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, ...
The Tor Project, Inc.

501(c)(3) non-profit organization dedicated to the research and development of tools for online anonymity and privacy
Estimated 600,000 daily Tor users
Threat model: what can the attacker do?

Alice
watch Alice!

Anonymity network
Control part of the network!

Bob
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!"
Anonymity serves different interests for different user groups.

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

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

- Blogger Alice
- 8-year-old Alice
- Sick Alice
- Consumer Alice
- Oppressed Alice
- Name, address, age, friends, interests (medical, financial, etc), unpopular opinions, illegal opinions....
- Hostile Bob: "I sell the logs."
- Incompetent Bob: "Oops, I lost the logs."
- Indifferent Bob: "Hey, they aren't my secrets."

The AOL fiasco: (the network can track too)
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.

Officer Alice

- Investigated suspect
  - "Why is alice.localpolice.gov reading my website?"

- Sting target
  - "Why no, alice.localpolice.gov! I would never sell counterfeits on ebay!"

- Organized Crime
  - "Is my family safe if I go after these guys?"

Witness/informer Alice

- Anonymous tips
  - "Are they really going to ensure my anonymity?"
Governments need anonymity for their security

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

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

“What does FBI Google for?”

“Somebody in that hotel room just checked his Navy.mil mail!”

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

Activist/Whistleblower Alice

Monitoring ISP

“Did you just post to that website?”

Monitored website

“Where are the bloggers connecting from?”
“I run livejournal and track my users”
“Of course I tell China about my users”

Filtered website

“What does the Global Voices website say today?”
“I want to tell people what's going on in my country”

Monitored network

“I think they're watching. I'm not even going to try.”

Blocked Alice
You can't get anonymity on your own: private solutions are ineffective...

Citizen Alice → Alice's small anonymity net → ... → “One of the 25 users on AliceNet.”

Officer Alice → Municipal anonymity net → Investigated suspect → “Looks like a cop.”

AliceCorp → AliceCorp anonymity net → Competitor → “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.
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 ⇒ 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
Directly connecting users from all countries

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

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

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

The Tor Project - https://metrics.torproject.org/
China (September 2009)

• China grabbed the list of public relays and blocked them
• They also enumerated one of the three bridge buckets (the ones available via https://bridges.torproject.org/)
• But they missed the other bridge buckets.
Relay versus Discovery

There are two pieces to all these “proxying” schemes:

- a **relay** component: building circuits, sending traffic over them, getting the crypto right
- a **discovery** component: learning what relays are available
The basic Tor design uses a simple centralized directory protocol.

Servers publish self-signed descriptors. Authorities publish a consensus list of all descriptors. Alice downloads consensus and descriptors from anywhere.
How do you find a bridge?

1) https://bridges.torproject.org/ will tell you a few based on time and your IP address
2) Mail bridges@torproject.org from a gmail address and we'll send you a few
3) I mail some to a friend in Shanghai who distributes them via his social network
4) You can set up your own private bridge and tell your target users directly
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)
Error: The requested page is unavailable.

If you believe the requested page should not be blocked please click here.

For more information about internet service in Saudi Arabia, please click here: www.internet.gov.sa

Access to this site is currently blocked. The site falls under the Prohibited Content Categories of the UAE's Internet Access Management Policy.
Chinese Tor users via bridges
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
Javascript, 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?
Tor Browser Bundle (TBB)
Tails (Tor LiveCD)

The Amnesic Incognito Live System
Orbot (Tor for Android)
Tor pluggable transports
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.
Step 6: Bob and Alice proceed to use their Tor circuits like normal.
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.