Tor: a quick overview

Roger Dingledine
The Tor Project
https://torproject.org/
What is Tor?

- Online anonymity software and network
- Open source, freely available
- Community of researchers, developers, users, and relay operators
The Tor Project, Inc.

• 501(c)(3) non-profit organization dedicated to the research and development of tools for online anonymity and privacy.
Estimated 300,000 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 cryptography: Cryptography just protects contents.

Alice

“Hi, Bob!”

<gibberish>

attacker

“Hi, Bob!”

Bob
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!”

Anonymity
Anonymity serves different interests for different user groups.

- **Governments**: “It's traffic-analysis resistance!”
- **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
Union member

Hostile Bob
Incompetent Bob
Indifferent Bob

“I sell the logs.”
“Oops, I lost the logs.”
The AOL fiasco
“Hey, they aren't my secrets.”

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

(the network can track too)
Law enforcement needs anonymity to get the job done.

- Investigated suspect
- Sting target
- Organized Crime
- Anonymous tips

"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?"
Businesses need to protect trade secrets ... and their customers

“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?”
Governments need anonymity for their security

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

“What about insiders?”

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

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

“What does FBI Google for?”

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

“What about insiders?”

“Do I want all my partners to know extent/pattern of my comms with other partners?”
Governments need anonymity for their security

“How can I securely and quickly exchange vital info with every sheriff's dept and Hazmat transporter without bringing them into my secure network?”

“How do I want every SIPRNET node to know where all the traffic on it is headed?”

“Can I hide where my MLS chat server/my automated regrader is?”

“Can my servers resist DDoS and physical attack even by authorized users?”
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?”

“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 $\rightarrow$ Alice's small anonymity net $\rightarrow$ Municipal anonymity net $\rightarrow$ Investigated suspect

Officer Alice $\rightarrow$ Municipal anonymity net

AliceCorp $\rightarrow$ AliceCorp anonymity net $\rightarrow$ Competitor

“Looks like a cop.”

“One of the 25 users on AliceNet.”

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

Citizen Alice → Shared anonymity net → Investigated suspect → Competitor

Officer Alice → Shared anonymity net → "???"

AliceCorp → Shared anonymity net → "???"
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)
One relay 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
Snooping on Exit Relays

• Lots of press in 2007 about people watching traffic coming out of Tor.
• If you want end-to-end encryption (like https), then you need to get it separately.
• Tor hides your location; it doesn't magically encrypt all traffic on the Internet.
• Though Tor does protect from your local network.
Javascript, cookies, history, etc

• Javascript refresh attack
• Cookies, History, browser window size, user-agent, language, http auth, ...
• Mike Perry's Torbutton extension for Firefox fixes many of these, but not all
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, Polipo, e.g. for USB stick
- Vidalia bundle: Windows/OSX installer
- Tor VM: Transparent proxy for Windows
- “Net installer” via our secure updater
- Incognito Linux LiveCD
Usability for relay operators is key.

• Rate limiting: shouldn't eat too much bandwidth
• Exit policies: not everyone is willing to emit arbitrary traffic.

```
allow 18.0.0.0/8:*  
allow *:22        
allow *:80        
reject *:*        
```
Run as a client only

- Relay traffic for the Tor network
- Help censored users reach the Tor network

**Basic Settings**

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.
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.
Governments and other firewalls can just block the whole Tor network.
Number of bridge users compared to June 1

June 1  | June 8  | June 15 | June 22 | June 29, 2009

https://torproject.org
Problem: Abusive users get the whole network blocked.

Minimize scope of blocking?
Some abuses we've seen

- Ransom note via Hotmail
- Spam via Google Groups
- IRC jerks → DDoS on Tor relay
- Somebody downloads a Vin Diesel movie
- Wikipedia, Slashdot block posts
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.
Community

• Many tools make a big splash in the press
  – Censors need to feel in control; publicity removes the appearance of control
• Increase community diversity
  – Strong social network
• Funding
  – Donations, grants, contracts
3-Year Development Roadmap

- Improve Performance
- Client Safety
- Ease of Use and Understanding
- Core Research & Development

https://torproject.org/press/ for details
Lessons?

● 1) Bad people don't need Tor. They're doing fine.
● 2) Honest people need more security/privacy/anonymity.
● 3) Law enforcement can benefit from it too.
● 4) Tor is not unbreakable.
Suggestions: Run a Tor node

- General Caveat: All advice is that of a theory guy with a PhD in Philosophical Logic
  That said...

- Run a Tor node (preferably on a firewall)
  - enclave communications to/from Tor protected
  - CAVEAT: An adversary that watches everything on your internet connection and the other end will see who communicates with that Tor node
Suggestion: Know your network

- Most exit nodes run by people who want to defend: democracy, privacy, consumers, crime victims, dissidents, bloggers, etc.
  - most do this on principle: at varying risk to themselves and their property
  - please be aware of impact on volunteer operators of watching/interacting with bad guys over Tor network
  - please be aware of Tor (and open relays and botnets) if only identifier you have to investigate is a network address
  - Talk to me or Tor Project whenever you can
Suggestions: Know your adversary

- Destination adversary: lock down applications, etc. https://www.torproject.org/download.html/#Warning
- Exit node adversary: same advice, also worry about pseudonymous profiles.
  - DON'T assume passwords over otherwise unencrypted links are safe because they went through Tor first.
- Local/temporary adversary: you are probably OK just using (properly configured) Tor
  - CAVEAT: You might have other adversaries watching you even if they are not your immediate concern
Suggestions: Know your adversary

- Well-funded tech-savvy adversary: Be patient, onion routing is not there yet.
  - Using Tor is usually better than not using Tor or using anything else I know of.
  - Nothing to prevent someone from running a nontrivial percentage of Tor nodes and watching the traffic over them and/or watching internet connections.
  - Currently working on research to work trust into the model and design of Tor.