Challenges of Anonymous Communications

Sadia Afroz
UC Berkeley
Why Anonymous Communication?
Why Anonymous Communication?
Why Anonymous Communication?
Why Anonymous Communication?

Evade censorship!

forbidden.com

forbidden.com
Why Anonymous Communication?
Why Anonymous Communication?

This is Alice!
Why Anonymous Communication?
Why Anonymous Communication?

Protect privacy!

Entry  Middle  Exit  Google
Why Anonymous Communication?

Protect privacy!

Entry    Middle    Exit

Google
But ...

Google Sorry...

We're sorry...

... but your computer or network may be sending automated queries. To protect our users, we can't process your request right now.

See Google Help for more information.
This talk

Internet services are blocking Tor

Censors are blocking Tor
Internet services blocking Tor

- Network layer blocking
- Application layer blocking
Is Tor Blocked?

If R1 is successful, but R2 is unsuccessful then Tor is blocked
Network Layer Blocking

- SYN-ACK
- RST or No Response

Service
Network Layer Blocking

- Scan the entire IPv4 with open port 80 (over 3 billion IP addresses)
- 4 Tor exit nodes (USA, Netherland, Romania)
- 3 Control nodes (Berkeley, Michigan, Cambridge)
Network Layer Blocking

What if the response is lost?

SYN-ACK

Service

RST or No Response
Network Layer Blocking

- Web footprint:
  - Strict: Addresses that always respond from all the control nodes (over 52 million)
  - Lax: Addresses that respond at least once (over 103 million)
1.3 million IP addresses block Tor

- Wholesale blocking by ASNs: CHINANET and Airtel
- Content hosting and service providers: godaddy.com, and Dreamhost
Application Layer Blocking

HTTP GET
200 OK
Not 200
Application Layer Blocking

- HTTP request to Alexa top 1000 sites
- Once from Berkeley
- Once from every Tor exits (over 900)
- Scanned 5 days
Application Layer Blocking

- Over 3.5% of the top 1000 sites block Tor
- Individual sites: Yelp, craigslist
- CDNs: CloudFlare, Akamai
Example of Block Pages

Access Denied

You don't have permission to access "http://www.groupon.com/" on this server.

Reference #18.1a841402.1435475639.45cc72fb

Sorry, you're not allowed to access this page.

Your IP address is: e 212.117.180.65 78

Please retry your request and contact Yelp if you continue experiencing issues.
How many exits are blocked?
~20 sites block most of the exits

~60 sites block <25% of the exits
High bandwidth exits have higher chance of getting blocked
High bandwidth exits have higher chance of getting blocked
Akamai blocks most exits

Tor blocked by bestbuy.com

Exit probability

Fraction of webpages blocked

0% 3% 6% 9%

1e-06 1e-04 1e-02
Is Tor blocking new?

- Open Observatory Network Interference (OONI)
  - studies censorship in different countries
  - visits website through Tor and without Tor
  - over 2300 websites visited

http://api.ooni.io/
OONI data

Number of OONI http_requests reports per day
6.8% sites blocked Tor

Tor blocking rate over time

- timeout
- CloudFlare
- all others

Fraction of blocked requests

Solution?

• Anonymous blacklisting systems

• Contextual awareness:
  • redirect users to other exit nodes

• Redesigning anonymous networks:
  • charge small amount of money
  • fan out exit traffic

• Redesigning automated blocking:
  • activity based temporary blocking
Summary

- At least 1.3 million IP addresses block Tor
- At least 3.5% top Alexa 1000 sites block Tor
- Finer grained discrimination?
- Who else is second class citizen of the Internet?

Co-authors:
Sheharbano Khattak, David Fifield, Mobin Javed, Srikanth Sundaresan, Vern Paxson, Steven J. Murdoch, Damon McCoy
Censorship
Censorship

forbidden.com → forbidden.com
Censorship
Censorship

forbidden.com

Public Tor relay

Tor

forbidden.com
Censorship

forbidden.com
Public Tor relay
Non-public Tor relay

forbidden.com
Censorship

forbidden.com
Public Tor relay
Non-public Tor relay

forbidden.com
Censorship

forbidden.com

Public Tor relay

Non-public Tor relay

forbidden.com
We want to know

- How well a circumvention system works in practice?
- How does it compare to other systems?
Practical attacks on Tor

1. Using properties of the endpoints

Tor
Domain name
IP : Port

Does not possess

Tor
Practical attacks on Tor

1. Using properties of the endpoints

- Domain name
- IP : Port
- Does not possess

Happened in: Iran, China, Syria, Saudi Arabia, ...

15 of the 32 known cases
Practical attacks on Tor

2. Using properties of the protocol

- Tor
  - Cipher suite
  - SSL certificate lifetime
  - Is this SSL?
- Tor
  - Does not possess
Practical attacks on Tor

2. Using properties of the protocol

- Cipher suite
- SSL certificate lifetime
- Is this SSL?

Does not possess

Happened in: Iran, China, Syria, UAE, ...

14 of the 32 known cases
3. By unplugging the Internet


3 of the 32 known cases
Censor in real attacks

- Looks for the simplest features for blocking
  - scalable
  - low operational cost
  - low collateral damage
- Discovering the feature needs manual effort
Surveyed 34 academic and practical censorship circumvention approaches

Deployed tools

Research proposals

8
5
16
Research in censorship circumvention

- Surveyed 34 academic and practical censorship circumvention approaches

**Deployed tools**

- Obfs2/3/4
- Tor Sep 2011
- Skypemorph
- OSS

**Research proposals**

- 8
- 5
- 16

- Flash proxy
- Domain fronting
- OSS
Research in censorship circumvention

- What kind of attacks it defends?
- How?
Research in censorship circumvention

• What kind of attacks it defends?
  • end points, protocol, content

• How?
  • Polymorphism: Looking different
  • Steganography: Looking like something
Research Vs. Practice

Polymorphism on end points
Flash Proxy, VPN gate

Polymorphism on content
Obfs2, Obfs3, Obfs4

Steganography on content
Stegorotus, Skypemorph
Research Vs. Practice

- Development cost
- End game
- Operational cost
- Arms race
How to mitigate this gap?

• Practical evaluation criteria

• We found 60 different evaluation criteria

• Different papers use different evaluation criteria
Current evaluation criteria

The criteria fall under the following broad categories:

1. resistance to known attacks (e.g., address blocking, active probing),
2. cost of the evaders
3. collateral damage of the censor
4. performance,
5. traffic analysis,
6. usage.
New evaluation criteria

- **Total cost** of a system:
  - censor’s cost, user’s cost, system maintainer’s

- **Goodput**, how much productive traffic it enables
How to find censor’s cost?

- Check how long it takes to discover how to block a system

Blocking happens either before some major events or as soon as an event occurs
Summary

• No one evaluation criteria to compare circumvention systems

• Research and practical systems focus on different aspects of censorship

• List of attacks on Tor:

http://eecs.berkeley.edu/~sa499/tor_timeline.pdf