Attacking and Improving the Tor Directory Protocol

Zhongtang Luo¹, Adithya Bhat¹, Kartik Nayak², Aniket Kate¹³
Purdue University¹, Duke University², Supra Oracle³
Appearing at IEEE S&P 2024

What is the Tor Directory Network?
- The Tor network enhances clients' privacy by routing traffic through an overlay network of volunteered intermediate relays.
- Tor employs a distributed protocol among nine hard-coded Directory Authority (DA) servers to securely disseminate information about these relays to produce a new consensus document every hour.

Cool. Why is it vulnerable?
- The Tor network itself does not defend against attacks on the relay list (e.g., Sybil relays, relays with irregular information). Therefore, all defense relies on external audits.
- Tor uses an outdated consensus system that uses two rounds of broadcast...

How can we attack the protocol?
An attacker needs to...
- Play nice with half of the authorities.
- Lie to the other half of the authorities and inject some incorrect information on the relay.
He can then run away with an incorrect relay list signed by a majority of the authorities without being found!

That sounds very convoluted. What is so bad about an incorrect relay list?

Figure: A demonstration of the attack from an experiment. Note the very large bandwidth 14597871 (although in a very small font).
The attacker can use incorrect parameters (e.g., very large bandwidth) to attract users to use only his relays, which totally breaks the anonymity without anyone finding out about it.

How should we fix it?
We provide two fixes:
- Patch the consensus health monitor so that it includes an equivocation detection mechanism
- Patch the protocol so that it is a robust consensus protocol

Figure: Inspired by the famous Dolev-Strong protocol, we design a protocol that secures the directory protocol.

Comparable performance with the original protocol!