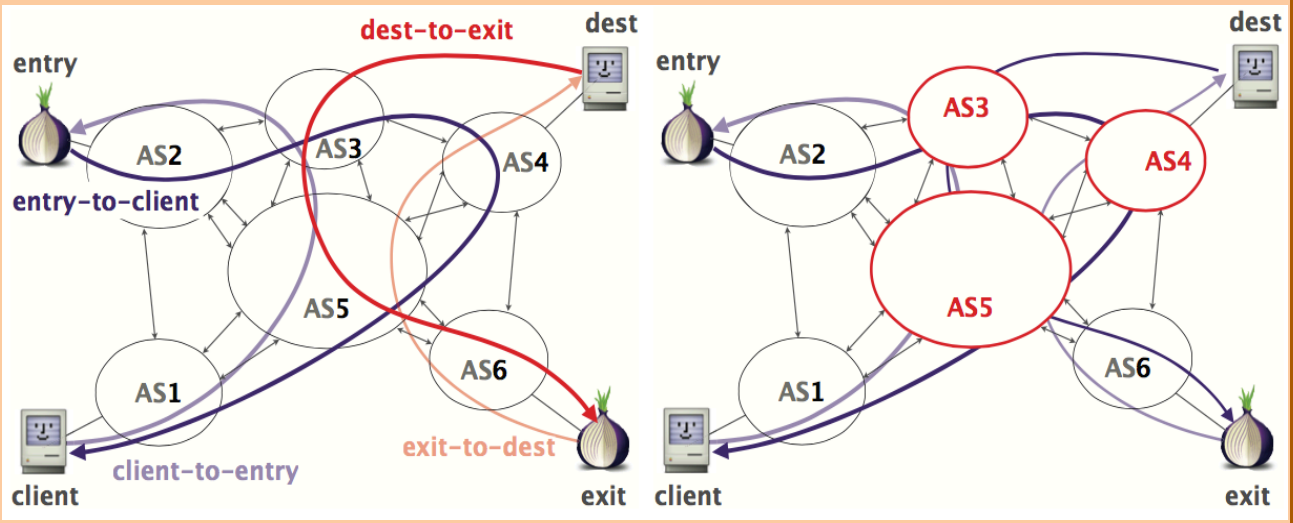
Anonymity Against AS-level Adversaries

The Challenge:

- Anonymity systems like Tor can be attacked by adversaries who control an AS.
- This AS-level adversary may attack Internet routing to see more traffic.



AS: A network in the Internet, from ISPs up to major networks like AT&T.

Adversary: If a compromised AS can see traffic from the Client to the Entry, and from the Exit to the Destination, then that AS can link the Client with her Destinations. ASes 3-5 can all deanonymize the user.

Our Studies:

- RAPTOR: a set of routing-based attacks called that show how much damage can be done (USENIX Sec.'15).
- DeNASA: IDs which ASes pose the most risk to users and avoids them. (PETS '16)
- New defenses against RAPTOR attacks are coming.
- Exploring cover traffic (ESORICS '16)

Scientific Impact:

- Understanding a new threat to anonymity.
- Exploring new approaches to defend against these threats.

Broader Impact:

- Stronger privacy: Activists, whistleblowers, journalists, businesses, military, law enforcement, regular users.
- Outreach: Summer Camps and 1-day events
- Education: New materials, Videos forthcoming

Awards: CNS-1423139
PIs: Prateek Mittal (Princeton) and Matt Wright (RIT)

PRINCETON UNIVERSITY

R·I·T