Laura M. Roberts

Princeton University

Traffic Correlation Attacks Using DNS

laurar@princeton.edu

Tor is a very popular anonymity network that is known to be susceptible to end-to-end traffic correlation attacks that can be performed by network-level adversaries such as ASes and IXPs. Previous work on such attacks has focused on the TCP streams while the accompanying DNS traffic has been completely ignored. In our work we study the nature of DNS resolution in Tor and how DNS traffic can be used by network-level adversaries to deanonymize Tor traffic. For example, we are investigating how DNS traffic can be used to boost the success of website fingerprinting attacks. Our contributions include drawing attention to the role DNS can play in Tor deanonymization attacks and improving upon earlier Tor measurement techniques in order to produce results and estimates that are more practical and realistic.