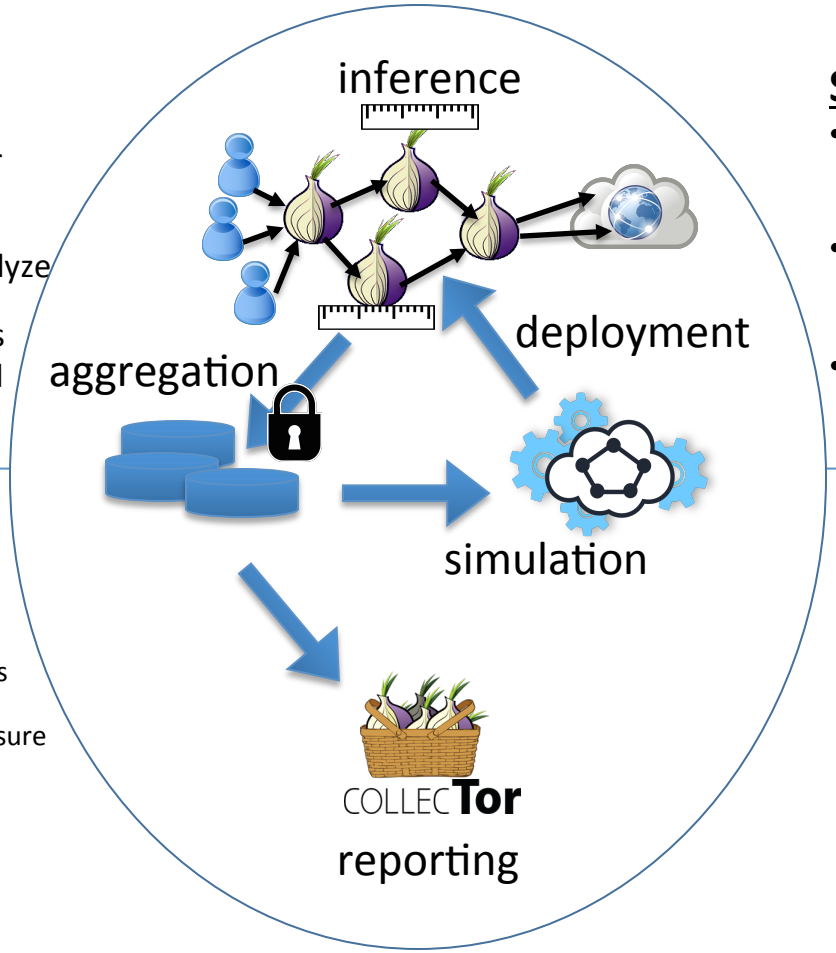
Measurement-Based Design and Analysis of Censorship Circumvention Schemes



Challenge:

- Safely measure use of Tor and similar private communication systems
- Safely and accurately analyze security and efficiency impacts of measurements
- Design new protocols and fine-tune existing ones based on results

Solution:

- Relays locally estimate global results
- Robust, differentially private aggregation of local inferences
- Simulation-based approach to proving "what is safe" to measure
- *Shadow* simulation engine for testing and deployment
- *CollecTor* site for reporting to broader community

CNS-1314637; University of Minnesota & The Tor Project; Nicholas Hopper, Roger Dingledine; hoppernj@umn.edu, arma@torproject.org

Scientific Impact:

- Improved understanding of security and performance impacts of Tor user behavior
- New algorithms, protocols and parameters to improve efficiency and privacy
- Aggregation techniques applicable to other privacy-preserving systems

Broader Impact:

- Improved privacy, performance for 2M daily Tor users
- Increased time to first compromise, network throughput
- More accurate, reliable statistics available to users, reporters