Hiding Amongst the Clouds: A Proposal for Cloud-Based Onion Routing

Nicholas Jones, Matvey Arye, Jacopo Cesareo, and Michael J. Freedman
Princeton University

Motivation

- Tor
  - Widely Used
  - Secure
  - Free to use
  - Poor performance: bandwidth limited by volunteers
  - Vulnerable to censorship: directories published publicly

System Overview

1. User sends cryptographic token to ASP
2. ASP relay receives token
3. Bank checks token validity
4. User adds relay to his circuit; repeats steps 1-3 for each additional relay

Monitoring Adversary

- Encrypted
- Inter-ASP Token Peering
- ASP 1 Token Bank
- ASP 2 Token Bank

Proposal

Cloud Based Onion Routing
- High speed, multi-homed connections
- Scale dynamically: add and remove relays as needed
- Censorship resistant: relays can easily change IP addresses
- Low cost
- Same secure backend as Tor
- Not free

Trust Model

- Tunnels built over multiple service and hosting providers
- Anonymity Service Providers (ASPs)
  - Purchase VM instances from cloud
  - Run COR relays within the cloud
  - Issue and redeem crypto tokens
- Cloud Hosting Providers (CHPs)
  - Provides infrastructure as a Service

Scale & Cost

- Dynamic provisioning: ASPs can create and destroy relays to meet changing demand
- Bandwidth costs dominate CPU costs
- Costs as low as 0.036c per MB

Access Control

- Cryptographic tokens provide access control while preserving privacy
- Cannot trace tokens between issuance and redemption
- Based on anonymous e-cash protocols

Censorship

- Nodes can easily change IP addresses within the cloud
- Cloud’s entire IP range must be blocked to censor COR
- Forces censors to inflict significant collateral damage

Benchmarks

- Consistently outperforms Tor in both multi-country and US only circuits
- Tested in both loaded and unloaded conditions using Alexa Top 10
- Each relay can easily support 100+ simultaneous users