Date: 25th Nov 2021

Time: 11 am

Title: Network Anonymity, Privacy, (Anti-)Censorship and the Whole Nine Yards.

Speaker: Dr. Sambuddho Chakraborty

Abstract: Countries like China use (homebrewed) firewalling infrastructure to censor web traffic -- sometimes with the pretext of preserving cultural and religious values, at other times to prevent political dissent. While such countries are inherently (constitutionally) undemocratic, democracies like India have also suppressed ``free speech'' over the Internet. In this context,

It is natural to ask how free and open is the Internet and how robust it is to censorship by countries like India.

In this talk, I present an overview of our work over the years that has focussed on the evolution of India's Internet censorship infrastructure, how it censors traffic (and now apps.), and how various ISPs implement it. Further, I shall also present some of our research efforts to evade censorship (and also Internet shutdowns/blackouts). Our research shows that it would not be difficult to centrally co-ordinate Internet censorship in India, as the network is already quite centralized. A few ``key'' ASes (~ 1% of Indian ASes, i.e. <4) and routers (<5000) collectively intercept approximately 95% of paths to the censored sites and to all publicly-visible DNS resolvers. Further, our study of the evolution of the current censorship model observed that indeed, the censorship middleboxes are now intelligently positioned at only a few locations, but intercept a large fraction of network traffic. As of 2021, we have extensively explored the evolution of web censorship (HTTPS) along with exactly how Chinese apps are being filtered in the country.

Existing solutions to evade web censorship include applications like VPN services and Tor. These rely on a single (or cascade) of proxies to re-route traffic and protect network privacy from eavesdropping adversaries. However, all such solutions that rely on proxies are easily identifiable from their network traffic signatures. Futuristic solutions like Decoy Routing, which rely on routers that could double as ``smart proxies'', are resilient to such filtering. They have hitherto relied mostly on commodity servers, and involve wide-scale traffic observation, inadvertently posing a threat to the privacy of users who do not require such services. To that end, we devised a SDN-based DR solution, SiegeBreaker, that not only performs at line rates (comparable to native TCP) but also does not require inspection of all network flows, thus preserving the privacy of oblivious users.

Finally, I would conclude the talk with our new system Dolphin, which emulates old school dial-up modems, sans the ISP support, to relay Internet traffic especially in the face of Internet shutdowns. Dolphin's protocol recovers from the losses and errors introduced by the cellular voice medium, while also assuring end-to-end confidentiality. At low data rates (<=64bps), the errors are under 5% and suitable for supporting delay-tolerant applications with acceptable latencies. E.g. a 280 character tweet can be posted in about a minute.