Anonymity & Censorship-free Communication

Steven J. Murdoch
VASCO & University College London
Who needs anonymity?

- Military personnel
- Law enforcement
- Bloggers
- Activists and whistle-blowers
- Ordinary people
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
- CAST5 & ElGamal

Mixmaster (1998–)
- Layered encryption
- Batching and re-ordering
- Based on Chaum Mix (1981)
- 3DES & RSA (PKCS #1 v1.5)

Mixminion (2002–)
- Fixed many problems
- Introduced replies
- AES, SHA-1, RSA OPEAP
- LIONESS wide-block cipher to resist tagging

There is no one security criterion for anonymity.
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
• CAST5 & ElGamal
messages

A

For D

K_{pub}

Mix

K_{priv}

B

For C

K_{pub}

C

D

Jamal
CAST5 & ElGamal

Mixmaster (1998–)
- Layered encryption
- Batching and re-ordering
- Based on Chaum Mix (1981)
- 3DES & RSA (PKCS #1 v1.5)

Mixminion (2002–)
CAST5 & ElGamal

Mixmaster (1998-)

- Layered encryption
- Batching and re-ordering
- Based on Chaum Mix (1981)
- 3DES & RSA (PKCS #1 v1.5)

Mixminion (2002-...)
• 3DES & RSA (PKCS #1 v1.5)

Mixminion (2002–)

• Fixed many problems
• Introduced replies
• AES, SHA-1, RSA OPEAP
• LIONESS wide-block cipher to resist tagging
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
- CAST5 & ElGamal

Mixmaster (1998–)
- Layered encryption
- Batching and re-ordering
- Based on Chaum Mix (1981)
- 3DES & RSA (PKCS #1 v1.5)

Mixminion (2002–)
- Fixed many problems
- Introduced replies
- AES, SHA-1, RSA OEAP
- LIONESS wide-block cipher to resist tagging
There is no one security criterion for anonymity.
Fixed many problems
Introduced replies
AES, SHA-1, RSA OEAP
LIONESS wide-block cipher to resist tagging

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 (IPSEC) ≈ Type-0
MixMinion ≈ Tor
Web browsing is hard to secure

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

Equivalent systems
Equivalent systems

Open proxies ≈ penet.fi

VPN (IPSEC) ≈ Type-0

MixMinion ≈ Tor
**Link encryption**

- Confidentiality and integrity
- Weak resistance to traffic analysis
- Concealment (not so useful now)
- TLS configured in similar way to web browser and client (RSA-1024 authenticating ECDH-P-256 & AES)
- Server to client authenticated
- (client to server uses custom auth)

**Circuit encryption**

- Cannot explain ciphertext so as to hide path length without padding
- AES CTR, with no MAC (positive)
- Keys negotiated using HFGC algorithm
- One-way authenticated Diffie-Hellman (ephemeral)
- Curve25519 elliptic curves
- Cells contain Circuit ID
Link encryption

- Confidentiality and integrity
- Weak resistance to traffic analysis
- Covertness (not so useful now)
- TLS configured in similar way to web browser and client (RSA-1024 authenticating ECDH P-256 & AES)
- Server to client authenticated
- (client to server uses custom auth)
Link encryption
- Confidentiality and integrity
- Weak resistance to traffic analysis
- Coveness (not so useful now)
- TLS configured in similar way to web browser and client (RSA-1024 authenticating ECDH P-256 & AES)
- Server to client authenticated
- (client to server uses custom auth)

Circuit encryption
- Cannot explain ciphertext so as to hide path length without padding
- AES CTR, with no MAC (postitive)
- Keys negotiated using kdf algorithm
- One-way authenticated Diffie-Hellman (identity)
- Curve25519 elliptic curves
- Cells contain Circuit ID
Circuit encryption

- Cannot expand ciphertext so as to hide path length without padding
- AES CTR, with no MAC (malleable)
- Keys negotiated using nTor algorithm
  - One-way authenticated Diffie Hellman (approx.)
  - Curve25519 elliptic curves
- Cells contain Circuit ID
Link encryption
- Confidentiality and integrity
- Weak resistance to traffic analysis
- Covertness (not so useful now)
- TLS configured in similar way to web browser and client (RSA-1024 authenticating ECDH P-256 & AES)
- Server to client authenticated
- (client to server uses custom auth)

User

Entry

Middle

Exit

Data

00 02 28 be ...

1d ae cd 59 ...

e4 50 de 5a ...

Circuit encryption
- Cannot explain ciphertext so as to hide path length without encoding
- AES CTR, with no MAC (one-pass)
- Keys negotiated using SNI
- One-way authenticated Diffie Hellman (negotiated)
- Curve25519 elliptic curves
- Cells contain Circuit ID

External access
- E2E MAC
- When connecting to SNI path forward
- Some Layer 7 in the channel
- Payload streaming
E2E encryption

- E2E MAC verified by exit node
- When MAC is verified to end of the path has been reached
- Some bits set to zero to optimise the check
- Payload contains command, Stream ID and data
Directory crypto

- List of nodes and their public keys maintained by 8 directory authorities
- Consensus algorithm to create agreed set and together signed with RSA-2048
- Each node signs descriptor with RSA-1024
- Will be moving to ED25519 to replace RSA-1024 and 2048
Node selection for security and performance

Metrics for Security and Performance in Low-Latency Anonymity Systems, Murdoch and Watson
**Link encryption**
- Confidentiality and integrity
- Weak resistance to traffic analysis
- Concealment (not so useful now)
- TLS configured in similar way to web browser and client (RSA-1024 authenticating ECDH P-256 & AES)
- Server to client authenticated
- (Client to server uses custom auth)

**Circuit encryption**
- Cannot expand ciphertext so as to hide path length without padding
- AES CTR, with re-MAC (post-sig)
- Keys negotiated using SSH algorithm
- One-way authenticated Diffie-Hellman (discret)
- Curve25519 elliptic curves
- Cells contain Circuit ID
The Web

Web browsing is hard to secure

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

Equivalent systems

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

Levels of Filtering: Pervasive | Substantial | Selective | Suspected | No evidence

Fingerprinting and developing blocking rules

[Image showing a map and a screenshot of a user interface with. Diagram on the right showing processes and decision flows related to fingerprinting and blocking rules.]
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)
Fingerprinting and developing blocking rules

Abuse

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

Normal Person + Anonymity + Audience = Total Fuckawd

3.67% of the most popular 1,000 websites block Tor


Nymble

Connections before complaint remain anonymous

$\text{t}_0$ $\times$ $\text{t}_1$ $\text{t}_2$ $\text{t}_3$

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

Server complains about ticket $\text{t}_1$ and receives linking token for misbehaving user
Unreal Tournament 2004 lends incontestable proof to John Gabriel's Greater Internet Fuckwad Theory.
3.67% of the most popular 1,000 websites block Tor


Connections before complaint remain anonymous

$t_0$ $t_1$ $t_2$ $t_3$

$t_4$ $t_5$

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

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

Nymble
Abuse

Unreal Tournament 2004 lends incontestable proof to John Gabriel’s Greater Internet Fuckwad Theory.

Normal Person + Anonymity + Audience = Total Fuckwad

Shitcock

3.67% of the most popular 1,000 websites block Tor


Connections before complaint remain anonymous:

- \( t_0 \)
- \( t_1 \)
- \( t_2 \)
- \( t_3 \)

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.

Nymble
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 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 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.
stability. The Tor Project reported a revenue of $1,681,101 in 2011, achieving revenue (unaudited) for the first time.
2011 Expenses

- Program Services: 86%
- Management and General: 11%
- Fundraising: 4%
Tor's fiscal 2012 marked another milestone in its development, having reached the steady revenue milestone of $1.25 million. Fiscal 2012 represented the first time since inception that Tor has reached this milestone.

### 2011 Income

- **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
THIS IS WHAT A Tor SUPPORTER LOOKS LIKE

DAN ELLSBERG AND PATRICIA MARX ELLSBERG, PRIVACY ACTIVISTS

#SUPPORTTor
Sustainability

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