Anonymous Communication with emphasis on Tor*
*Tor's Onion Routing

Paul Syverson
U.S. Naval Research Laboratory
Dining Cryptographers (DC Nets)

- Invented by Chaum, 1988
- Strong provable properties
- Versions without collision or abuse problems have high communication and computation overhead
- Don't scale very well
Mixes
Randomly permutes and decrypts inputs
Ciphertext = \( E_{PK_1}[E_{PK_2}[E_{PK_3}[message]]] \)
Mixes

• Invented by Chaum 1981 (not counting ancient Athens)
• As long as one mix is honest, network hides anonymity up to capacity of the mix
• Sort of
  – Flooding
  – Trickling
• Many variants
  – Timed
  – Pool
  – ...
Anonymous communications

1. What is it?

2. Why does it matter?

3. How do we build it?
1. What is anonymity anyway?
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!
Formally: anonymity means indistinguishability within an “anonymity set”
Formally: anonymity means indistinguishability within an “anonymity set”

- Can't distinguish?
  - Basic anonymity set size
  - Probability distribution within anonymity set
  - ....

Attacker can't distinguish which Alice is talking to Bob
We have to make some assumptions about what the attacker can do.

- Alice
- Anonymity network
  - Control part of the network!
- Bob
  - watch (or be!) Bob!

watch Alice!
Anonymity isn't confidentiality: Encryption 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.
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.

“Promise you won't look!”

“Promise you won't remember!”

“Promise you won't tell!”

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

“I didn't write my name on it!”

Not what we're talking about.

Nope!

(More info later.)

“Isn't the Internet already anonymous?”
2. Why does anonymity matter?
Anonymity serves different interests for different user groups.

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

- **Businesses**
  - “It's network security!”
  - “It's censorship circumvention!”

- **Private citizens**

- **Human rights advocates**

"It's censorship circumvention!"
Regular citizens don't want to be watched and tracked.

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

Hostile Bob

“I sell the logs.”

Incompetent Bob

“Oh, I lost the logs.”

Indifferent Bob

“Hey, they aren't my secrets.”

(the network can track too)
Many people don't get to see the internet that you can see...
and they can't speak on the internet either...

Iran Cracks Down on Bloggers

Associated Press 16:13 PM Mar, 28, 2006

DUBAI, United Arab Emirates -- On his last visit to Iran, Canadian-based blogger Hossein Derakhshan was detained and interrogated, then forced to sign a letter of apology for his blog writings before being allowed to leave the country. Compared to others, Derakhshan is lucky.

Dozens of Iranian bloggers have faced harassment by the government, been arrested for voicing opposing views, and fled the country in fear of prosecution over the past few years.
It's not only about dissidents in faraway lands.
Regular citizens don't want to be watched and tracked.

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

Crime Target
Alice

Human Rights Worker
Alice

Oppressed
Alice

Stalker Bob

Censor/Blocker Bob

“I look for you to do you harm.”

“I control your worldview and who you talk to.”

“I imprison you for seeing/saying the wrong things.”
Law enforcement needs anonymity to get the job done.

"Why is alice.fbi.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?”

“We attack Alice's customers with malware, and watch for when she notices us.”
Governments need anonymity for their security

“Agent Alice”

- **Untrusted ISP**
  - “What will you bid for a list of Baghdad IP addresses that get email from .gov?”
  - “What bid for the hotel room from which someone just logged in to foo.navy.mil?”

- **Compromised service**
  - “What does the CIA Google for?”
Governments need anonymity for their security

Coalition member Alice

- Shared network
- Hostile network
- Semitrusted network

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

“Do I want all my partners to know extent/pattern of my comms with other partners?”

“How can I establish communication with locals without a trusted network?”

“How can I avoid selective blocking of my communications?”
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?”

“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?”
You can't be anonymous by yourself: 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/malware host

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

- Citizen Alice
- Officer Alice
- AliceCorp

Shared anonymity net

- Investigated suspect
- Competitor

“???”
Don't bad people use anonymity?
Current situation:
Bad people on internet are doing fine

- Trojans
- Viruses
- Exploits
- Botnets
- Zombies
- Espionage
- DDoS
- Extortion
- Spam
- Phishing
Giving good people a fighting chance

- DDoS resistant servers
- Enable sharing threat info
- Freedom of access

Anonymity Network

- Encourage informants
- Protect free speech

- Protect operations and analysts/operatives

- Resist Identity Theft
- Reduce cyberstalking of kids
3. How does anonymity work?
Anonymity Systems for the Internet

Low-latency

- Single-hop proxies (~95-)
- NRL V0 Onion Routing (~96-97)
- NRL V1 Onion Routing (~97-00)
- Java Anon Proxy (~00-)
- ZKS “Freedom” (~99-01)
- Crowds (~96)
- Tor (01-)

High-latency

- Chaum's Mixes (1981)
- anon.penet.fi (~91-96)
- 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: \[ xx \ x \ xxxx \ x \]
Bob2 gets: \[ xx \ x \ xxxx \ x \]
Alice2 sends: \[ x \ x \ xx \ x \ x \]
Bob1 gets: \[ x \ x \ xx \ x \ x \]

High-latency: Alice1 sends: \[ xx \ x \ xxxx \]
Alice2 sends: \[ x \ x \ xx \ x \ x \]
Bob1 gets: \[ xx \ xxxx \ ..... \]
Bob2 gets: \[ x \ xxxxx \ ..... \]

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:* hundreds at most?

And if anonymity loves company....?
The simplest designs use a single relay to hide connections.
But an attacker who sees Alice can see who she's talking to.
Add encryption to stop attackers who eavesdrop on Alice.

(e.g.: some commercial proxy providers, Anonymizer)
But a single relay is a single point of failure.
But a single relay is 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 someone is talking to Bob, but not who it is.
Alice makes a session key with R1
Alice makes a session key with R1
...And then tunnels to R2
Alice makes a session key with R1
...And then tunnels to R2...and to R3
Alice makes a session key with R1
...And then tunnels to R2...and to R3
Then talks to Bob over circuit
Feasible because onion routing uses (expensive) public-key crypto just to build circuits, then uses (cheaper) symmetric-key crypto to pass data.
Can multiplex many connections through the encrypted circuit
That's Tor* in a nutshell

* Tor's Onion Routing
Focus of Tor is anonymity of the communications pipe, not the application data that passes through it.
Tor anonymizes TCP streams only: it needs other applications to clean high-level protocols.
Tor: The Big Picture

- Freely available (Open Source), unencumbered, and
- Comes with a spec and full documentation:
  - Docs and instructions translated into 15+ languages
  - German univ. implemented compatible Java Tor clients
  - Researchers use it to study anonymity
- Several commercial imitators
- Focus on Usability/Scalability/Incentives
- 200000+ active users, including various govt. and law enforcement users
- PC World magazine: Tor in the Top 100 Products of 2005.
- Began as NRL research project 2001 (1995)
- Tor Project now a US 501(c) 3 with a handful of employees and many volunteers
New or returning Tor clients per day

- China
- Iran

https://torproject.org
Usability for relay operators

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

![Network Configuration]

- Middle-man node: no exit from Tor network (reject *:*).
- Bridge node: not part of public Tor network at all.
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
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.
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.
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: 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.
Location Hidden Servers

- Alice can connect to Bob's server without knowing where it is or possibly who he is
- Already told you why this is desirable, but...
- How is this possible?
1. Server Bob creates onion routes to Introduction Points (IP)

(All routes in these pictures are onion routed through Tor)
Location Hidden Servers

1. Server Bob creates onion routes to Introduction Points (IP)
2. Bob publishes his xyz.onion address and puts Service Descriptor incl. Intro Pt. listed under xyz.onion
2'. Alice uses xyz.onion to get Service Descriptor (including Intro Pt. address) at **Lookup Server**
Location Hidden Servers

3. Client Alice creates onion route to **Rendezvous Point (RP)**
3. Client Alice creates onion route to Rendezvous Point (RP)

4. Alice sends RP address and any authorization through IP to Bob
5. If Bob chooses to talk to Alice, connects to **Rendezvous Point**

6. **Rendezvous Point** mates the circuits from Alice and Bob
Location Hidden Servers

Final resulting communication channel

Rendezvous Point

Alice's Client

Bob's Server

Location Hidden Servers
Further Questions?

- Contact me:  
  http://www.syverson.org
- Onion Routing homepage:  
  http://www.onion-router.net
- Download/read about Tor:  
  https://www.torproject.org
- Major papers on anonymity:  
  http://freehaven.net/anonbib