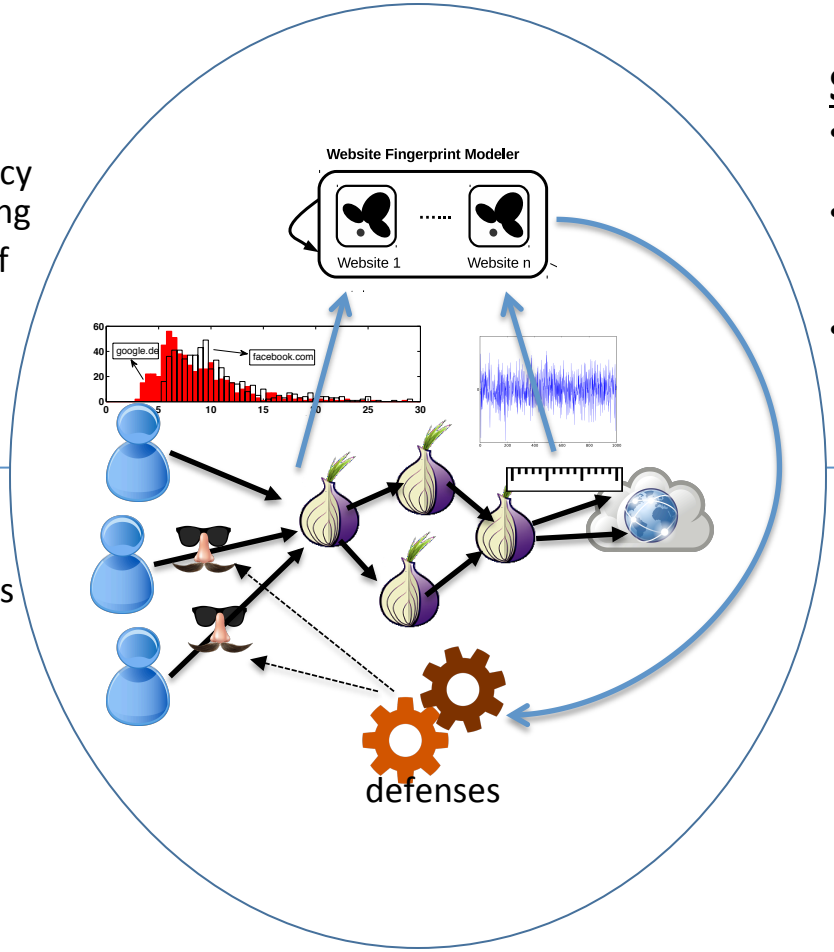
Models and Measurements for Website Fingerprinting

Challenge:

- Measure the realistic privacy risk of website fingerprinting
- While preserving privacy of Tor users
- Design efficient defenses that reduce the risk

Solution:

- Design probabilistic models of website fingerprints
- Use differentially-private algorithms to train the models on live network
- Tune defenses to create “false positive” clusters



Scientific Impact:

- Improved understanding of threats to anonymity systems
- New models, data, and methodology for evaluating of defense mechanisms
- New methods to protect against website fingerprinting attacks

Broader Impact:

- Improved measurements of privacy for ~10M daily Tor users
- Expected tech transfer of defensive techniques to improve the privacy of Tor users

NSF 1815757, University of Minnesota, PI: Nicholas Hopper (hoppernj@umn.edu)