Tor: a quick overview

Roger Dingledine
The Tor Project
https://torproject.org/
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, ...
501(c)(3) non-profit organization dedicated to the research and development of tools for online anonymity and privacy.
Estimated 500,000 daily Tor users
Threat model: what can the attacker do?

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

“It's privacy!”

Private citizens
Anonymity serves different interests for different user groups.

- Private citizens: “It's privacy!”
- Businesses: “It's network security!”

Anonymity
Anonymity serves different interests for different user groups.

"It's traffic-analysis resistance!"

Governments

Anonymity

Private citizens

"It's privacy!"

Businesses

"It's network security!"
Anonymity serves different interests for different user groups.

- Governments
  - “It's traffic-analysis resistance!”

- Human rights activists
  - “It's reachability!”

- Private citizens
  - “It's privacy!”

- Businesses
  - “It's network security!”
Regular citizens don't want to be watched and tracked.

Hostile Bob

Incompetent Bob

Indifferent Bob

“I sell the logs.”

“Oops, I lost the logs.”
The AOL fiasco

“Hey, they aren't my secrets.”

(the network can track too)

Name, address, age, friends, interests (medical, financial, etc), unpopular opinions, illegal opinions....

Blogger Alice

8-year-old Alice

Sick Alice

Consumer Alice

Oppressed Alice

...
Businesses need to keep trade secrets.

“Oh, your employees are reading our patents/jobs page/product sheets?”

“Hey, it's Alice! Give her the 'Alice' version!”

“Wanna buy a list of Alice's suppliers? What about her customers? What about her engineering department's favorite search terms?”
Law enforcement needs anonymity to get the job done.

“Why is alice.localpolice.gov reading my website?”

“Why no, alice.localpolice.gov! I would never sell counterfeits on ebay!”

“Is my family safe if I go after these guys?”

“Are they really going to ensure my anonymity?”
Governments need anonymity for their security

“What will you bid for a list of Baghdad IP addresses that get email from .gov?”

“What about insiders?”

“What does FBI Google for?”

“Do I really want to reveal my internal network topology?”

“What about insiders?”
Journalists and activists need Tor for their personal safety

Activist/Whistleblower Alice

- Monitoring ISP
- Monitored website
- Filtered website
- Monitored network

“Did you just post to that website?”

“Where are the bloggers connecting from?”
“Did you just post to that website?”

“I run livejournal and track my users”
“Of course I tell China about my users”

“What does the Global Voices website say today?”

“I want to tell people what's going on in my country”

“I think they're watching. I'm not even going to try.”
You can't get anonymity on your own: private solutions are ineffective...

- Citizen Alice
- Alice's small anonymity net
- Municipal anonymity net
- Officer Alice
- Investigated suspect
- AliceCorp
- AliceCorp anonymity net
- Competitor

"One of the 25 users on AliceNet."

"Looks like a cop."

"It's somebody at AliceCorp!"
... so, anonymity loves company!

Citizen Alice

Officer Alice

AliceCorp

Shared anonymity net

Investigated suspect

Competitor

“???”

“???”

“???”
Yes, bad people need anonymity too. But they are already doing well.

Evil Criminal Alice

- Compromised botnet
- Stolen mobile phones
- Open wireless nets
- .....
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.
A corrupt first hop can tell that Alice is talking, but not to whom.
A corrupt final hop can tell that somebody is talking to Bob, but not who.
Alice makes a session key with R1
...And then tunnels to R2...and to R3
Number of relays

The Tor Project - https://metrics.torproject.org/
Total relay bandwidth

Advertised bandwidth
Bandwidth history

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

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

The Tor Project - https://metrics.torproject.org/
Directly connecting users from the Syrian Arab Republic

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

The Tor Project - https://metrics.torproject.org/
What we spend our time on

Performance and scalability
Maintaining the whole software ecosystem
Blocking-resistance (circumvention)
Basic research on anonymity
Reusability and modularity
Advocacy, education, and trainings around the world
Metrics, data, and analysis
Javascrip, cookies, history, etc

Javascript refresh attack
Cookies, History, browser window size, user-agent, language, http auth, ...
Our Torbutton Firefox extension tackles many of these
Flash is dangerous too

Some apps are bad at obeying their proxy settings.

Adobe PDF plugin. Flash. Other plugins. Extensions. Especially Windows stuff: did you know that Microsoft Word is a network app?
Choose how to install it

- Tor Browser Bundle: standalone Windows exe with Tor, Vidalia, Firefox, Torbutton, e.g. for USB stick
- Tails Linux LiveCD
Run as a client only
- Relay traffic for the Tor network
- Help censored users reach the Tor network

Basic Settings  Bandwidth Limits  Exit Policies

What internet resources should users be able to access from your relay?

- Websites
- Secure Websites (SSL)
- Retrieve Mail (POP, IMAP)
- Instant Messaging (IM)
- Internet Relay Chat (IRC)
- Misc Other Services

Tor will still block some outgoing mail and file sharing applications by default to reduce spam and other abuse.
Step 1: Bob picks some introduction points and builds circuits to them.
Step 2: Bob advertises his hidden service -- XYZ.onion -- at the database.
Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.
Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.
Step 5: Bob connects to the Alice’s rendezvous point and provides her one-time secret.
**Hidden Services: 6**

**Step 6:** Bob and Alice proceed to use their Tor circuits like normal.

*Diagram showing the network setup with various nodes labeled as IP1, IP2, IP3, DB, RP, and Tor cloud.*

*Legend:*
- Tor cloud
- Tor circuit
- IP1-3: Introduction points
- PK: Public key
- cookie: One-time secret
- RP: Rendezvous point
Tor is only a piece of the puzzle

• Assume the users aren't attacked by their hardware and software
  – No spyware installed, no cameras watching their screens, etc
• Assume the users can fetch a genuine copy of Tor: from a friend, via PGP signatures, etc.
Advocacy and education

- Unending stream of people (e.g. in DC) who make critical policy decisions without much technical background
- Worse, there's a high churn rate
- Need to teach policy-makers, business leaders, law enforcement, journalists, ...
- Data retention? Internet driver's license?
I CAN HAZ FREEDOM?

TorProject.org
Lessons?

1) Bad people don't need Tor. They're doing fine.
2) Honest people need more security/privacy/anonymity.
3) Law enforcement benefits from it too.
4) Tor is not unbreakable.