Planet Blackout: The Reach Of Global Censorship

Roya Ensafi
Simple observation

- Worldcup websites can be blocked
What's the goal?

- The global reach of censorship for popular domains from different sub-categories
- From 156 countries from geographically diverse vantage points
How do we measure?

• Using TCP/IP side channels
• In particular: hybrid idle scan that uses **IP identification** and **SYN backlog**

• Using DNS injection analysis by Ben Jones from Georgia Institute of Technology.
In a nutshell

- We can **manipulate** and **probe** shared resources (using IP spoofing)

[Diagram showing a network connection between Domain, UNM/ICSI, and Client, with 5 Spoofed SYNs and SYN/ACKs indicated.]
Ethical concerns

- Our hybrid idle scan create unsolicited traffic between a random global IPID client and a target domain.
Better solutions

- Not choosing end personal systems as a client:
  - Choosing routers
  - Choosing embedded systems