. In 2013, Johnson et al evaluated the security of Tor users over a period and showed that a network-layer adversary with deanonymize any user within three months with 50% probability and within six months with 80% probability using timing correlation. In 2015, Sun et al, showed that Routing Attacks on Privacy on Tor (RAPTOR) could detrimentally affect the security and privacy of Tor clients. RATPOR have been shown to been shown to be able to deanonymize users with 90% accuracy without any false positives by performing a longest a longest prefix attack for less than 5 minutes. In addition, network correlation, circuit linking, and BGP hijacking attacks have all been shown to effective attacks against the privacy of Tor clients

. Counter-RAPTOR and Trust-Aware Path Selection (TAPS) have elucidated methods of combating these types of attacks. Counter-Raptor seeks to maximize Tor clients’ resilience to hijack attacks by selecting a guard relay based on client location. In Taps, client ASes are grouped into clusters around representative ASes which limits the amount of information that can be learned observing how the client creates circuits. However, Tempest attacks these Tor privacy frameworks have been shown to degrade Tor client privacy over time. For Counter-RAPTOR, Tempest attacks show that use of the same guard relay degrades resilience of the guard as clients move to new countries. For TAPS, Tempest attacks show that repeated clustering on changing networks results in unique identification of ASes leading to intersection attacks. In Tempest, it is suggested to choose a few guards for possible client locations and change the guard depending on the current client location for Counter-RAPTORs approach and to use consistent clustering for TAPS, but leaves analysis for future study.

I propose to perform this analysis of the suggested methods for Counter RAPTOR and Taps to understand the privacy implications of the suggested methods. (Based on prior research the guard churn caused by selection of new guards as the user changes location, may leave the user more vulnerable for the Counter RAPTOR suggestion). Further I propose the following for the selection of the guard relay for the TAPS and Counter RAPTOR approaches.

I propose to quantify the privacy of guard selection using differential private algorithms for the Counter-Raptor and Taps approaches to Tor security. For TAPS, I propose using the DLP Lloyd algorithm to obtain provably consistent and private clustering of ASes over periods of time to prevent intersection attacks. I propose a similar clustering for Counter-RAPTOR as well because these clusters are still based on client location and with differentially private could allow the client to not give up as much privacy upon moving to a different physical location