Tor: Online anonymity, privacy, and security.

Runa A. Sandvik
runa@torproject.org

12 September 2011

TorProject.org

About Runa

- Studied at the Norwegian University of Science and Technology
- Worked for the Tor Project during Google Summer of Code in 2009
- Developer, security researcher, translation coordinator

What are we talking about?

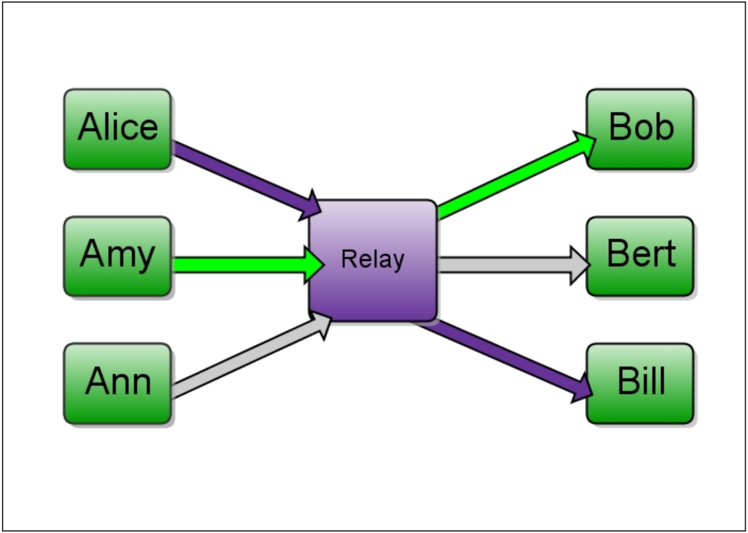
- Crash course on anonymous communications
- Quick overview of Tor
- Tor and circumvention
- Future work

The Tor Project, Inc.

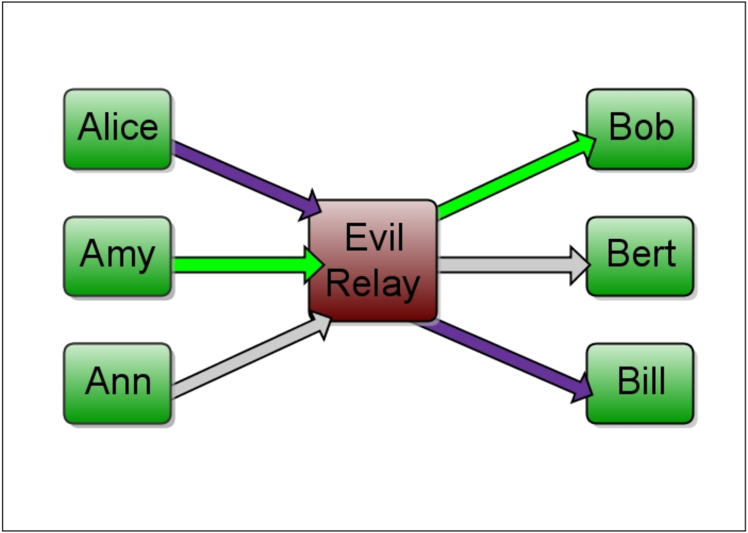
501(c)(3) non-profit organization dedicated to the research and development of technologies for online anonymity and privacy

What is anonymity?

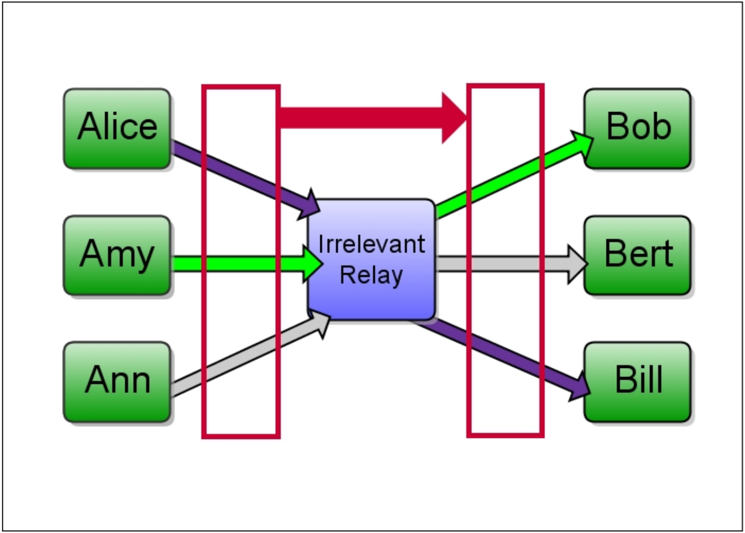
Threat model: what can the attacker do?



Threat model: what can the attacker do?

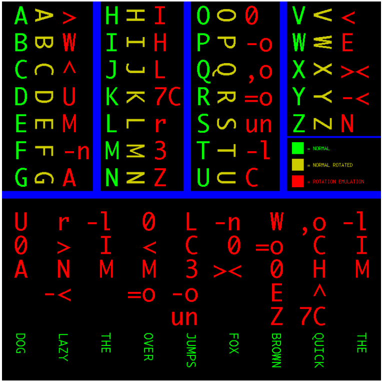


Threat model: what can the attacker do?



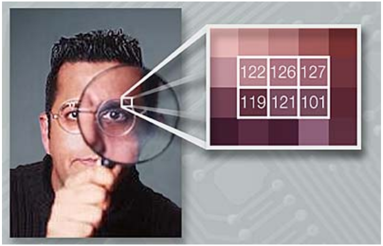
Anonymity isn't cryptography

- Cryptography protects the contents in transit
- You still know who is talking to whom, how often, and how much data is sent.



Anonymity isn't steganography

Attacker can tell Alice is talking to someone, how often, and how much data is sent.



Anonymity isn't just wishful thinking...

- "You can't prove it was me!"

Anonymity isn't just wishful thinking...

- "You can't prove it was me!"
- "Promise you won't look"

Anonymity isn't just wishful thinking...

- "You can't prove it was me!"
- "Promise you won't look"
- "Promise you won't remember"

Anonymity isn't just wishful thinking...

- "You can't prove it was me!"
- "Promise you won't look"
- "Promise you won't remember"
- "Promise you won't tell"

Anonymity isn’t just wishful thinking...

- "You can’t prove it was me!"
- "Promise you won’t look"
- "Promise you won’t remember"
- "Promise you won’t tell"
- "I didn’t write my name on it!"

Anonymity isn't just wishful thinking...

- "You can't prove it was me!"
- "Promise you won't look"
- "Promise you won't remember"
- "Promise you won't tell"
- "I didn't write my name on it!"
- "Isn't the Internet already anonymous?"

Anonymous communication

- People have to hide in a crowd of other people ("anonymity loves company")
- The goal of the system is to make all users look as similar as possible, to give a bigger crowd
- Hide who is communicating with whom
- Layered encryption and random delays hide correlation between input traffic and output traffic

Anonymity serves different interests for different user groups

- Private citizens: it's privacy
- Businesses: it's network security
- Governments: it's traffic-analysis resistance
- Human rights activists: it's reachability

What is Tor?

- Online anonymity software and network

What is Tor?

- Online anonymity software and network
- Open source, freely available (3-clause BSD license)

What is Tor?

- Online anonymity software and network
- Open source, freely available (3-clause BSD license)
- Active research environment:
  Rice, UMN, NSF, NRL, Drexel, Waterloo, Cambridge UK, Bamberg Germany, Boston Univ, Harvard, MIT, RPI, Georgia Tech

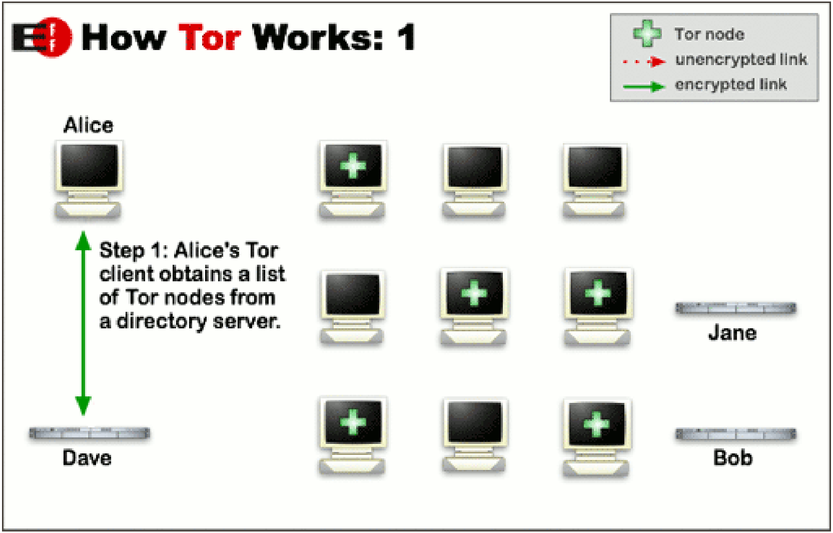
What is Tor?

- Online anonymity software and network
- Open source, freely available (3-clause BSD license)
- Active research environment:
  Rice, UMN, NSF, NRL, Drexel, Waterloo, Cambridge UK, Bamberg Germany, Boston Univ, Harvard, MIT, RPI, Georgia Tech
- Funding from US DoD, EFF, Voice of America, Google, NLNet, Human Rights Watch

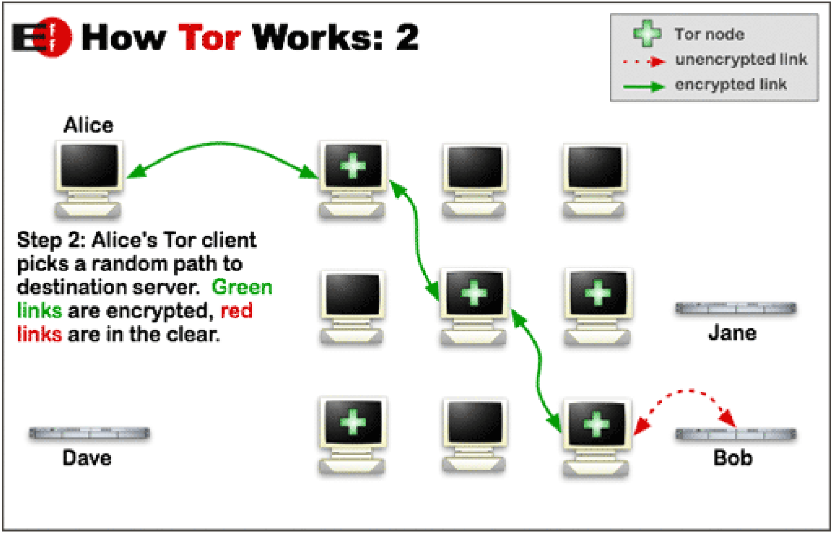
What is Tor?

- Online anonymity software and network
- Open source, freely available (3-clause BSD license)
- Active research environment:
  Rice, UMN, NSF, NRL, Drexel, Waterloo, Cambridge UK, Bamberg Germany, Boston Univ, Harvard, MIT, RPI, Georgia Tech
- Funding from US DoD, EFF, Voice of America, Google, NLNet, Human Rights Watch
- Increasingly diverse toolset:
  Tor, Torbutton, Tor Browser Bundle, TAILS Anonymous Operating System, Tor Weather, GetTor, Thandy, Orbot, Tor Check, Arm, Torouter, Tor Cloud and more

How is Tor different from other systems?


How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Jane
Dave
Bob

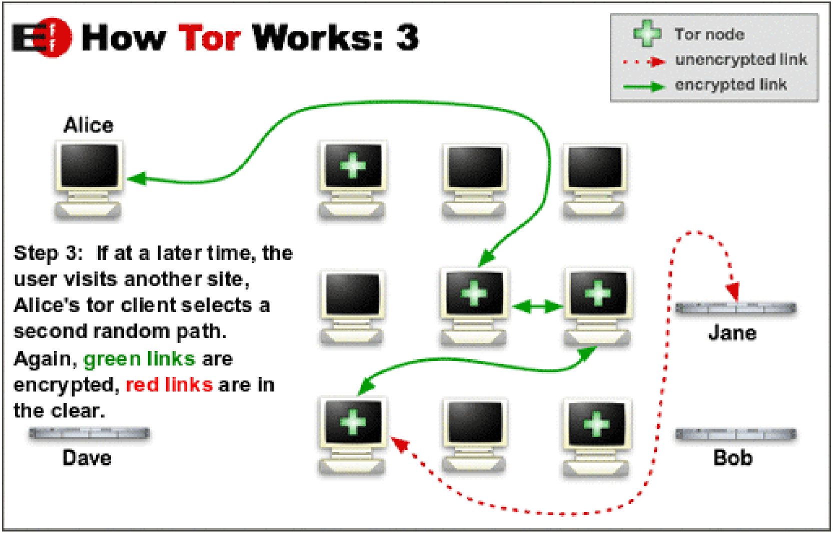
How is Tor different from other systems?



How Tor Works: 2

Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

How is Tor different from other systems?



How Tor Works: 3

Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

Tor uses a simple centralized directory protocol

- Relays publish self-signed descriptors to directory authorities
- Authorities publish a consensus list of all relay descriptors
- Clients download latest consensus from a directory authority or a directory cache

Bridges versus relays

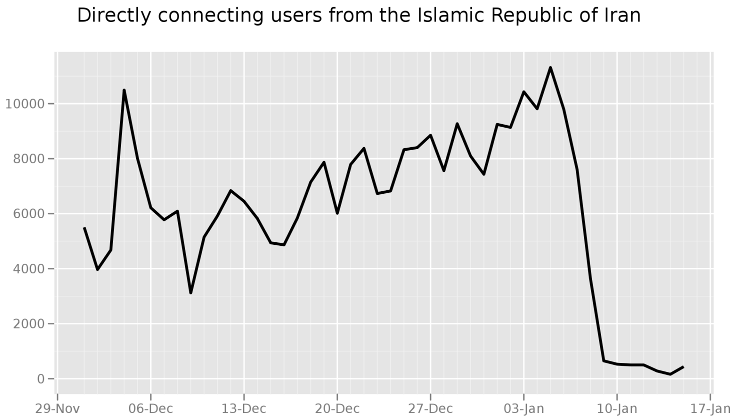
- A step forward in the blocking resistance race
- Bridge relays (or "bridges" for short) are Tor relays that aren't listed in the main Tor directory
- To use a bridge, you will need to locate one first (can be done using bridges.torproject.org, email, social media etc)
- A bridge will act as the first hop in the circuit

Hidden services

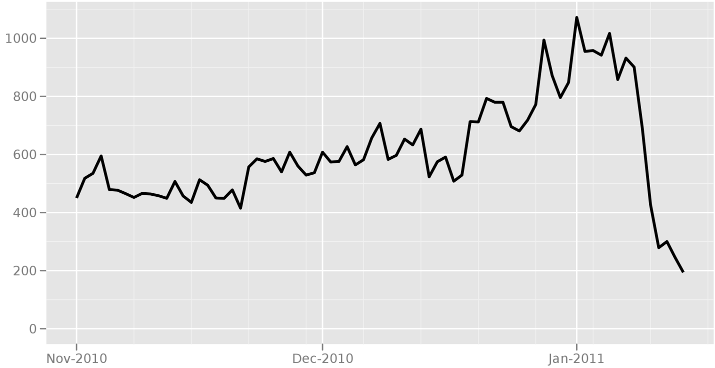
- Tor makes it possible for users to hide their locations while offering various kinds of services, such a website or an im server
- Using Tor "rendezvous points," other Tor users can connect to these hidden services, each without knowing the other's network identity
- A hidden service will have an address that ends in .onion, e.g. http://duskgytldkxiuqc6.onion/

Encryption

- Tor uses the 128-bit AES cipher in counter mode to generate a cipher stream
- And the signing keys are 1024-bit RSA
- We used to use a 1024-bit safe prime from RFC 2409, section 6.2 as the DH parameter...



The Tor Project - https://metrics.torproject.org/

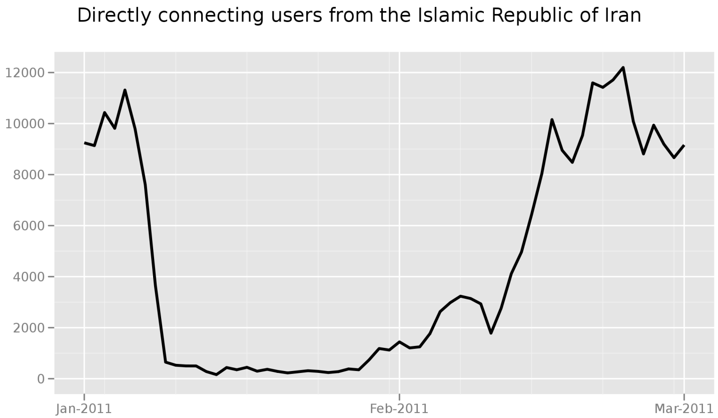


Bridge users from the Islamic Republic of Iran

The Tor Project - https://metrics.torproject.org/

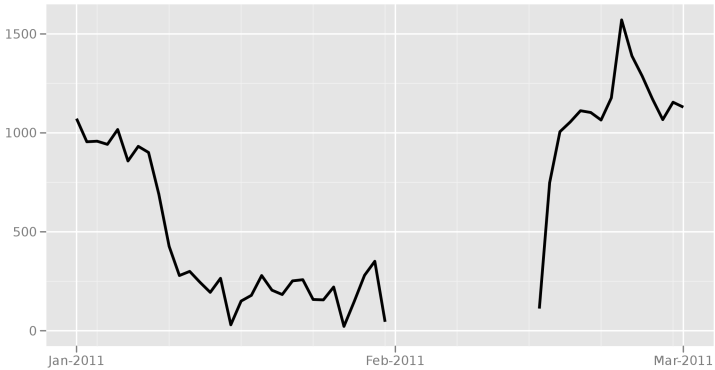
Encryption

- But then we made the DH parameter we use for TLS match the one from Apache's mod_ssl...



The Tor Project - https://metrics.torproject.org/

Bridge users from the Islamic Republic of Iran

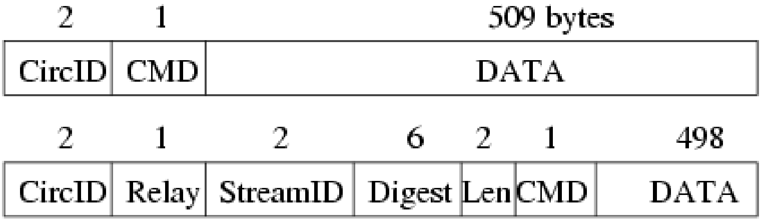


The Tor Project - https://metrics.torproject.org/

Keys

- Each relay maintains a long-term identity key and a short term onion key:
  - The identity key is used to sign relay descriptors
  - The directory authorities also use the identity key to sign the consensus
  - The onion key is used to decrypt requests from clients to set up a circuit and negotiate ephemeral keys
  - The TLS protocol also establishes a short-term link key when communicating between relays

Cells

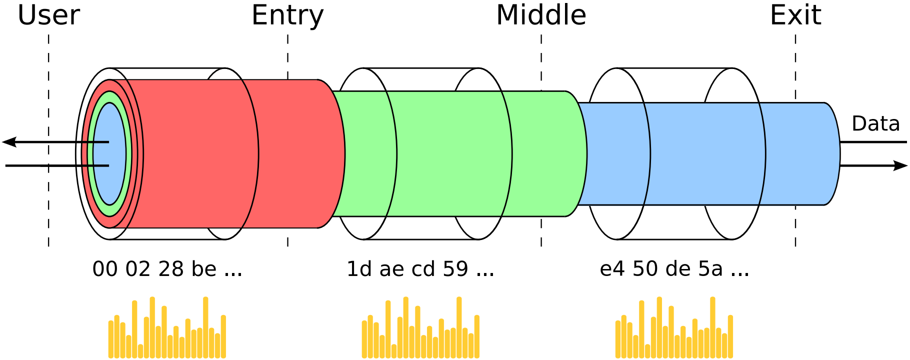


2	1	509 bytes
CircID	CMD	DATA

2	1	2	6	2	1	498
CircID	Relay	StreamID	Digest	Len	CMD	DATA

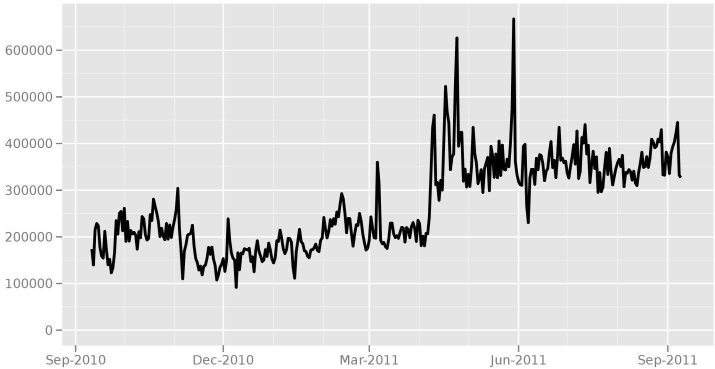
- Traffic passes along circuits in the Tor network in fixed-size cells (512 bytes):
    - The header includes a circuit identifier that specifies which circuit the cell refers to
    - The command describes what to do with the cells payload
    - The entire contents of the header and payload is encrypted/decrypted together as the relay cell moves along the circuit

Tor on the wire



How many people use Tor daily?

Directly connecting users from all countries

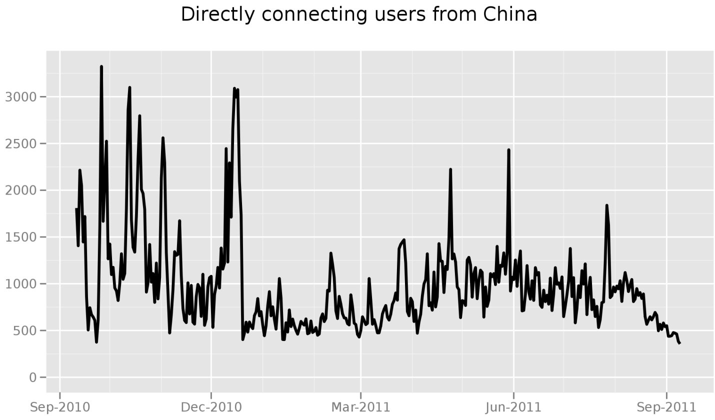


The Tor Project - https://metrics.torproject.org/

Attackers can block access to the network

- By blocking access to the directory authorities
- By blocking access to all the relays in the network
- By blocking access to all known bridges in the network
- By preventing users from finding the software

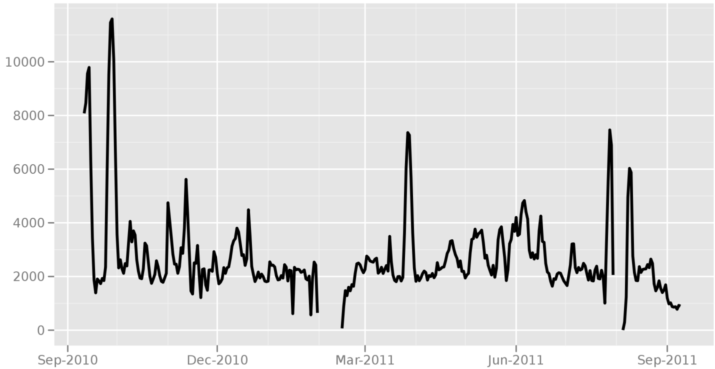
Tor and circumvention in China



The Tor Project - https://metrics.torproject.org/

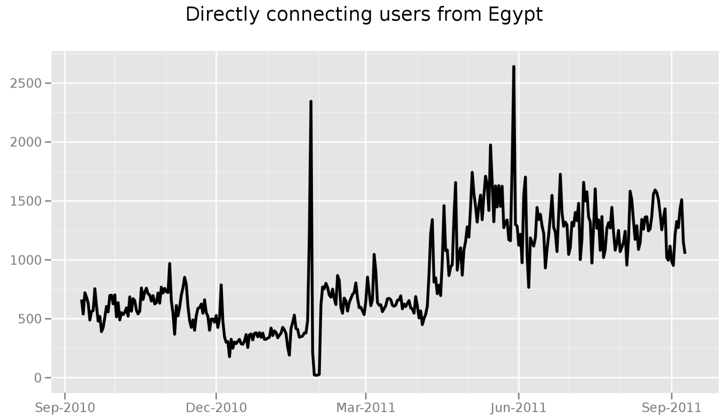
Tor and circumvention in China

Bridge users from China



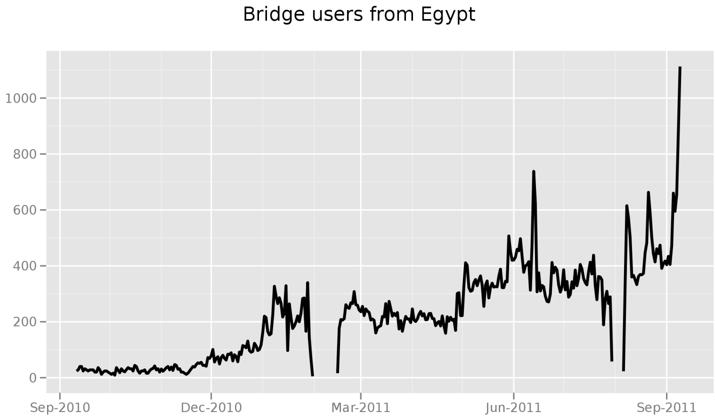
The Tor Project - https://metrics.torproject.org/

Tor and circumvention in Egypt



The Tor Project - https://metrics.torproject.org/

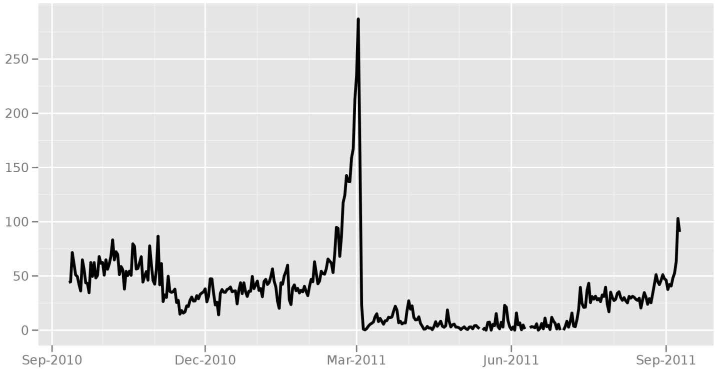
Tor and circumvention in Egypt



The Tor Project - https://metrics.torproject.org/

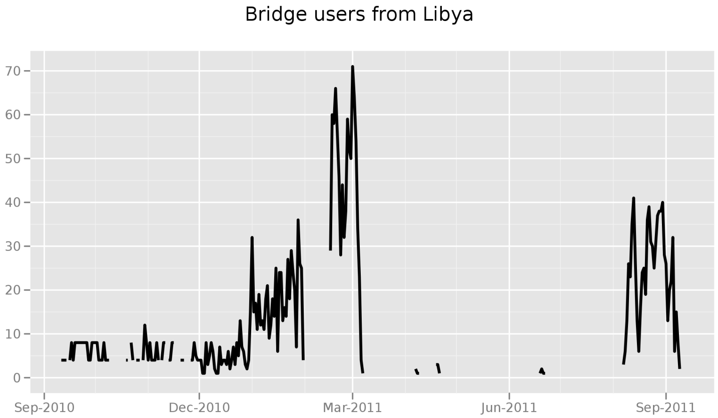
Tor and circumvention in Libya

Directly connecting users from Libya



The Tor Project - https://metrics.torproject.org/

Tor and circumvention in Libya



The Tor Project - https://metrics.torproject.org/

Future work, part 1

- The Torouter project: hardware project to provide an easy to setup Tor bridge or relay
- The Tor Cloud project: provides bridge-by-default and relay-by-default images for Amazon EC2

Future work, part 2

- Pluggable transports: a plug-in system that can evade many censorship systems by disguising Tor traffic as, for example, standard HTTP traffic
- Obfuscated proxy: protocol obfuscation for TCP protocols prevent third party from identifying protocol based on message contents

Future work, part 3

- Censorship resistance research: reachability testing of the Tor network from within certain countries
- IPv6: goal for Tor 0.2.3.x is for bridges to handle IPv6-only clients and exits can handle IPv6 addresses

Time for a demo

Demonstration of Tor Browser Bundle

Questions?

runa@torproject.org
https://www.torproject.org/