Censorship-Resistant Architectures

Henry Tan    Micah Sherr

Georgetown University
Internet censorship is a problem in certain areas of the world. In some cases, censorship may be ubiquitous, e.g. government imposed censorship.

Users in these areas are

- unable to access restricted services
- are punished if they are observed accessing restricted services

Most existing services do not work against these powerful adversaries.
Existing Methods

Anonymity Services

- Tor - Relay traffic through a series of anonymizing routers.
- VPNs
- Anonymizing proxy websites etc.

Very effective for their designed purposes
Less so against censorship
Powerful Adversary known to control large portion of ‘nearby’ network.

- performs traffic analysis
- participates in any communication system
- controls some peers outside of censored region
Adversary’s Goals

The adversary wins if it
- discovers that Alice has been communicating with Bob
- is able to prevent Alice from communicating with Bob
1) Blocking off entire communication network/service

If a service:
- is dedicated to providing anonymity
- and can be identified by the adversary (e.g. entry IP addresses are published, differentiable traffic)
then the adversary can shutdown the entire network without repercussions

Solution

Build a general purpose communication system
- primary purpose is not censorship resistance
- provides cover traffic and encourages usage, e.g. in business.
2) Traffic Analysis

SkypeMorph: shape traffic as Skype traffic
FreeWave: encodes data stream as audio stream

Recent work shows that this may not be enough due to VBR encoding.

Solution
Avoid VBR encoding.
Ensure encoding schemes and traffic patterns are sufficiently similar among communication types
May imply inefficient traffic for data stream
Service’s IP Addresses must be published for clients to access them. Censor can also obtain and block these IP addresses.

**Solution**

Use trusted third parties to relay traffic to published destination. Same basic idea is used in Skype for reachability.
Approach #1 - Fully Centralized

Based on standard client/server model.
Broker controls network, users register with Broker
Approach #1 - Fully Centralized

Users are identified by usernames and broker does not reveal IP addresses. Broker disseminates public keys and binds keys to usernames.
Requirements and assumptions

**Broker**
- Does not collude with Adversary
- Is outside of Adversary’s influence
- Does not necessarily reveal Alice’s identity to Bob

**Use Cases**
More useful for multi-party communication, e.g. Google hangouts
Approach # 2 - Distributed

Users create certificates - `<username, public key, timestamp>` signed by a known and trusted root certificate authority.
Approach # 2 - Distributed

Alice contacts Charlie, a known and trusted friend. Charlie acts as a relay between Alice and Bob.
## Requirements and assumptions

### Intermediary (Charlie)
- Does not collude with Adversary
- Is outside of Adversary’s influence
- Does not reveal Alice’s identity to Bob

### Communication Network
- Allows for one way authentication (protect Alice’s identity)
- Has indirection capabilities built in and available on demand
In Conclusion …

Most existing systems are ineffective against a country level adversary. Use described architectures and techniques to build a general purpose censorship resistant network.