CFEM & CTIC workshop:
Theory and Practice of Secure Multiparty Computation
May 30 to June 3, 2016
Aarhus University, Denmark

Title: Private Measurement of Tor

Aaron Johnson, Carnegie Mellon University, USA

The Tor network provides low-latency anonymous communication online to millions of users. Most of what happens within the Tor network is deliberately hidden to protect user privacy and is therefore unknown. This prevents Tor's developers and operators from understanding how the network is performing in order to improve it. It also prevents Tor from detecting attacks or abuses inside its network. Moreover, to the extent that Tor does measure itself, it does so either with high inaccuracy or using privacy-leaking techniques. We consider the application of privacy-preserving data-aggregation techniques to make useful measurements within Tor. We describe the PrivCount system that we developed for this purpose and report on lessons that we have learned during its use. We conclude by describing how general SMC protocols might be used to perform even more useful privacy-preserving measurements of Tor.