Anonymous Communications and Tor

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:
- Alice unleashed a google on DNT 6 hours before footage of her human rights abuses were aired
- Bali, who had seen our criminal organization sent an encryption email to the FBI a week before our house got burned
- Charlie keeps bugging our website of illegal material, maybe we should give him their data?
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

- Simply stripped headers off emails sent via reemailer
- 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
penet.fi (1993-1996)

- Simply stripped headers off emails sent via reminer
- 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
messages

A

For D

K_{pub}

Mix

K_{priv}

For C

K_{pub}

B

C

D
Mixmaster (1998–)

- Layered encryption
- Batching and re-ordering
- Based on Chaum Mix (1981)
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 ≈ 0
- Simply stripped headers off emails sent via reemailer
- 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

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 \(\approx\) penet.fi
VPN \(\approx\) Type-0
MixMinion \(\approx\) Tor
Censorship resistance

Open problems

- Protocol obfuscation
- Scanning resistance
- Distribution mechanisms
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

- Protocol obfuscation
- Scanning resistance
- Distribution mechanisms
Unreal Tournament 2004 lends incontestible 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

Connections before complaint remain anonymous

\[ t_0 \rightarrow t_1 \rightarrow t_2 \rightarrow t_3 \]

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

\[ t_4 \rightarrow t_5 \]

Server complains about ticket t1 and receives linking token for misbehaving user
Abuse

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

Normal Person + Anonymity + Audience = Total Fuckward

Google

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:  

subm

See Google Help for more information.

© 2010 Google - Google Home

Nymble

Connections before complaint remain anonymous

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

Server complains about ticket 11 and receives linking token for misbehaving user
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 net 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 Cooperation 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 expand research and development efforts.

The 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.
tability. The Tor Project
gaining the revenue
$1,681,101 in 2011,
ion in revenue (unaud
ievement. for the first
Tor's fiscal 2012 marked another milestone of $1,250,000.

Fiscal 2012 was the first time since income growth has been steady.

The pie chart shows the following income sources for 2011:

- Contributions: 4%
- U.S. Government based income: 60%
- Foundation and Other Grants: 18%
- Donated Services: 18%
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
**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