USENIX Workshop on Free and Open Communications on the Internet (FOCI '11)

August 8, 2011
San Francisco, CA

[Note: For the remainder of the workshop program, including full papers and presentation slides, see http://www.usenix.org/events/foci11/tech/.]

Measuring Censorship

Summarized by Nick Jones (najones@cs.princeton.edu)

Three Researchers, Five Conjectures: An Empirical Analysis of TOM-Skype Censorship and Surveillance

Jeffrey Knockel, Jedidiah R. Crandall, and Jared Saia, University of New Mexico

Knockel began by introducing TOM-Skype, a modified version of Skype produced by TOM Group in China. When Skype users in China attempt to download Skype, they are automatically redirected to TOM-Skype. Since TOM-Skype is interoperable with regular Skype, it uses the Skype network for all of its communication. Due to this, TOM-Skype performs censorship locally on users' computers. TOM-Skype performs this monitoring using keyfiles, which are lists of encrypted words to monitor for.

In this work, the authors reverse engineered the cryptographic algorithm used to encrypt the keyfiles. They approached this problem by using known blocked words in conversation, and monitoring the program's behavior. Notably, the latest version of TOM-Skype (5.1) contains two separate keyfiles. One keyfile triggers a surveillance message which is sent to TOM Group, while the second keyfile triggers both surveillance and censorship of the user's conversation. From this work, the authors propose five conjectures which they believe are a useful model for studying Internet censorship: (1) censorship is effective, despite attempts to evade it; (2) censored memes spread differently from uncensored memes; (3) keyword-based censorship is more effective when the censored keywords are unknown and online activity is, or is believed to be, under constant surveillance; (4) the types of keywords censored in peer-to-peer communications are fundamentally different from the types of keywords censored in client-server communications; (5) neologisms are an effective technique for evading keyword-based censorship, but censors frequently learn of their existence.

One audience member asked if the authors retained copies of the sets of blocked keywords that TOM-Skype has used over time. Knockel said that the keywords were retained, and that they may analyze the changes in future work.

Fine-Grained Censorship Mapping: Information Sources, Legality, and Ethics

Joss Wright, Oxford Internet Institute; Tulio de Souza, Oxford University Computing Laboratory; Ian Brown, Oxford Internet Institute

Wright argued that every country engages in censorship at some level, and that it is useful to examine censorship at a more fine-grained level than national borders. In this work, the authors used DNS servers across China to check for blocked Web site addresses. They tested 278 DNS servers, and performed a DNS query for each of the top 80 blocked Web sites. Different servers within China provided different results for the same blocked Web sites. Some servers listed the site as non-existent, others returned no results, and some redirected a user to Beijing before returning no result.

In addition to the censorship study, Wright discussed the challenges inherent to studying censorship problems. He talked about the legal and ethical implications of asking end users to access blocked Web sites, specifically when doing so may place these users at some risk. He stressed the importance of getting informed consent from participating users, and this inspired a discussion about best practices for communicating risks to users.

During Q&A, one audience member asked about the difference between a user requesting access to a Web site and a user successfully accessing the Web site. Wright responded that this depends on which country the user resides in, and that it is necessary to examine the laws of each country. Another person asked about building censorship detection tools which incorporate plausible deniability. Wright responded that the problem has numerous ethical and legal challenges that must be addressed before we could build such tools.

CensMon: A Web Censorship Monitor

Andreas Sfakianakis, Elias Athanasopoulos, and Sotiris Ioannidis, Foundation for Research and Technology, Hellas

Sfakianakis began by discussing the dynamic nature of censorship and the drawbacks of existing tools for detecting and reporting censorship. Sfakianakis then introduced CensMon, a distributed system for detecting censorship at a global level. CensMon is designed around a central server, which uses a network of agents to report censorship. CensMon agents monitor multiple systems including Twitter, Google Alerts, and Google Trends in order to extract URLs for censorship checking by the agent network. Additionally, CensMon checks for filtering at different protocol levels, including DNS filtering, IP blocking, and changes in accessibility to known censored Web sites. The initial deployment of CensMon was tested over 14 days with agents in 33 countries: 86% of the agents reported no filtering, with China's agent node reporting 176 censored domains.

In addition to domain blocking, CensMon can detect partial content censorship, such as news articles which have been changed by a censor. In their initial study, while 3% of the URLs tested saw some content changes, no partial content filtering was detected. Sfakianakis argued that one major advantage of the CensMon system is that monitoring multiple streams of information in multiple locations provides an ability, under certain circumstances, to detect content that has been modified but not completely blocked.

Audience members asked whether CensMon can handle dynamic content. Sfakianakis replied that CensMon currently only handles Web pages that have an "article-like" format. Can CensMon handle syndicated content such as newspaper stories? CensMon does not have any special handling of this type of content. Is it possible to use Tor exit nodes as CensMon agents? This is technically possible, but not implemented in the current CensMon software.

Work-in-Progress: Automated Named Entity Extraction for Tracking Censorship of Current Events

Antonio M. Espinoza and Jedidiah R. Crandall, University of New Mexico

Espinoza presented this study, which analyzes censorship in China by performing named entity extraction on Chinese-language sources to pick out people, places, and other relevant terms from news texts. The authors trained their named entity extractor on the Chinese-language version of Wikipedia, using part of Wikipedia as a training set and part as a test set. The authors then queried Chinese search engines with phrases extracted from their training data. They repeated these searches every 12 hours, looking for changes in the returned results, as well as GET request censorship. Several sensitive terms were discovered, such as "nobel prize," "norway," and "jasmine flower."

Espinoza said that the list of censored terms used for GET request censorship is relatively static and slow-changing. In the future, the authors hope to improve their named entity extraction and to support other languages. Additionally, they would like to add other input sources into their monitoring study, such as the list of censored words used by TOM-Skype.

One audience member asked about the time frame during which these experiments were run. Espinoza responded that they were conducted during a two-month period around the beginning of 2011. Another question addressed the possibility that the queries might return different results when executed within China. Espinoza acknowledged this and said that they have not yet been able to test that, but would like to do so in future work.