A Taxonomy of Censors and Anti-Censors Part II: Anti-Censorship Technologies

Christopher S. Leberknight, Department of Computer Science, William Paterson University, Wayne, NJ, USA

Mung Chiang, Department of Electrical Engineering, Princeton University, Princeton, NJ, USA

Felix Ming Fai Wong, Department of Electrical Engineering, Princeton University, Princeton, NJ, USA

ABSTRACT

This paper presents a conceptual study of Internet anti-censorship technologies. It begins with an overview of previous research on Internet anti-censorship systems and discusses their social, political and technological dimensions. Then for deployed Internet anti-censorship technologies, a taxonomy of their principles and techniques is presented, followed by a discussion of observed trends and implications. Based on the observations, the paper concludes with a discussion on the most critical design features to enable a successful and effective system.

Keywords: Anti-Censorship, Circumvention Technology, Filtering, Internet Censorship, Taxonomy

1. INTRODUCTION

The evolution of Internet censorship and anti-censorship technologies is an endless arms race: Internet users constantly apply new methods to circumvent blocks and filters imposed by online censors, and censors constantly update their deployed systems in response. With the ever-increasing speeds and capabilities of computers, one can only expect this arms race to be more dynamic. This paper is a sequel to the authors’ previous paper on Internet censorship (Leberknight et al., 2012). One of the main objectives of this research is to advance the state of the art of circumvention technologies, by stimulating discussion on the directions and development of these systems.

Circumvention is approached in mainly three directions. The first is anonymity, which is to allow users to communicate undetected in a censored network. The second is content protection, which is to protect a communication channel from being attacked by censors. The last direction is content filtering or detection evasion, which is to evade detection even when message contents can be directly monitored. A successful system should exploit simultane-
ously a censorship system’s vulnerabilities from the social, political and technological dimensions.

A main contribution of this conceptual paper is a taxonomy of Internet anti-censorship technologies. The taxonomy is presented at three levels of detail. At the principles level the paper presents a list of criteria for a system to be successful. At the techniques level these systems attempt to defeat blocking according IP addresses, URLs, or message contents. It is found that these systems usually implement some form of forwarding, with the help of computers located geographically outside a censorship system. Finally, at the technologies level the paper studies the available systems individually. Specifically, the systems are tabulated to show which techniques they apply, and the times of deployment of various censorship and anti-censorship technologies are visualized in a timeline. A number of interesting implications can be drawn from the taxonomy.

Even if an anti-censorship system is theoretically sound, it will not succeed if end-users refuse to adopt it for usability issues, or even worse, refuse to try it if they perceive it to be untrustworthy in terms of anonymity, content protection, or detection evasion. To address this, the paper discusses the most important design features to enable a successful and effective system. Trust is an important factor, both in terms of a user’s social network (from which a new anti-censorship technology is learnt), and the technology itself (whether it is reliable and financially sustainable). A somewhat surprising fact that simpler and faster technologies are more popular suggests that performance is often a more dominant factor than trust.

2. PREVIOUS RESEARCH

Extant literature on circumvention technologies discusses several techniques and strategies for designing censorship resistant systems. There are two main dimensions: free access to information and free publication of information, the second being even more challenging than the first.

A key component for any censorship resistant system or circumvention technology is to ensure privacy by enabling users to communicate undetected in a censorship network. This is often accomplished by incorporating certain techniques such pseudonymity and anonymity into the system. However, previous research suggests that current techniques to ensure privacy still reveal a significant amount of identifying information (Rao & Rohatgi, 2000). Rao and Rohatgi (2000) indicate that techniques from linguistics and stylometry can use the identifying information to compromise pseudonymity. They suggest some countermeasures to address syntactic and semantic leaks of information. With respect syntactic leaks the authors suggest using a thesaurus tool, which could prompt the user to use alternatives while composing messages thereby reducing variations in vocabulary. For semantic leaks, they suggest translating the message to another language and then back again to the original language (Rao & Rohatgi, 2000).

In addition to addressing the limitations for ensuring privacy using tools, other research has introduces four properties: anonymity, unlinkability, unobservability, and pseudonymity, and a set of anonymity metrics, which can be used to improve the design and evaluation of censorship resistant systems (Danezis & Diaz, 2008). Expanding on research which has introduced tools, properties and metrics for ensuring privacy and specific applications to censorship resistant systems, privacy via anonymity has also been explored by investigating the limitation of different network topologies and document storage techniques. Due to the single point of failure or ability to conduct denial of service attacks on centralized designs, network topologies such as peer-to-peer approaches for addressing anonymity have been suggested. One example is a peer-to-peer protocol that guaran-
Related Content

Social and Human Elements of Information Security: A Case Study
www.igi-global.com/chapter/social-human-elements-information-security/39708?camid=4v1a

Impact of Information Technology on Lifestyle: A Literature Review and Classification
www.igi-global.com/article/impact-of-information-technology-on-lifestyle/182729?camid=4v1a

Effects of Social Media on Project Management
Mark Sponselee (2016). Strategic Integration of Social Media into Project Management Practice (pp. 16-34).
www.igi-global.com/chapter/effects-of-social-media-on-project-management/145665?camid=4v1a
Social Identity in Facebook Community Life
Shaoke Zhang, Hao Jiang and John M. Carroll (2010). International Journal of Virtual Communities and Social Networking (pp. 64-76).
www.igi-global.com/article/social-identity-facebook-community-life/52990?camid=4v1a