Anticensorship in the Network

Eric Wustrow

Abstract:

Many countries restrict the information their citizens can access on the Internet by using a sophisticated censorship infrastructure to block websites, keywords, or communication that the government deems inappropriate. Although proxies can occasionally be used to circumvent such blocks, these proxies can themselves be discovered and blocked by the censor, resulting in an arms race between censors and circumventors.

In this talk, I will describe a fundamentally new approach to anticensorship that leverages the unique network perspective of ISPs to create proxies that make censoring an all-or-nothing decision. These proxies are designed to resist a censor’s attempt to detect or prevent usage, even when all information for using the proxy is made public. Blocking access to such a system involves additionally blocking economically or politically desirable sites unrelated to the censorship system, a cost that most censors are unwilling to pay. I will also describe the challenges to deploying this type of system in practice, as well as ongoing work to overcome these obstacles. Ultimately, these efforts enable a state-level response to state-sponsored censorship, giving sympathetic governments the tools needed to encourage Internet freedom.

Biography:

Eric Wustrow is a PhD candidate at the University of Michigan in Computer Security. His research focuses on systems security, network security, and developing technologies to support freedom and government transparency throughout the world. Previously, he has worked to expose vulnerabilities in insecure electronic voting systems in the US and abroad, detect widespread vulnerabilities in embedded systems on the Internet, and has developed new tools and techniques for circumventing Internet censorship in countries such as Iran and China. He is a recipient of a National Science Foundation Graduate Research Fellowship.