The Tor Project

Our mission is to be the global resource for technology, advocacy, research and education in the ongoing pursuit of freedom of speech, privacy rights online, and censorship circumvention.
What is Tor?

Online anonymity 1) open source software, 2) network, 3) protocol
Community of researchers, developers, users, and relay operators
Funding from US DoD, Electronic Frontier Foundation, Voice of America, Google, NLnet, Human Rights Watch, NSF, US State Dept, SIDA, Knight Foundation, ...
The Tor Project, Inc.

501(c)(3) non-profit organization dedicated to the research and development of tools for online anonymity and privacy.
Estimated 1,000,000+ daily Tor users
Threat model: what can the attacker do?

- Alice
- Anonymity network
- Bob

- watch Alice!
- Control part of the network!
- watch (or be!) Bob!
Anonymity isn't encryption: Encryption just protects contents.
Anonymity serves different interests for different user groups.

- **Governments**: “It's traffic-analysis resistance!”
- **Businesses**: “It's network security!”
- **Private citizens**: “It's privacy!”
- **Human rights activists**: “It's reachability!”

Diagram:
- Anonymity connects:
  - Governments
  - Businesses
  - Private citizens
  - Human rights activists
Current situation: Bad people on the Internet are doing fine

- Trojans
- Viruses
- Exploits
- Botnets
- Zombies
- Espionage
- DDoS
- Extortion
- Spam
- Phishing
The simplest designs use a single relay to hide connections.

(example: some commercial proxy providers)
But a single relay (or eavesdropper!) is a single point of failure.
... or a single point of bypass.

Timing analysis bridges all connections through relay \( \Rightarrow \) An attractive fat target
So, add multiple relays so that no single one can betray Alice.
Alice makes a session key with R1
...And then tunnels to R2...and to R3
Tor's safety comes from diversity

• #1: Diversity of relays. The more relays we have and the more diverse they are, the fewer attackers are in a position to do traffic confirmation. (Research problem: measuring diversity over time)

• #2: Diversity of users and reasons to use it. 50000 users in Iran means almost all of them are normal citizens.
Tor's anonymity comes from...

- The first 1,000 relays (location diversity)
- The first 100,000 users (user diversity)
- The last 1,000,000 users (end-to-end correlation resistance)
Attackers can block users from connecting to the Tor network

1) By blocking the directory authorities
2) By blocking all the relay IP addresses in the directory, or the addresses of other Tor services
3) By filtering based on Tor's network fingerprint
4) By preventing users from finding the Tor software (usually by blocking website)
Directly connecting users from the Islamic Republic of Iran

The Tor Project - https://metrics.torproject.org/
Directly connecting users from Iran

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

obfsproxy client | CENSOR | obfsproxy server

Tor Client | Tor Bridge
Two paradigms

- “Look like nothing”
- “Look like something they expect”

- Active probing: what should your service look like if the client doesn't auth right?
- “Be not there” vs “Be innocent service”
Pluggable transports

- Flashproxy (Stanford), websocket
- FTEProxy (Portland St), http via regex
- Stegotorus (SRI/CMU), http
- Skypemorph (Waterloo), Skype video
- uProxy (Google/UW), webrtc
- Lantern (BNS), social network based
- ScrambleSuit (Karlstad), obfs-based
- Telex (Michigan/Waterloo), traffic divert
meek-server

INTERNET

tor

Browser

meek-client

SNI: www.google.com (front domain)
Host: meek-reflect.appspot.com (actual destination)

HTTPS

Google frontend server

meek-reflect.appspot.com

www.google.com
maps.google.com
drive.google.com
gmail.com...

HTTP

tor
meek-server
“Still the King of high secure, low latency Internet Anonymity”

Contenders for the throne:

• None
NSA targets the privacy-conscious
von J. Appelbaum, A. Gibson, J. Goetz, V. Kabisch, L. Kampf, L. Ryge

One of NSA's German targets is 212.212.245.170. The string of numbers is an IP address assigned to Sebastian Hahn, a computer science student at the University of Erlangen. Hahn operates the server out of a grey high-security building a few kilometers from where he lives. Hahn, 28 years old and sporting a red beard, volunteers for the Tor Project in his free time. He is especially trusted by the Tor community, as his server is not just a node, it is a so-called Directory Authority. There are nine of these worldwide, and they are central to the Tor Network, as they contain an index of all Tor nodes. A user's traffic is automatically directed to one of the directory authorities to download the newest list of Tor relays generated each hour.

Hahn's predecessor named the server Gabelmoo, or Fork Man, the nickname of a local statue of Poseidon. After a look at the NSA source code, Hahn quickly found his predecessor listed in...
Pervasive surveillance

- Design changes to improve robustness
- Internet is more centralized than we'd like
- Defending against end-to-end correlation attacks is a good idea in theory
- Surveillance (DPI) and censorship (DPI) more related than we realized
Client registers its address using secure rendezvous

1. Client
2. Proxy polls
3. Facilitator responds with address
4. Proxy connects to client
5. Proxy connects to relay

Facilitator

Censor

Tor relay
Transport plugin

Flash proxy (web browser)
Transport plugin

to Tor