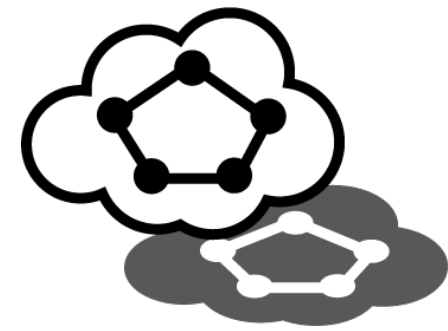


# Expanding Research Frontiers with a Next-Generation Anonymous Communication Experimentation (ACE) Framework



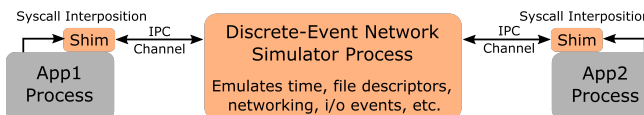
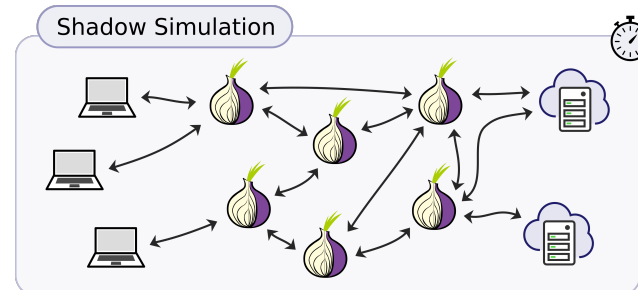
## Challenge:

- Lack of experimental frameworks for safely and accurately evaluating large-scale distributed systems
- Simulation is especially important for anonymity networks, since real-world experimentation can put actual users at risk
- High-fidelity simulation requires running unmodified application code (e.g., Tor)
- Existing simulators tend to focus on either compatibility (running existing code) or performance (via low-fidelity application abstractions), but not both

## Solution:

- Discrete-event network simulator that directly executes unmodified applications
- Uses seccomp-based multi-process architecture to offer better performance than existing uni-process simulators, while supporting more applications
- Time, network traffic, thread synchronization and more are all deterministically controlled, enabling reproducible experiments

ACE is integrated into Shadow to achieve large-scale high-performance network simulations for unmodified apps



## Scientific Impact:

- Enables improved experimentation and analysis of system security and performance in realistic settings against realistic adversaries
- Helps advance research on location- and network-aware communication, website fingerprinting attacks/defenses, and censorship circumvention

## Broader Impact and Broader Participation:

- ACE helps researchers develop protocols and tools that allow people to communicate more privately and securely
- ACE technologies have been added to Shadow, which is available for download at <https://shadow.github.io/>

CNS-1925497

Georgetown University (PI: Micah Sherr)

U.S. Naval Research Laboratory (PI: Rob Jansen)

Tor Project, Inc (PI: Roger Dingledine)