CAREER: Private Communication in Strongly Adversarial Networks
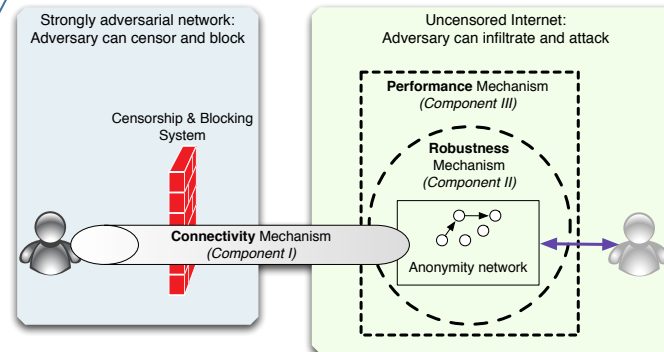
GEORGETOWN UNIVERSITY
17 89

Challenge:

- Existing privacy-enhancing technologies perform poorly when network is fully-controlled by a (state) adversary

- Adversary's abilities need to be understood and countered at all levels of protocol stack

Solution:

Provide unfiltered, anonymous, and high performance Internet access in networks controlled by a nation-state adversary:

- achieve connectivity via hidden channels that are difficult to block;
- improve the resilience of anonymity networks from DDoS and other attacks
- provide methods for high performance anonymous messaging

Strongly adversarial network:
Adversary can censor and block

Censorship & Blocking System

Connectivity Mechanism
(Component I)

Uncensored Internet:
Adversary can infiltrate and attack

Performance Mechanism
(Component III)

Robustness Mechanism
(Component II)

Anonymity network

Goal: **provide private communication in a strongly adversarial network** by
(1) improving connectivity;
(2) increasing robustness to attack; and
(3) improving performance

Scientific Impact:

- Develop new fully-decentralized routing protocols based on human mobility patterns

- Introduce algorithms for censorship detection using multiple vantage points

- Increase understanding of queuing properties in anonymous overlays

Broader Impact:

- Allow users, even in networks controlled by oppressive governments, to communicate privately

- Activities increase the participation of groups whose ability to communicate is currently muted

- Research components being added to coursework at Georgetown University