Online Anonymity

Andrew Lewman
The Tor Project
andrew@torproject.org
Outline

- Why anonymity?
- Crash course on Tor
- Future
Informally: anonymity means you can't tell who did what

“Who wrote this blog post?”

“Who's been viewing my webpages?”

“Who's been emailing patent attorneys?”
Formally: anonymity means indistinguishability within an “anonymity set”

Attacker can't tell which Alice is talking to Bob!
Anonymity isn't cryptography: Cryptography just protects contents.

Alice

“Hi, Bob!”

<gibberish>

attacker

“Hi, Bob!”

Bob
Anonymity isn't steganography: Attacker can tell that Alice is talking; just not to whom.

(Strong high-bandwidth steganography may not exist.)
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?”
...since “weak” anonymity isn't.

“You can't prove it was me!”

Proof is a very strong word. With statistics, suspicion becomes certainty.

Will others parties have the ability and incentives to keep their promises?

Promise you won't look!”

Promise you won't remember!”

Promise you won't tell!”

“I didn't write my name on it!”

Not what we're talking about.

“I didn't write my name on it!”

Nope!

(More info later.)

“Isn't the Internet already anonymous?”
Anonymity serves different interests for different user groups.

Anonymity

"It's privacy!"

Private citizens
Regular citizens don't want to be watched and tracked.

Hostile Bob

"I sell the logs."

Incompetent Bob

"Oops, I lost the logs."

Indifferent Bob

"Hey, they aren't my secrets."

(the network can track too)

Name, address, age, friends, interests (medical, financial, etc), unpopular opinions, illegal opinions....
Anonymity serves different interests for different user groups.

“Anonymity”

Private citizens

“‘It’s privacy!’”

Businesses

“It’s network security!”
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?”
Anonymity serves different interests for different user groups.

“It's traffic-analysis resistance!”

“It's network security!”

“It's privacy!”

Governments

Anonymity

Businesses

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

“What does the CIA Google for?”

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

“What about insiders?”
Anonymity serves different interests for different user groups.

- **Governments**: "It's traffic-analysis resistance!"
- **Private citizens**: "It's privacy!"
- **Blocked users**: "It's traffic-analysis resistance!"
- **Businesses**: "It's reachability!"

"It's network security!"
You can't get anonymity on your own: private solutions are ineffective...

"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

“???”

“???”

“???”
Current situation: Bad people on the Internet are doing fine

- Trojans
- Viruses
- Exploits
- Phishing
- Spam
- Botnets
- Zombies
- Espionage
- DDoS
- Extortion
- Phishing
IP addresses can be enough to bootstrap knowledge of identity.

Alice
18.244.x.x

- Hotlinked ad
- Amazon account
- Wikipedia post
Tor is not the first or only design for anonymity.

**Low-latency**

- Single-hop proxies
- V1 Onion Routing (~96)
- Java Anon Proxy (~00-)
- Crowds (~96)
- ZKS “Freedom” (~99-01)
- Tor (01-)

**High-latency**

- Chaum's Mixes (1981)
- anon.penent.fi (~91)
- Remailer networks:
  - cypherpunk (~93),
  - mixmaster (~95),
  - mixminion (~02)

...and more!
Low-latency systems are vulnerable to end-to-end correlation attacks.

**Low-latency:**
- Alice1 sends: \( xx \quad x \quad xxxx \)  
  - Bob2 gets: \( xx \quad x \quad xxxx \quad x \)  
- Alice2 sends: \( x \quad x \quad xx \quad x \quad x \)  
  - Bob1 gets: \( x \quad x \quad xx \quad x \quad x \)  
  - Bob2 gets: \( xx \quad xxxx \)  

**High-latency:**
- Alice1 sends: \( xx \quad x \quad xxxx \)  
- Alice2 sends: \( x \quad x \quad xx \quad x \quad x \)  
- Bob1 gets: \( xx \quad xxxx \)  
- Bob2 gets: \( x \quad xxxx \)  

These attacks work in practice. The obvious defenses are expensive (like high-latency), useless, or both.
Still, we focus on low-latency, because it's more useful.

*Interactive apps*: web, IM, VOIP, ssh, X11, ...

# users: millions?

*Apps that accept multi-hour delays and high bandwidth overhead*: email, sometimes.

# users: tens of thousands at most?

And if anonymity loves company....?
Outline

- Why anonymity?
- *Crash course on Tor*
- Future
What is Tor?

- online anonymity software and network
- open source, freely available
- active research environment
The Tor Project, Inc.

- 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
The simplest designs use a single relay to hide connections.

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

Eavesdropping the relay works too.
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
Tor anonymizes TCP streams only: it needs other applications to clean high-level protocols.
We added a control protocol for external GUI applications.

(Change configuration, report errors, manage circuits, etc.)
Usability for server operators is key.

- Rate limiting: eating too much bandwidth is rude!
- 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.
Server discovery must not permit liars to impersonate the whole network.

1. Alice says, “Describe the network.”

2. Alice is now in trouble.
Server discovery is hard because misinformed clients lose anonymity.
Early Tor versions used a trivial centralized directory protocol.

Servers publish self-signed descriptors.

Authorities publish signed lists of all descriptors.

Alice downloads any signed list.
We redesigned our directory protocol to reduce trust bottlenecks.

Servers publish self-signed descriptors.

Evil Trusted directory

Alice

Alice downloads all statements; believes the majority; downloads descriptors as needed.

(Also uses less bandwidth!)

Authorities publish signed statements about descriptors.
Location Hidden Services

- Developed by US NRL and Finnish Defense
- Hides location and routing information of both the server and client
- DHT Directory design
- Tor software required to host a hidden service
MoD 'how to stop leaks' document is leaked

October 4, 2009

By Tom Chivers (Telegraph)[1]

The Defence Manual of Security is intended to help MoD, armed forces and intelligence, foreign spies and others.
We're currently the largest strong anonymity network ever deployed.

> 1800 running

> 500,000 in a day

> 350 MB/sec
Problem: Abusive users get the whole network blocked.

Minimize scope of blocking?
Other common abuses

- Somebody connects to Hotmail, and sends an obnoxious mail.
- Somebody connects to IRC and yells -> DDoS on Tor exit server.
- Somebody tries to get you shut down by connecting to Google Groups and posting spam.
- Somebody uses Tor to download a movie, and your ISP gets a DMCA takedown.
Who uses Tor?

- Normal people
- Law Enforcement
- Human Rights Activists
- Business Execs
- Militaries
- Abuse Victims

https://torproject.org/torusers
• Tor doesn't magically encrypt the Internet
• Operating Systems and Applications leak your info
• Browser Plugins, Cookies, Extensions, Shockwave/Flash, Java, Quicktime, and PDF all conspire against you
Outline

- Why anonymity?
- Crash course on Tor
- *Future*
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
Copyrights

• who uses tor?
  http://www.flickr.com/photos/mattw/2336507468/sizes/l/
  , Matt Westervelt, CC-BY-SA

• danger!,
  http://flickr.com/photos/hmvh/58185411/sizes/o/
  , hmvh, CC-BY-SA

• 300k,
  http://flickr.com/photos/tochis/1169807846/sizes/o/
  , tochis, CC-BY-NC