1. Routing and Traffic Analysis Attacks

- Force traffic to area under control
- Conduct traffic analysis attack
  - Website fingerprinting
  - End-to-end confirmation

Block guard by stressing

2. Denial of Service Mitigation in Tor

Client ▸ Circuit ▸ Entry Guard
IP: 123.456.7.8

- DoSConnectionMax Concurrent
  - Too many connections from IP address
- DoSCircuitCreationMinConnections
- DoSCircuitCreationRate
- DoSCircuitCreationBurst
  - Too many circuits from client

3. Preliminary Experiments: Stressing Features

Experiments Goal: Stress mitigation options and record behavior

4. Results

Logging the mitigation effects:
notice.log
info.log
DoS mitigation since startup: 0
circuits killed with too many cells.
5535 circuits rejected, 2 marked
addresses. 3390 connections closed.

5. Attacker Model

123.456.7.8
TCP Man-in-the-Middle

Requirement:
1. Spoof IP address
2. Connect and create circuits

Open Questions:
1. How to predict relays in the guard set?
2. Do we need to know this in advance?

Guard Set Prediction

6. Next Steps

Client ▸ Entry Guard

- Gather Empirical Data
  - Circuit buildup procedure
  - Timing relations of connections
  - Distribution of relays
- What if...? Empirical Simulation
  - Analysis of different scenarios
  - Statistical evaluation

7. Summary

Attack Concept:
1. Conduct routing attacks on the application layer
2. Empower traffic analysis attacks

Current Status:
1. Verify behavior of DoS mitigation features
2. Simulate and analyze impact