247. Springer-Verlag, LNCS 2137, 2001.
- Chaum, D. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*.
- Danezis, George and Anderson, Ross. (2004). *Economics of Censorship Resistance*. In the proceedings of Workshop on Economics and Information Security (WEIS 04).
- Dingledine, R. (2000). The Free Haven Project: Design and deployment of an anonymous secure data haven. Master's thesis, Massachusetts Institute of Technology.
- Dingledine, R., Freedman, M., Hopwood, D. & Molnar, D. (2001). A Reputation System to increase MIX-net Reliability. In Ira S. Mokowitz, editor *Information Hiding (IH 2001)*, pages 126-141. Springer-Verlag, LNCS 2137, 2001.
- Dingledine, R., & Freedman, M. (2000). The Free Haven project: Distributed anonymous storage service. In *Proceedings of the Workshop on Design Issues in Anonymity and Unobservability*.
- Dingledine, R., Mattherson, N., & Syverson, P. (2004). The Second-Generation Onion Router. *Usenix Security 2004*.
- Free Haven. Consulted April 16, 2006, [www.freehaven.net](http://www.freehaven.net).
- Kim, B., Laas, C., O'Gilvie, S., & Yip, A. (2001). *Anonymity Tools for the Internet*.
- Lessig, Lawrence. (1999). *Code and Other Laws of Cyberspace*. USA: Basic Books.
- O'Harrow, Robert. (2005). *No Place to Hide*. USA: Free Press.
- Stubblebine, S., & Syverson, P. (2001). Authentic attributes with fine-grained anonymity protection. In Yair Frankel, editor, *Financial Cryptography (FC 2000)*. Pages 276-294. Springer-Verlag, LNCS 1962.
- Tor: An Anonymous Internet Communication System. Retrieved April 16, 2006, from <http://tor.eff.org/>.