Anonymous Communications

Number of users ≈ 0

Steven J. Murdoch
University College London
Who needs anonymity?

- Military personnel
- Law enforcement
- Bloggers
- Activists and whistle-blowers
- Ordinary people

Encryption doesn't work!
BBC Horizon
Encryption doesn’t work

TLS, PGP, S/MIME only hide what is being said

- Alice uploaded a gigabyte to CNN 6 hours before footage of human rights abuses were aired
- Bob, who just joined our criminal organization sent an encrypted email to the FBI a week before our boss got arrested
- Charlie keeps browsing our website of illegal material, maybe we should give him fake data?
## Remailers

<table>
<thead>
<tr>
<th>Description</th>
<th>System</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>penet.fi (1993–1996)</td>
<td>Type-1 (Cypherpunk)</td>
<td>Mix decrypts messages, Uses PGP</td>
</tr>
<tr>
<td>Simply stripped headers off emails sent via retranslator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allowed replies to be sent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Easy to use, but single point of compromise</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shut down following compromise by CoS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Mixmaster (1998–) | | Layered encryption, 
| | | Batching and re-ordering |
| Based on Chaum Mix (1981) | | |
| Mixminion (2002–) | | Fixed many problems, 
| | | Introduced replies |
penet.fi (1993-1996)

- Simply stripped headers off emails sent via remailer
- Allowed replies to be sent
- Easy to use, but single point of compromise
- Shut down following compromise by CoS
Type-1 (Cypherpunk)

- Mix decrypts messages
- Uses PGP
Mixmaster (1998–)

- Layered encryption
- Batching and re-ordering
- Based on Chaum Mix (1981)

Mixminion (2002–)
Mixmaster (1998–)

- Layered encryption
- Batching and re-ordering
- Based on Chaum Mix (1981)
Mixminion (2002–)

- Fixed many problems
- Introduced replies
**Remailers**

**penet.fi (1993-1996)**
- Simply stripped headers off emails sent via remailer
- Allowed replies to be sent
- Easy to use, but single point of compromise
- Shut down following compromise by CoS

**Type-1 (Cypherpunk)**
- Mix decrypts messages
- Uses PGP

**Mixmaster (1998-)**
- Layered encryption
- Batching and re-ordering
- Based on Chaum Mix (1981)

**Mixminion (2002-)**
- Fixed many problems
- Introduced replies

**Number of users \( \approx 0 \)**
- Simply stripped headers off emails sent via remailer
- Allowed replies to be sent
- Easy to use, but single point of compromise
- Shut down following compromise by CoS

- Layered encryption
- Batching and re-ordering
- Based on Chaum Mix (1981)

Mixminion (2002–)
- Fixed many problems
- Introduced replies

Number of users ≈ 0
The Web

Web browsing is hard to secure

- Requires low latency
- High variability
- Low tolerance to padding

Equivalent systems

Open proxies ≈ penet.fi
VPN ≈ Type-0
MixMinion ≈ Tor
The Web

Web browsing is hard to secure

- Requires low latency
- High variability
- Low tolerance to padding

Equivalent systems
Equivalent systems

Open proxies ≈ penet.fi
VPN ≈ Type-0
MixMinion ≈ Tor
The Web

Web browsing is hard to secure

- Requires low latency
- High variability
- Low tolerance to padding

Equivalent systems

Open proxies ≈ penet.fi
VPN ≈ Type-0
MixMinion ≈ Tor
Censorship resistance

Open problems for bridges

- Protocol obfuscation
- Scanning resistance
- Distribution mechanisms

Domain fronting: run proxy as cloud service, connect to cloud via HTTPS (e.g. Google.com)
Recurring, directly connecting Chinese Tor users (past 180 days)
Get Bridges!

BridgeDB can provide bridges with several types of Pluggable Transports, which can help obfuscate your connections to the Tor Network, making it more difficult for anyone watching your internet traffic to determine that you are using Tor.

Some bridges with IPv6 addresses are also available, though some Pluggable Transports aren't IPv6 compatible.

Additionally, BridgeDB has plenty of plain-of-vanilla bridges — without any Pluggable Transports — which maybe doesn't sound as cool, but they can still help to circumvent internet censorship in many cases.

Just give me bridges!
Chinese Tor users via bridges (past 180 days)
Open problems for bridges

- Protocol obfuscation
- Scanning resistance
- Distribution mechanisms

Domain fronting: run proxy as cloud service, connect to cloud via HTTPS (e.g. Google.com)
Abuse

Unreal Tournament 2004 lends incontroversial proof to John Gabriel's Greater Internet Fuckwad Theory.

Normal Person + Anonymity + Audience = Total Fuckwad

Nymble

Connections before complaint remain anonymous:

\[ t_0, t_2, t_3 \]

Future connections from the same user are linkable, and the user is blocked:

\[ t_4, t_5 \]

To continue searching, please type the characters you see below:

Google Help for more information.

© 2010 Google - Google Home
Unreal Tournament 2004 lends incontestable proof to John Gabriel's Greater Internet Fuckwad Theory.
We're sorry...

... but your computer or network may be sending automated queries. To protect our users, we can't process your request right now.

To continue searching, please type the characters you see below:

See Google Help for more information.
Nymble
Abuse

Unreal Tournament 2004 lends incontrovertible proof to John Gabriel's Greater Internet Fuckwad Theory.

Normal Person + Anonymity + Audience = ? Total Fuckwad

Nymble

Connections before complaint remain anonymous:

- $t_0$
- $t_1$ (crossed out)
- $t_2$
- $t_3$

Future connections from the same user are linkable, and the user is blocked:

- $t_4$
- $t_5$

Server complains about ticket $t_1$ and receives linking token for misbehaving user.

We're sorry...

... but your computer or network may be sending automated queries. To protect our users, we can't process your request right now.

To continue searching, please type the characters you see below: [input field] [Invisible image with characters to be entered]
Incentives

- Many users are unable to pay (tragedy of the commons)
- Giving better performance to users who contribute could reduce anonymity
- If money is changing hands, volunteers may give up
Financial Review

Tor's fiscal 2012 marked another year of financial improvement and stability. The Tor Project has seen steady revenue growth since its inception. Since meeting the revenue milestones of $1,253,241 in 2009, $1,574,119 in 2010 and $1,681,101 in 2011, Tor has reached new heights in 2012 with over $2 million in revenue (unaudited). Fiscal 2012 results also provided a new financial achievement, for the first time since inception: The Tor Project Inc. had no operating income. Tor's revenue growth was driven by diversity in funding sources which include U.S. government federal funding, Knight Foundation, SRI International, Google, the Swedish International Development Cooperative Agency, and private donations, among others.

Fiscal responsibility is important to The Tor Project Inc. In order to maintain financial stability, Tor maintains cash reserves sufficient to maintain operations for a minimum of 90 days. Tor is proud to report that, since 2009, over 80% of its revenue has been directed towards spending on programs.

As plans for 2013 commence, Tor will continue to improve and expand revenues to fund research and development efforts.

Tor's accounts and financial statements of The Tor Project are maintained in accordance with generally accepted principles in the United States. Our audits are performed in accordance with government auditing standards and in accordance with OMB A133 which requires a higher level of assurance with respect to compliance and internal controls. Tor is proud to report that in both fiscal 2010 and 2011, we obtained an unmodified audit opinion and had no compliance or internal control findings.

To view Tor's audited financial reports visit www.torproject.org/about/financials.
stability. The Tor Project reported revenue of $1,681,101 in 2011, achieving revenue (unaudited) for the first
As per the data provided, the expenses for 2011 are as follows:

- **Program Services**: 86%
- **Management and General**: 11%
- **Fundraising**: 4%

The pie chart visually represents these percentages, indicating the distribution of expenses.
Tor’s fiscal 2012 marked another milestone as it has seen steady revenue growth. Fiscal 2012 results are the first time since income has reached milestones of $1,250,000.

Revenue growth is attributed to contributions, which accounted for 18% of total income. U.S. Government based income contributed 60%, followed by foundation and other grants at 18%. Donated services were 4% of total income.
Incentives

• Many users are unable to pay (tragedy of the commons)
• Giving better performance to users who contribute could reduce anonymity
• If money is changing hands, volunteers may give up
Juice Media Rap News
September 2012
THIS IS WHAT A 
SUPPORTER LOOKS LIKE

DAN ELLSBERG AND PATRICIA MARK ELLSBERG, PRIVACY ACTIVISTS

#SUPPORTTOR
Incentives

- Many users are unable to pay (tragedy of the commons)
- Giving better performance to users who contribute could reduce anonymity
- If money is changing hands, volunteers may give up