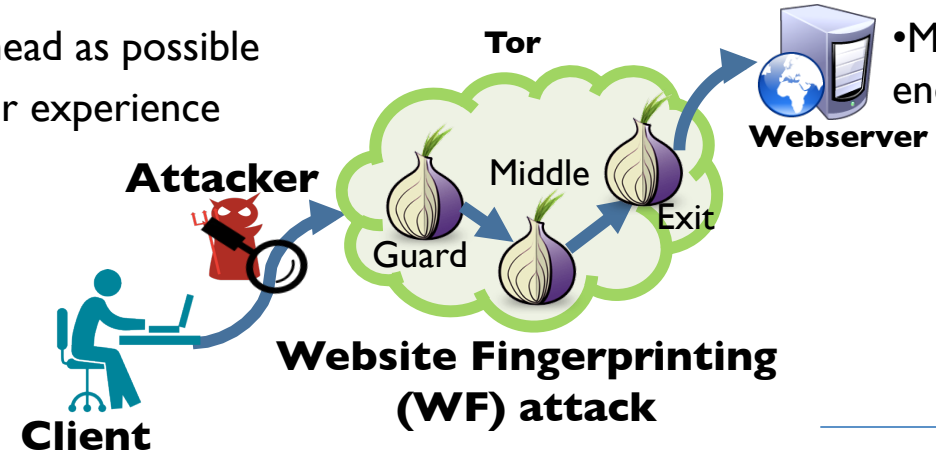
TTP: Defending Against Website Fingerprinting in Tor

Challenge

Website Fingerprinting (WF) attacks reveal a user's web browsing activity to an eavesdropper, even when using Tor. Goals:

- Prevent the attack
- Cost as little overhead as possible
- Provide a good user experience



Scientific Impact

- Reduces state-of-the-art attack from 90% accuracy to 17%
- No added latency, moderate bandwidth overhead.
- May also make more powerful end-to-end attacks harder.

Solution

- Pad the traffic with fake bursts of activity, masking key features used in WF algorithms
- Smart design converting the users traffic to the generic web traffic.
- TTP: Deploying it into Tor

Broader Impact

Tor is used by millions of people every day, including businesses, military intelligence, whistleblowers, and regular people. WF presents a dangerous threat to their privacy, so deploying a defense is critical.

Center for Cybersecurity

Dingledine, Perry, Wright