Berlin Institute of Technology
FG Security in Telecommunications

“Practical P2P-Based Censorship Resistance”

SPRING 6: SIDAR Graduierten-Workshop über Reaktive Sicherheit

Benjamin Michéle, March 21, 2011, Bochum, Germany
ben@sec.t-labs.tu-berlin.de

Agenda

- Introduction
- The problem – Censorship
- A solution – P2P and HTTPS proxies
- The details

Introduction

- People use Internet for many good things
  - Information acquisition
    - Google, news papers
  - Information publishing / expression of opinion
    - Blogs, Twitter
  - Social networking incl. organization of protest
    - Facebook

The Problem

- Threat to oppressive regimes' information monopole
- Citizens can
  - acquire too much information
  - publish “negative” information
  - mobilize against regimes

- Regimes apply firewalls to filter information
  - control what citizens know
  - suppress protest
  - prosecute dissidents

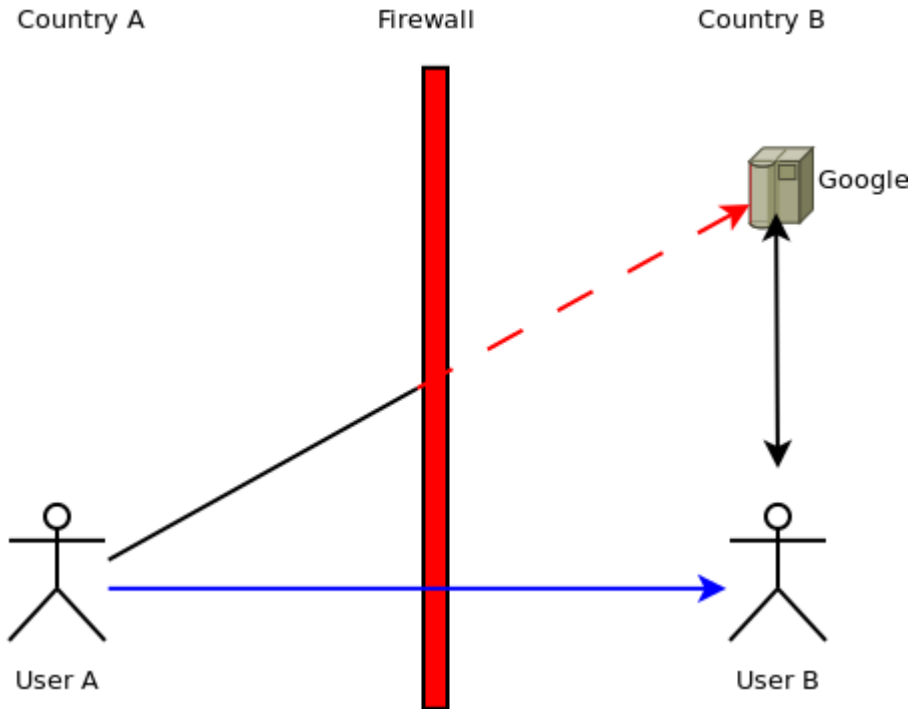
The Problem (cntd.)

- Need tools to circumvent firewall on a large scale
- Simple HTTP(S) Proxies
  - Easily blockable
- TOR
  - Built for anonymity rather than censorship resistance
  - Varying performance
- P2P-Based
  - Mainly academic

A Solution

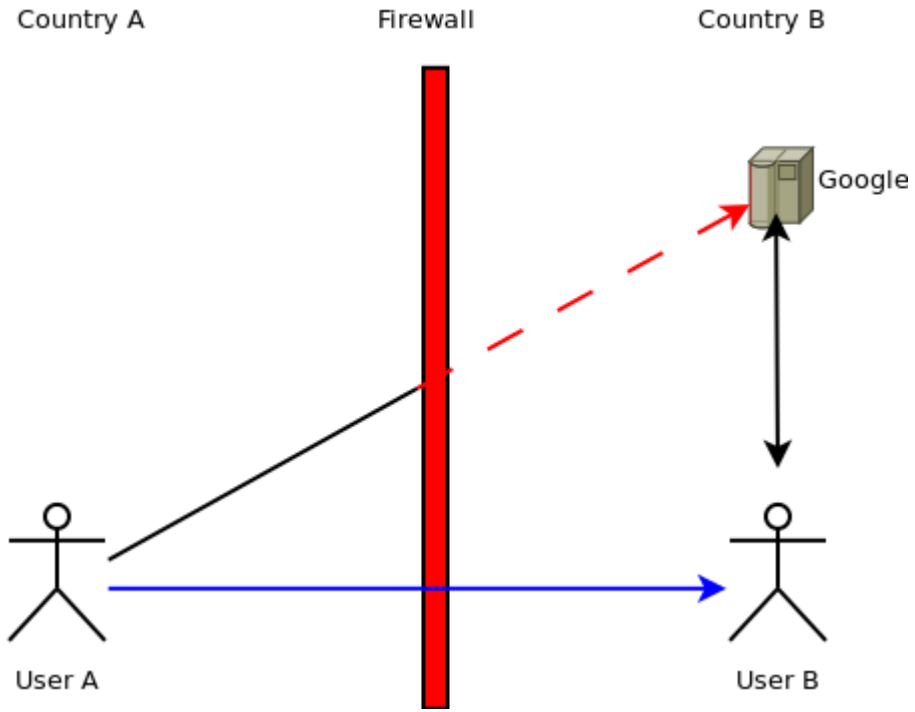
- Practical P2P-based HTTPS proxy
  - Nodes offer and use proxy service at the same time
  - Use existing DHT network for node lookup
  - Whitelist approach
  - Anti-forgery with signing servers

Details – Mode of Operation



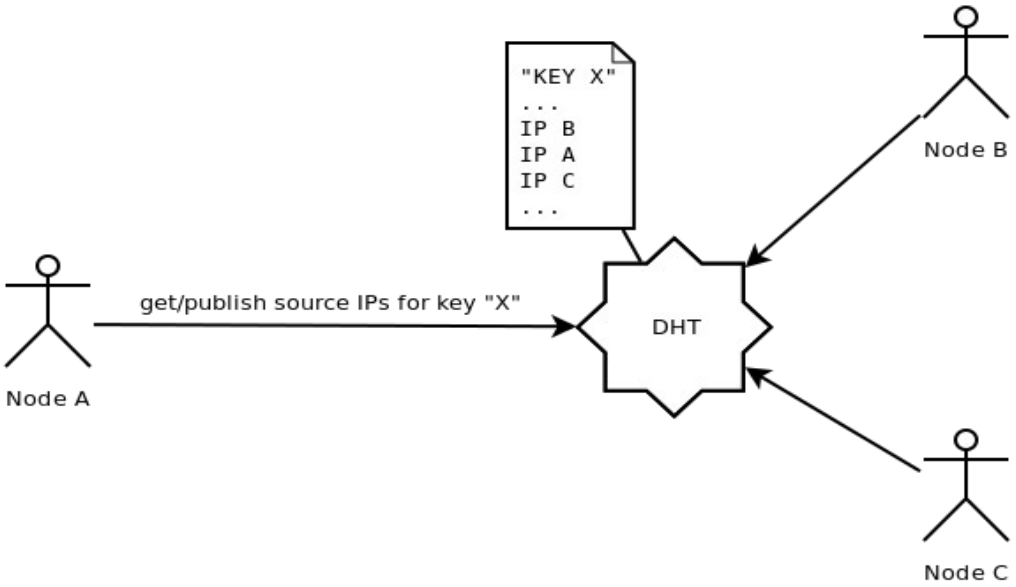
- HTTPS Proxy circumvents Firewall

Details – Mode of Operation



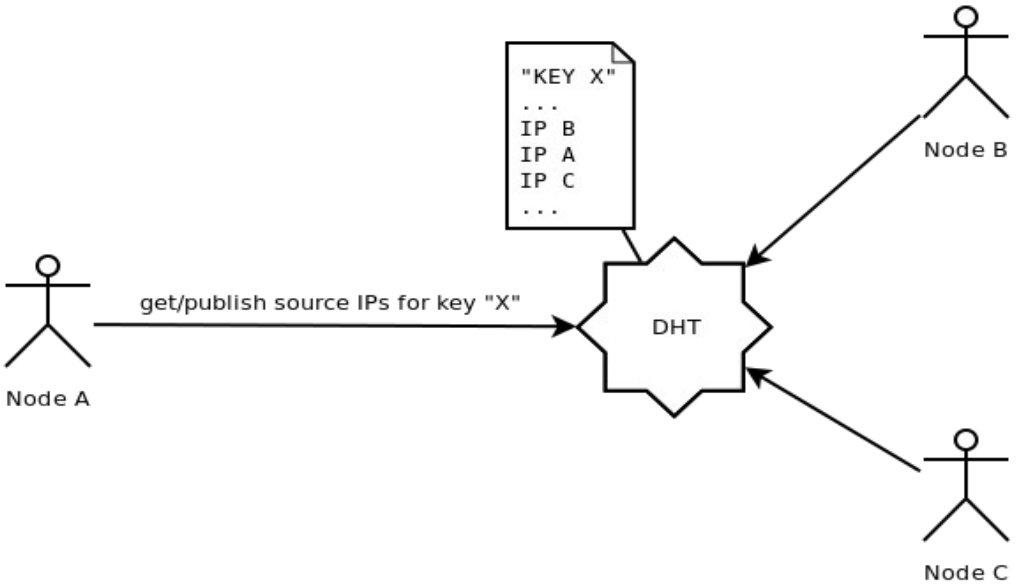
- HTTPS Proxy circumvents Firewall
- But how to find Proxy IPs?

Details – Node Discovery



- Publish own IP in DHT as source for key “X”
- Query source IPs for key “X”
- Quick variation of node list

Details – Node Discovery



- Publish own IP in DHT as source for key “X”
- Query source IPs for key “X”
- Quick variation of node list

- But how to detect IP spoofing?

Details – IP Signing Servers

- Central signing servers
- Generate signature for requesting IP address
- Nodes present this signature to prove their IP address
  - Not possible for firewall to generate fake signature
  - ➔ Cannot spoof IP

More Details

- Whitelisting – Only allow “legal” web sites
  - Google, news papers, Facebook, Twitter…
  - → Legal protection for relay nodes
- Only allow HTTPS traffic
  - → No eavesdropping on relay side

Questions?

Thank you!