Announcement and Call for Papers **USENIX**

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

Sponsored by USENIX, the Advanced Computing Systems Association

http://www.usenix.org/foci11

August 8, 2011 **San Francisco, CA**

FOCI '11 will co-located with the 20th USENIX Security Symposium (USENIX Security '11), which will take place August 8–12, 2011.

Important Dates

Submissions due: *May 8, 2011, 11:59 p.m. PDT*
Notification to authors: *June 15, 2011*
Final paper files due: *July 11, 2011*

Workshop Organizers

Program Co-Chairs

Nick Feamster, *Georgia Institute of Technology*
Wenke Lee, *Georgia Institute of Technology*

Program Committee

Dorothy Chou, *Google*
Richard Clayton, *Cambridge University*
Jed Crandall, *University of New Mexico*
Nicolas Christin, *Carnegie Mellon University*
George Danezis, *Microsoft Research*
Roger Dingledine, *Tor Project*
Mike Freedman, *Princeton University*
Krishna Gummadi, *Max Planck Institute for Software Systems*
Alex Halderman, *University of Michigan*
Josh Karlin, *BBN Technologies*
Jennifer Rexford, *Princeton University*
Hal Roberts, *Berkman Center, Harvard University*
Pablo Rodriguez, *Telefónica*
Wendy Seltzer, *Princeton CITP and Berkman Center, Harvard University*
Paul Syverson, *United States Naval Research Laboratory*
Santosh Vempala, *Georgia Institute of Technology*
Joss Wright, *University of Oxford*

Overview

The first USENIX Workshop on Free and Open Communications on the Internet (FOCI) seeks to bring together researchers and practitioners from both technology and policy who are working on policies or technologies to detect or circumvent practices that inhibit free and open communications on the Internet.

The growth of the Internet offers great promise for improving the communication capabilities of many users, but our increasing dependence on networked communications also makes it easier for organizations to control, monitor, or block user communications. ISPs and governments routinely restrict access to Internet content and services, either by censoring access to the information or by degrading the performance of various services (e.g., violating network neutrality). Indeed, although we think of the Internet as enabling the "democratization" of communications, free and open access is at risk: the Open Net Initiative reports that nearly 60 countries censor some access to information on the Internet. Similarly, ISPs can degrade network performance for certain subsets of users for some or all services. For example, some ISPs have been found to routinely block or throttle certain application traffic (e.g., BitTorrent). This growing trend towards blocking, tampering with, or otherwise restricting communications on the Internet calls for better techniques for both monitoring the state of restrictions on Internet content and communications (i.e., improving "transparency") and circumventing attempts to censor, degrade, or or otherwise tamper with Internet communications. In many cases, this technology must be both deniable (i.e., it must allow the user to deny knowledge about using the technology) and robust to blocking.

Topics

We encourage submissions of new, interesting work on a wide variety of topics of interest, including but not limited to the following areas:

- Evaluation or analysis of existing anti-censorship systems
- Comparisons of existing performance-measurement tools that might be used to detect tampering (e.g., violations of "network neutrality")
- Studies and findings on censorship or tampering from field deployments (e.g., what content various countries are currently censoring, the extent to which ISPs are degrading certain types of content)
- Analysis of the economic impact of censorship
- Metrics for deniability and robustness
- Performance metrics and benchmarks for detecting content tampering or performance degradation
- Detecting and measuring the censorship of search results
- The design of network protocols and topologies that resist tampering or censorship
- Techniques to counter mass surveillance
- Policy-related issues

What to Submit

We invite short position papers or work-in-progress reports. The workshop will have no printed proceedings, and we do not regard appearance at FOCI to be prior publication for future submission purposes. FOCI will favor interesting and new ideas and early results that lead to well-founded position papers. We envision that work presented at FOCI will ultimately be published at relevant, high-quality conferences. Papers will be selected primarily based on technical merit and originality, with additional consideration given to their potential to generate discussion at the workshop.

Submission Guidelines

Submitted papers must be no longer than six 8.5" x 11" pages, based on the standard USENIX format. Specifically, your paper should be typeset in two-column format in 10-point type on 12 point (single-spaced) leading, with a text block of no more than 6.5" wide by 9" deep. Submissions are single-blind; authors should include their names and affiliations as part of their submissions. Papers must be submitted via the Web submission form on the FOCI '11 Call for Papers Web site, http://www.usenix.org/foci11/cfp.

All accepted papers will be available online to registered attendees before the workshop. If your paper should not be published prior to the event, please notify production@usenix.org. The papers will be available online to everyone beginning on the day of the workshop, August 8, 2011.

Simultaneous submission of the same work to multiple venues, submission of previously published work, or plagiarism constitutes dishonesty or fraud. USENIX, like other scientific and technical conferences and journals, prohibits these practices and may take action against authors who have committed them. See the USENIX Conference Submissions Policy at http://www.usenix.org/submissionspolicy. Questions? Contact your program co-chairs, foci11chairs@usenix.org, or the USENIX office, submissionspolicy@usenix.org. Note, however, that we expect that many papers accepted for FOCI '11 will eventually be extended as full papers suitable for presentation at future conferences.

Papers accompanied by nondisclosure agreement forms will not be considered. Accepted submissions will be treated as confidential prior to publication on the USENIX FOCI '11 Web site; rejected submissions will be permanently treated as confidential.