Tor: a quick overview

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

• Online anonymity 1) software, 2) network, 3) protocol
• Open source, freely available
• Community of researchers, developers, users, and relay operators
• Funding from US DoD, Electronic Frontier Foundation, Voice of America, Google, NLnet, Human Rights Watch, ...
The Tor Project, Inc.

• 501(c)(3) non-profit organization dedicated to the research and development of tools for online anonymity and privacy
Estimated 400,000 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!”

Private citizens
Anonymity serves different interests for different user groups.

“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

Private citizens

Blocked users

Businesses

“It's traffic-analysis resistance!”

“It's privacy!”

“Anonymity”

“It's reachability!”

“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

Hostile Bob

Incompetent Bob

Indifferent Bob

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

“I sell the logs.”

“Oops, I lost the logs.”

The AOL fiasco

“Hey, they aren't my secrets.”

(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

Sting target

Organized Crime

Witness/informer Alice

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?”
Governments need anonymity for their security

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

“What about insiders?”

“What does FBI Google for?”

“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!”

Agent Alice
- Untrusted ISP
- Compromised service
- Shared network
- Defense in Depth

Coalition member Alice
Journalists and activists need Tor for their personal safety

“Did you just post to that website?”

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

“What does the Global Voices website say today?”
“I run livejournal and track my users”
“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...

“Looks like a cop.”

“One of the 25 users on AliceNet.”

“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.

Alice1

E(Bob3, “X”)

Evil Relay

E(Bob1, “Y”)

E(Bob2, “Z”)

Bob1

Bob2

Bob3

Alice2

Alice3
... 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?
The basic Tor design uses a simple centralized directory protocol.

- **S1, S2, S3**: Servers publish self-signed descriptors.
- **Trusted directory**: Alice downloads consensus and descriptors from anywhere.
- **Authorities**: Publish a consensus list of all descriptors.
Choose how to install it

- Tor Browser Bundle: standalone Windows exe with Tor, Vidalia, Firefox, Torbutton, Polipo, e.g. for USB stick
- Vidalia bundle: an installer for Windows or OS X
- 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 *::*
```
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.
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.
Download times for 50 KiB files

median = 7.7 s
Six performance problems

- Tor's congestion/flow control is not good
- Some users bulk-transfer over Tor
- Not enough capacity (run a relay!)
- Load balancing isn't right
- Not just high latency, but high variability
- High directory downloading overhead
How to scale the network?

- The clients need to learn info about the relays they can use. Eventually this means partial network knowledge, and non-clique topology.
- Everybody-a-relay, and the anonymity questions that come with that.
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?
New or returning Tor clients per day

- China
- Iran

https://torproject.org
I CAN HAZ FREEDOM?

TorProject.org
Publicity attracts attention

- Many circumvention tools launch with huge media splashes. (The media loves this.)
- But publicity attracts attention of the censors.
- We threaten their appearance of control, so they must respond.
- We can control the pace of the arms race.