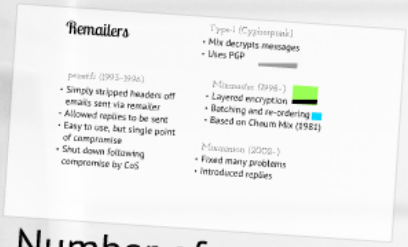
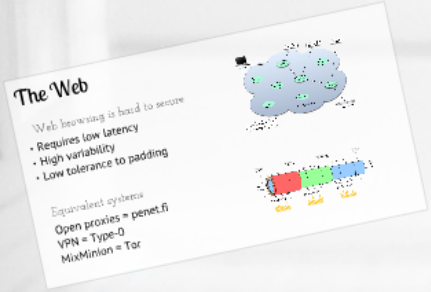
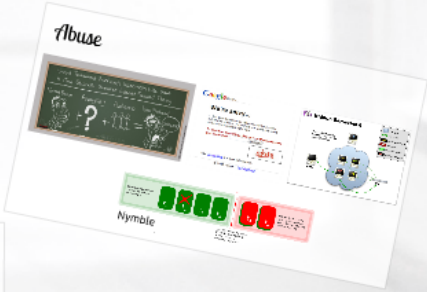
Anonymous Communications and Tor: History and Future Challenges



Number of users ≈ 0





Steven J. Murdoch
University of Cambridge Computer Laboratory

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?

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?

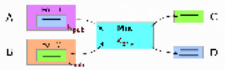
Remailers

penet.fi (1993–1996)

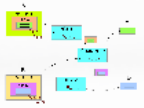
- Simply stripped headers off emails sent via remailer
- Allowed replies to be sent
- Easy to use, but single point of compromise
- Shut down following compromise by CoS

Type-1 (Cypherpunk)

- Mix decrypts messages
- Uses PGP



Mixmaster (1998–)



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

Mixminion (2002–)

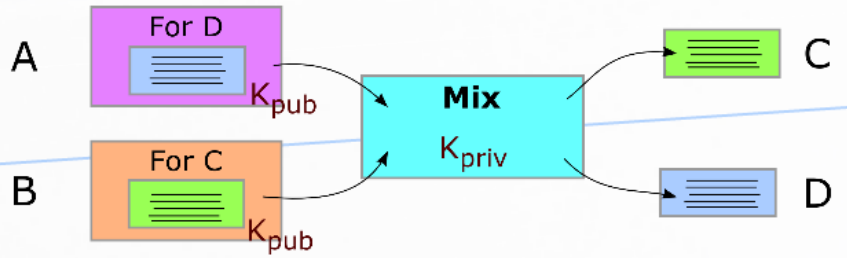
- Fixed many problems
- Introduced replies

penet.fi (1993-1996)

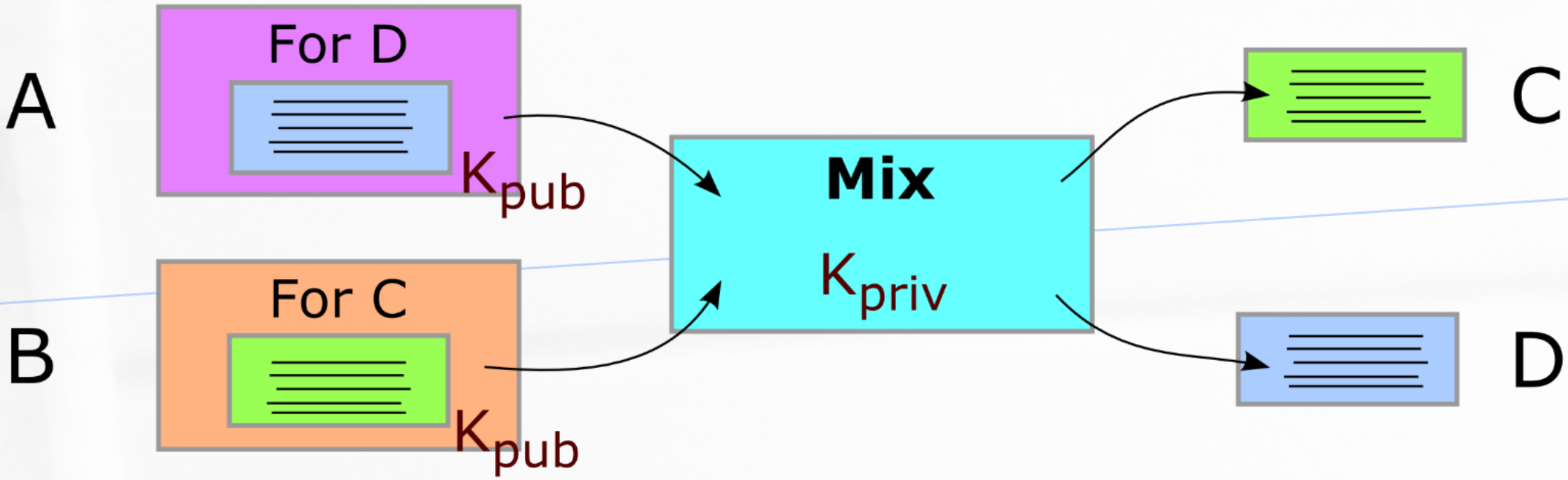
- Simply stripped headers off emails sent via remailer
- Allowed replies to be sent
- Easy to use, but single point of compromise
- Shut down following compromise by CoS

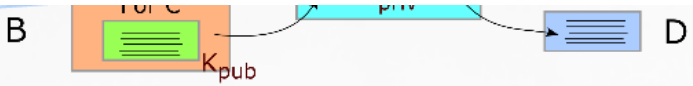
Type-1 (Cypherpunk)

- Mix decrypts messages
- Uses PGP

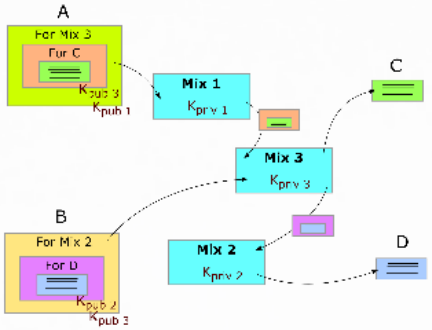


messages



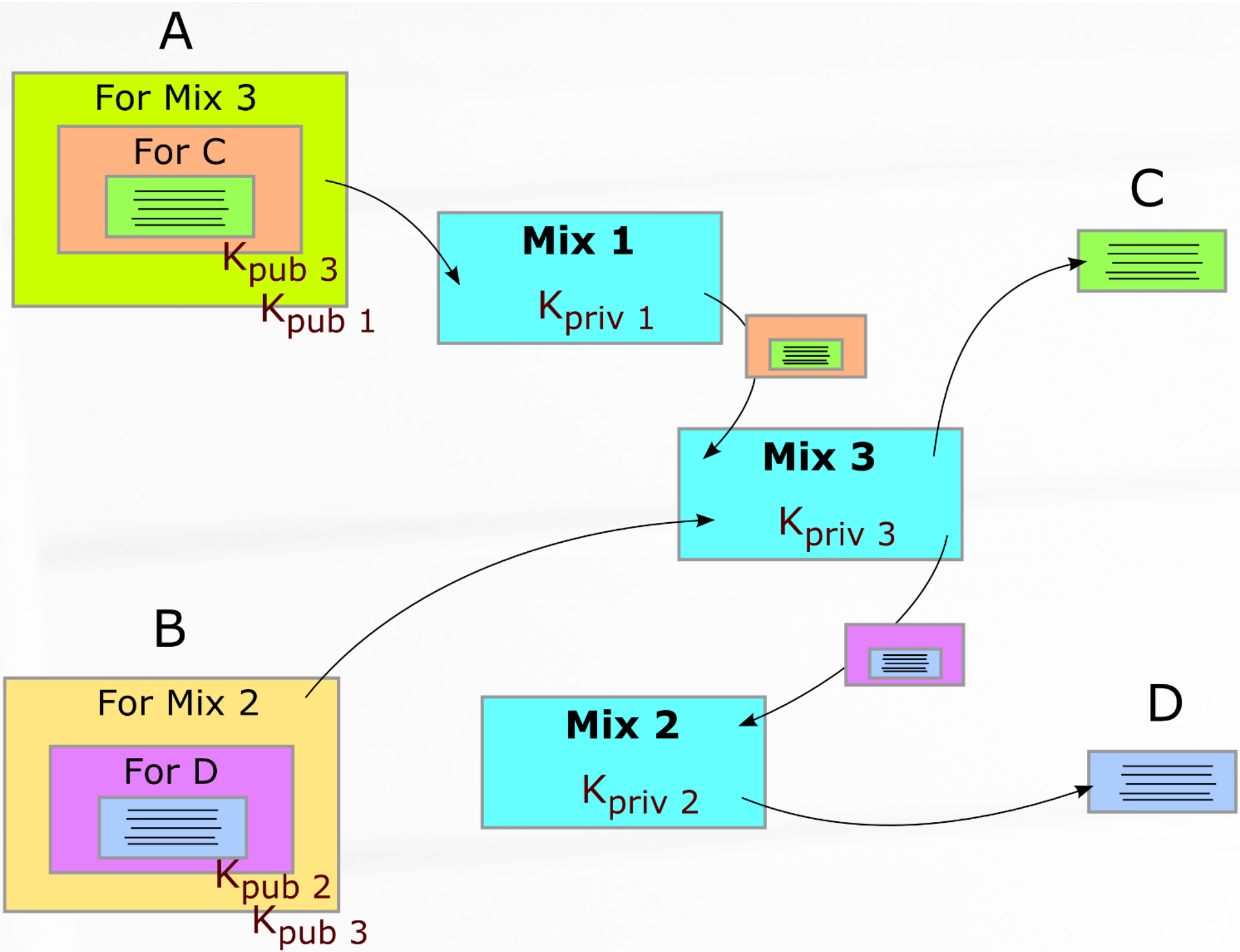


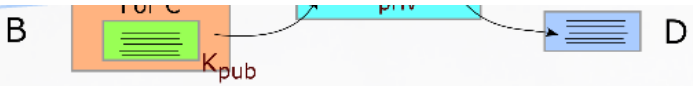
Mixmaster (1998-)



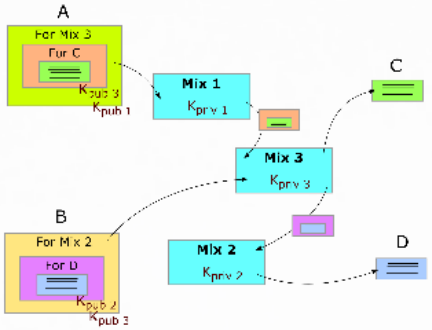
- Layered encryption
- Batching and re-ordering
- Based on Chaum Mix (1981)

Mixminion (2002-)


A
For Mix 3
For C
$K_{pub\ 3}$
$K_{pub\ 1}$
Mix 1
$K_{priv\ 1}$
C
Mix 3
$K_{priv\ 3}$
B
For Mix 2
For D
$K_{pub\ 2}$
$K_{pub\ 3}$
Mix 2
$K_{priv\ 2}$
D



Mixmaster (1998-)



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

Mixminion (2002-)


Senders
Receivers
Mix

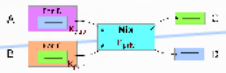
Mixminion (2002-)

- Fixed many problems
- Introduced replies

Remailers

Type-1 (Cypherpunk)

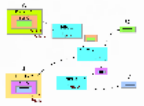
- Mix decrypts messages
- Uses PGP



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

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 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-)

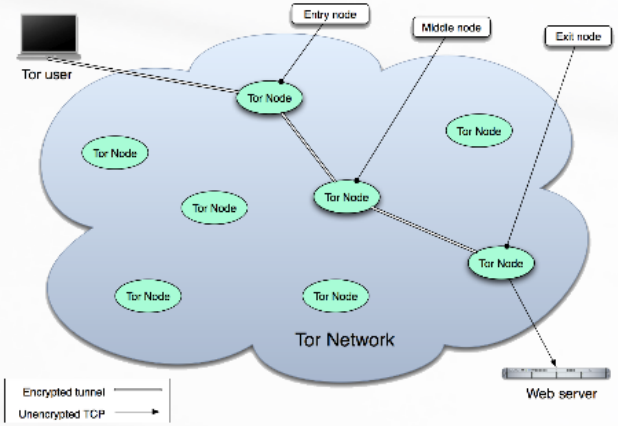
- Fixed many problems
- Introduced replies

Number of users ≈ 0

The Web

Web browsing is hard to secure

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

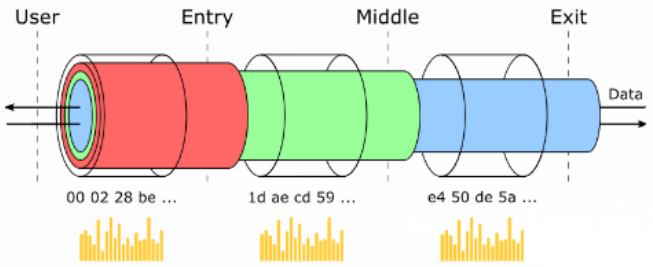


Equivalent systems

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

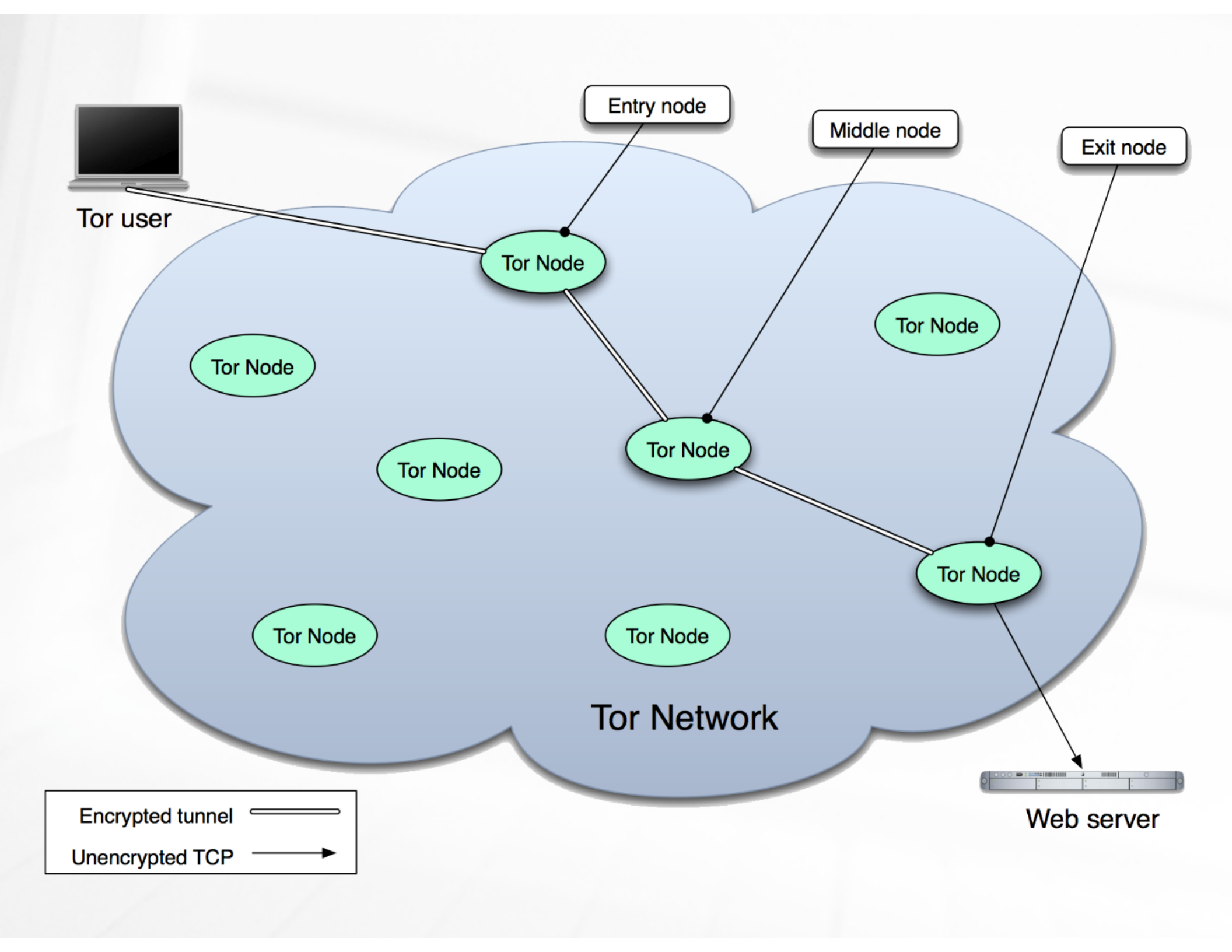
Equivalent systems

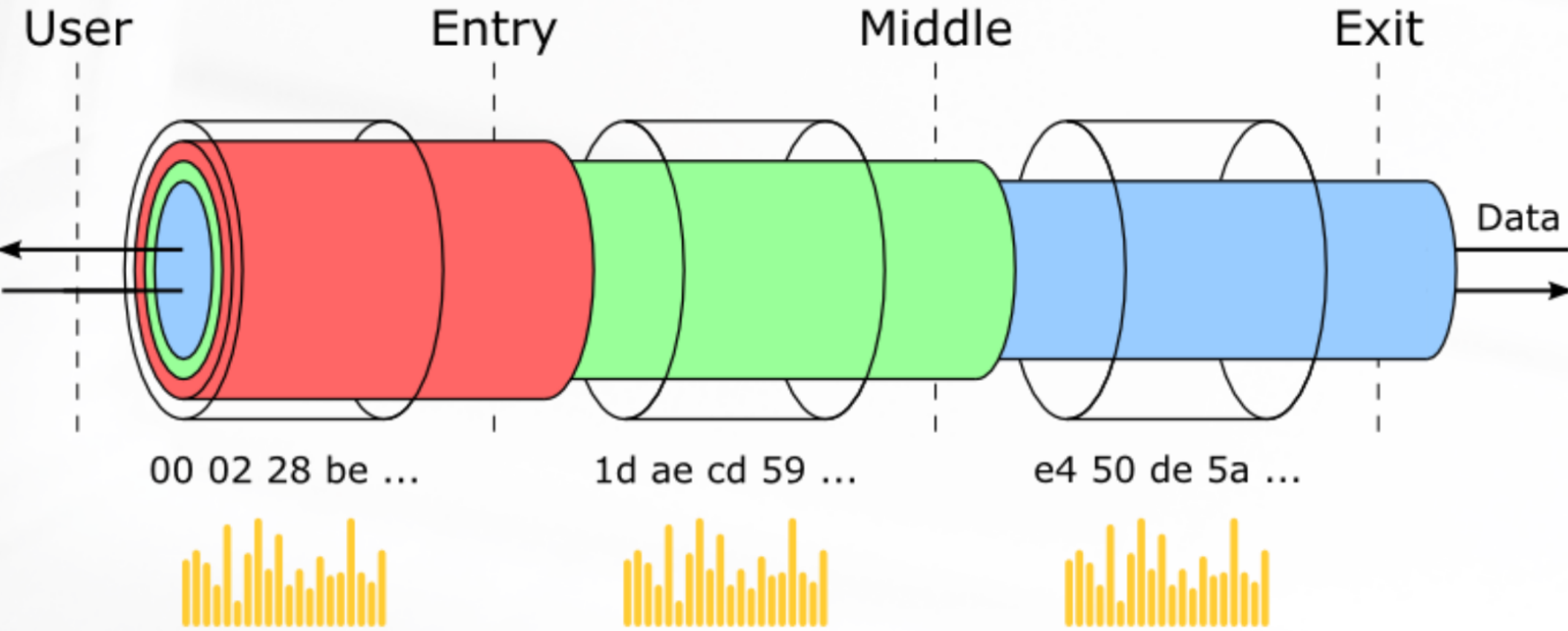
Equivalent systems

Open proxies ≈ penet.fi

VPN ≈ Type-0

MixMinion ≈ Tor

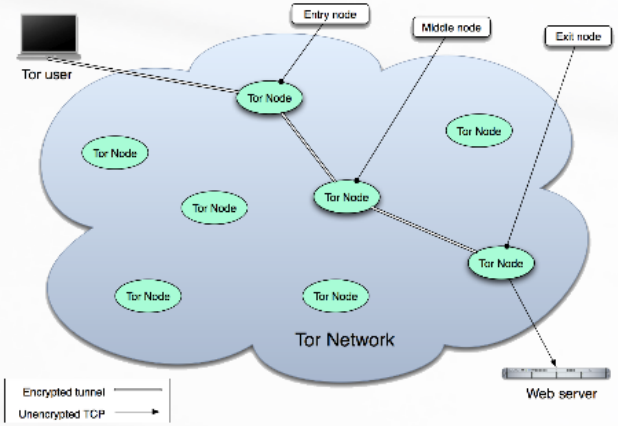

Entry node
Middle node
Exit node
Tor user
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Network
Web server
Encrypted tunnel
Unencrypted TCP


User
Entry
Middle
Exit
Data
00 02 28 be ...
1d ae cd 59 ...
e4 50 de 5a ...

The Web

Web browsing is hard to secure

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

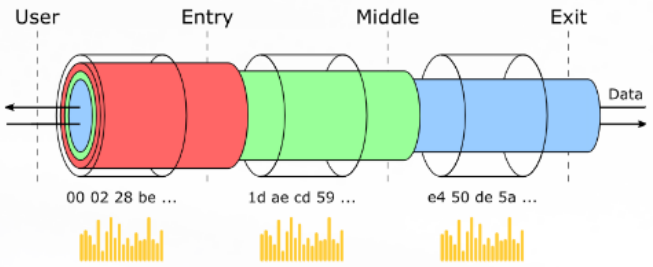


Equivalent systems

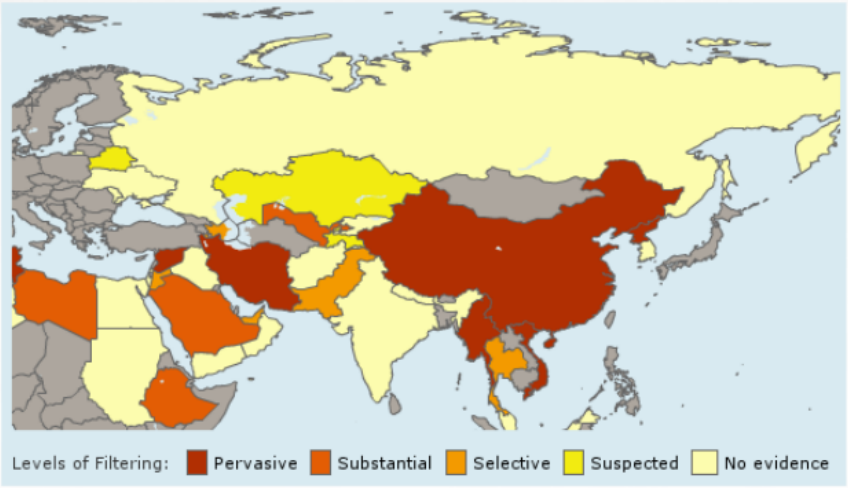
Open proxies ≈ penet.fi

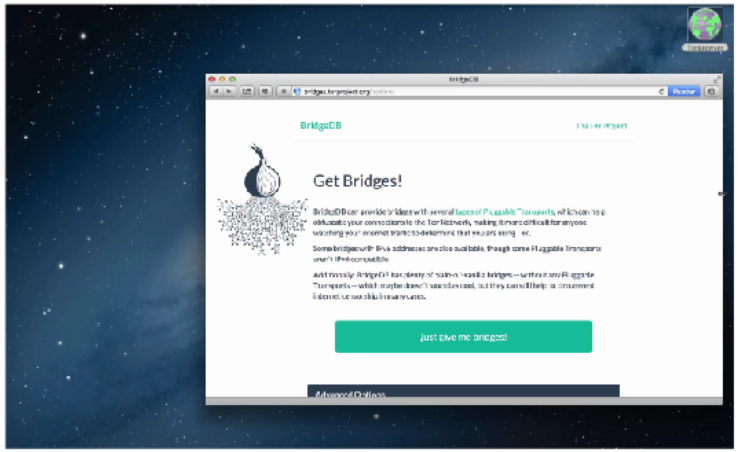
VPN ≈ Type-0

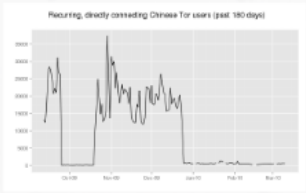
MixMinion ≈ Tor



Censorship resistance

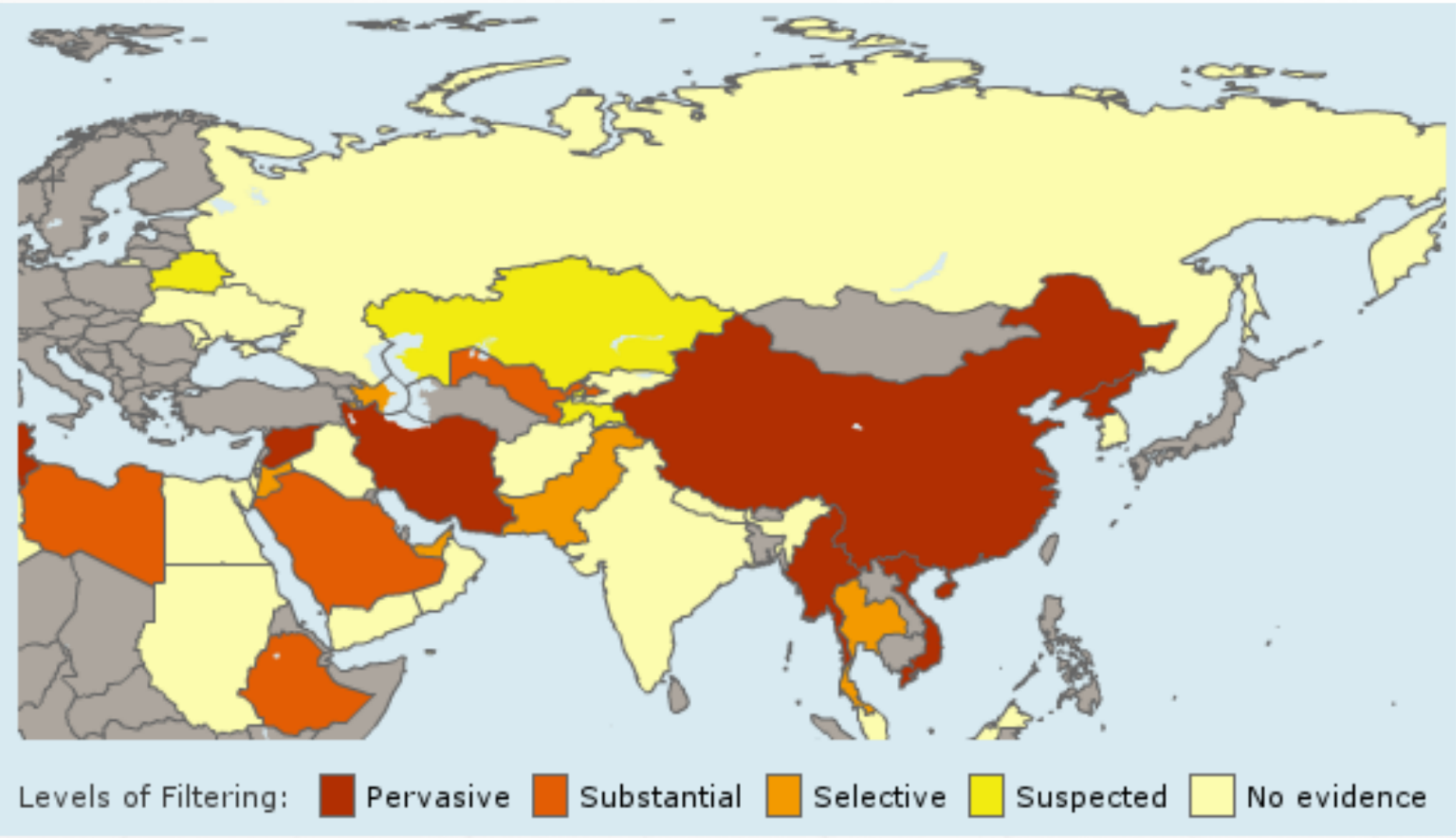






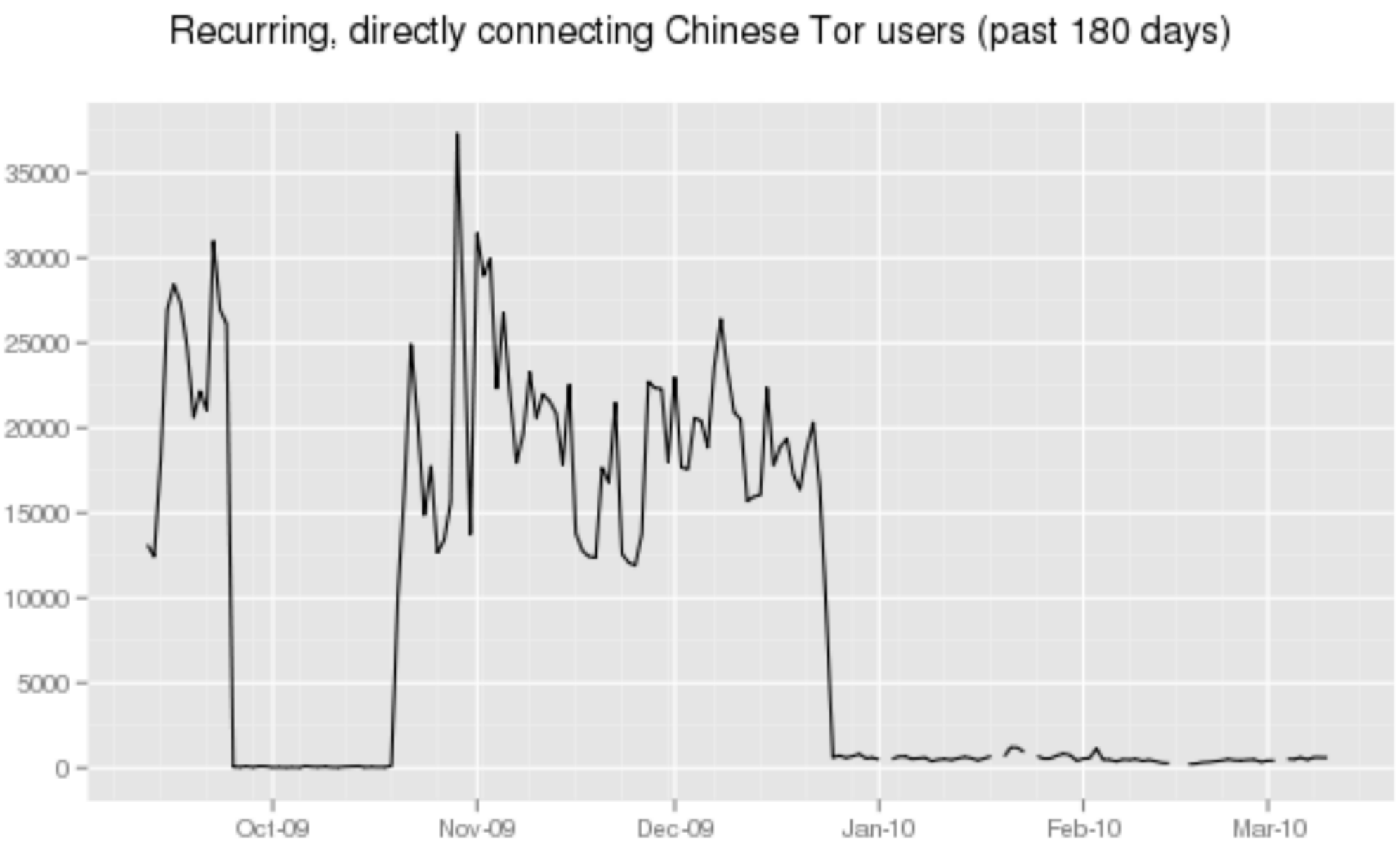
Open problems

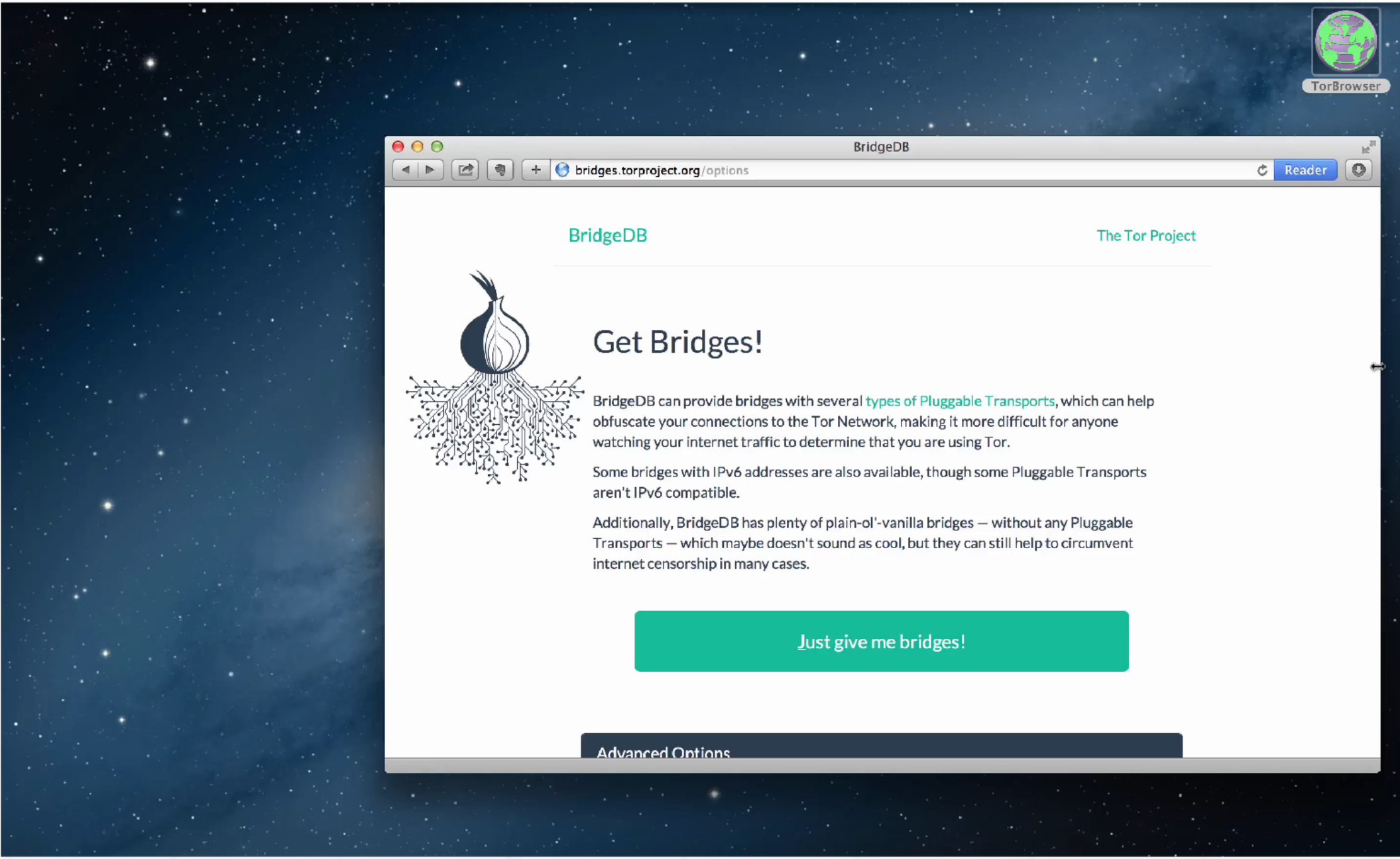
- Protocol obfuscation
- Scanning resistance
- Distribution mechanisms

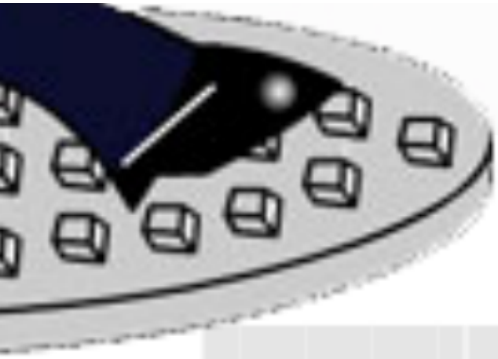

Levels of Filtering:
Pervasive
Substantial
Selective
Suspected
No evidence

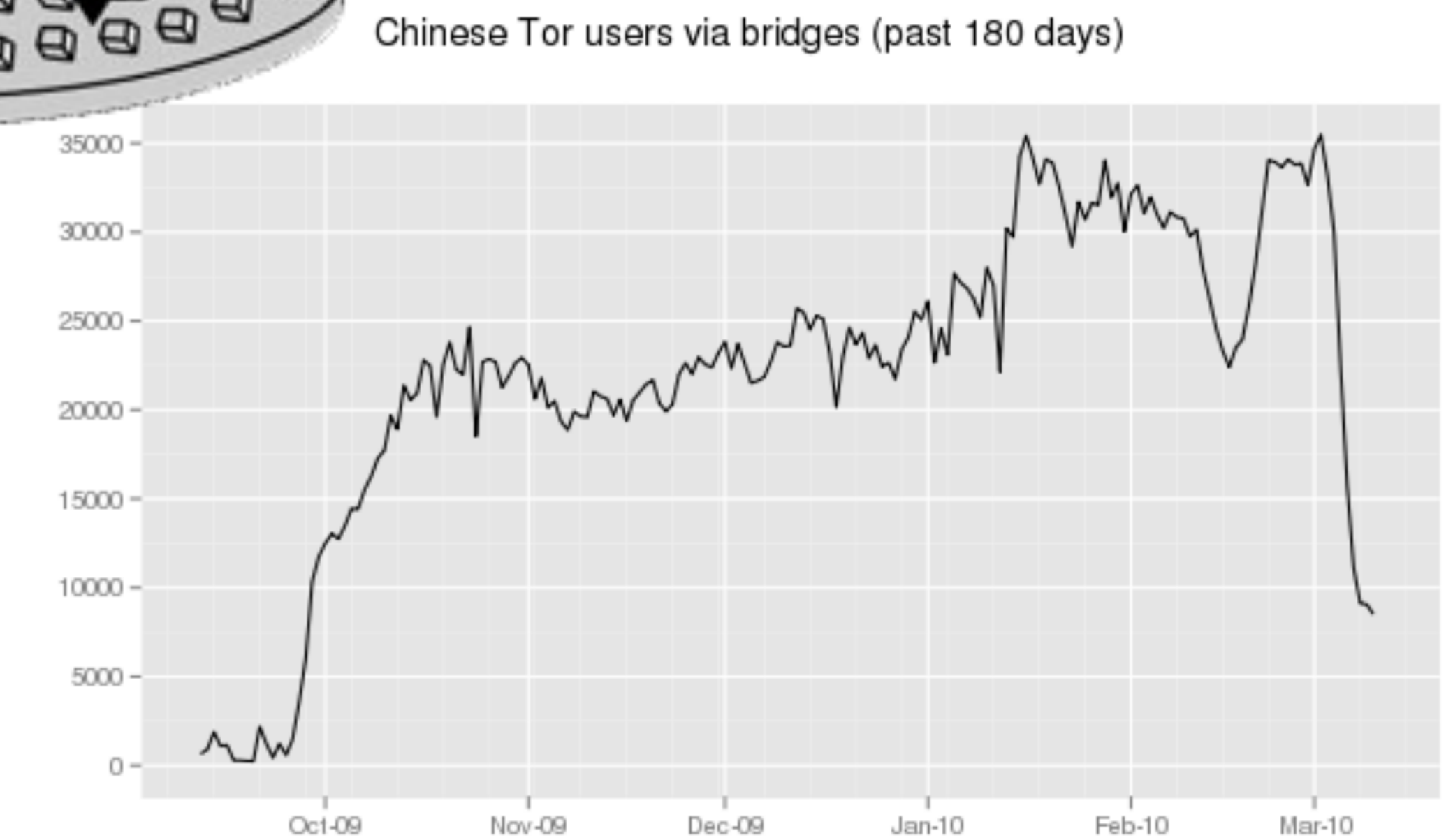
Levels of Filtering: Pervasive Substantia

Chin


Recurring, directly connecting Chinese Tor users (past 180 days)
35000
30000
25000
20000
15000
10000
5000
0
Oct-09
Nov-09
Dec-09
Jan-10
Feb-10
Mar-10


TorBrowser
BridgeDB
bridges.torproject.org/options
Reader
BridgeDB
The Tor Project
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-ol'-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!
Advanced Options

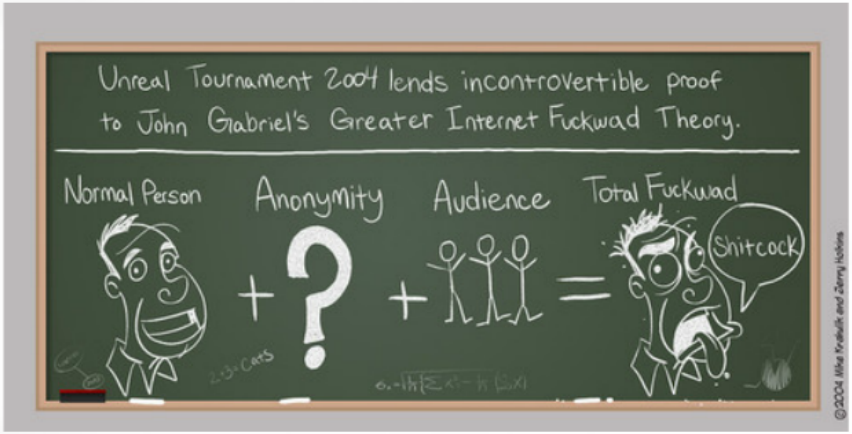


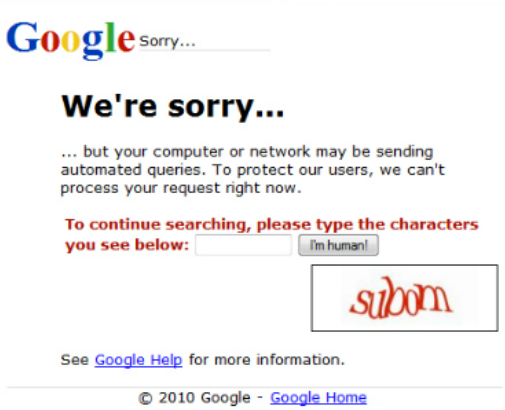

Chinese Tor users via bridges (past 180 days)
35000
30000
25000
20000
15000
10000
5000
0
Oct-09
Nov-09
Dec-09
Jan-10
Feb-10
Mar-10

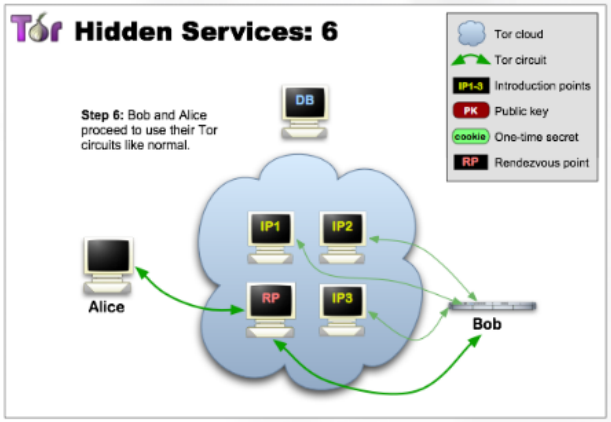
Open problems

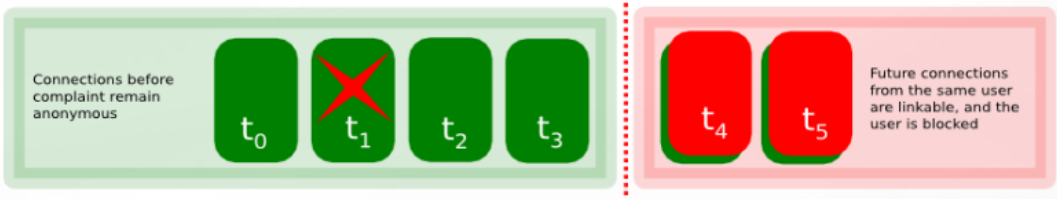
- Protocol obfuscation
- Scanning resistance
- Distribution mechanisms

Abuse



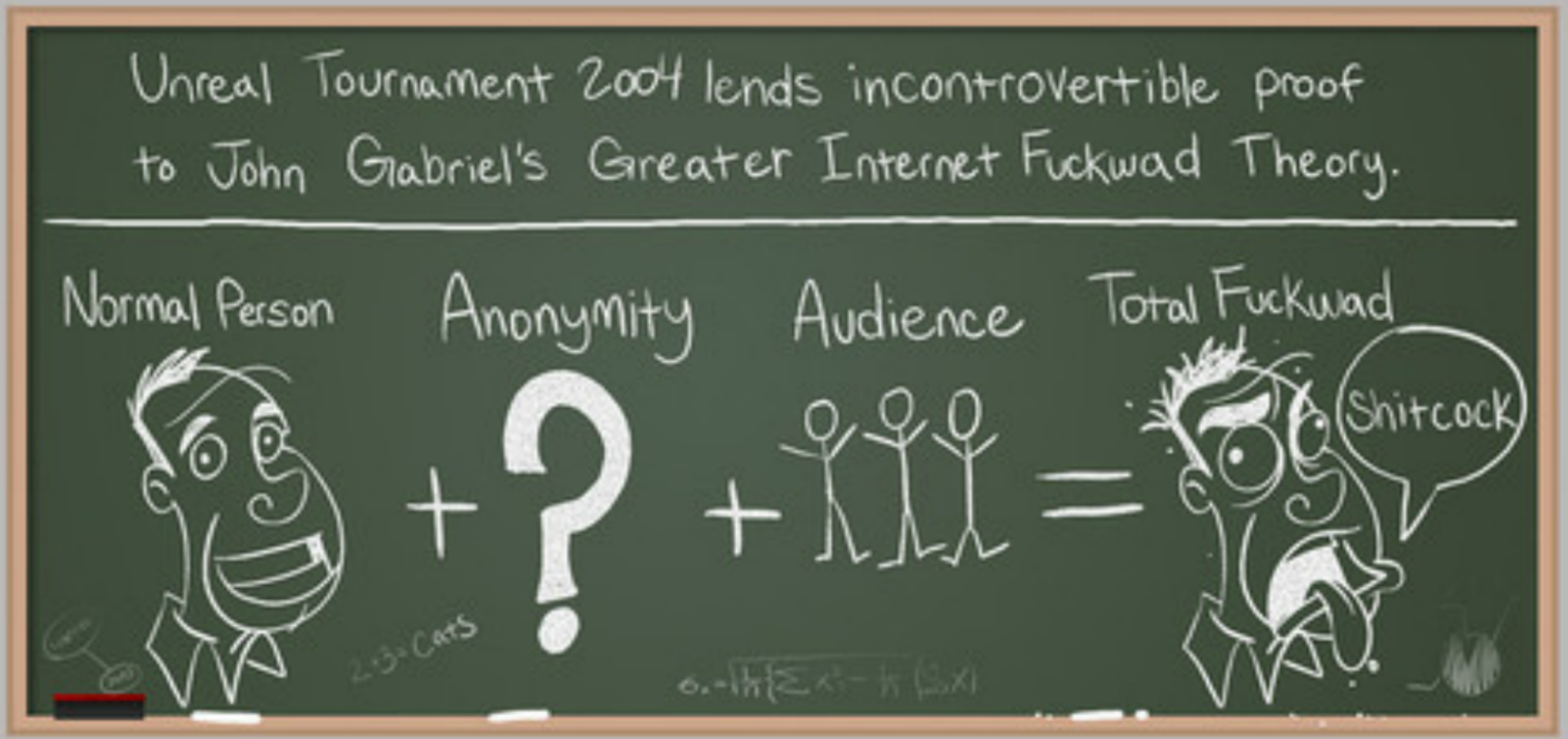






Server complains about ticket **t1** and recieves linking token for misbehaving user

Nymble


Unreal Tournament 2004 lends incontrovertible proof
to John Gabriel's Greater Internet Fuckwad Theory.
Normal Person
Anonymity
Audience
Total Fuckwad
Shitcock
©2004 Mike Krahulik and Jerry Holkins

Google Sorry...

We're sorry...

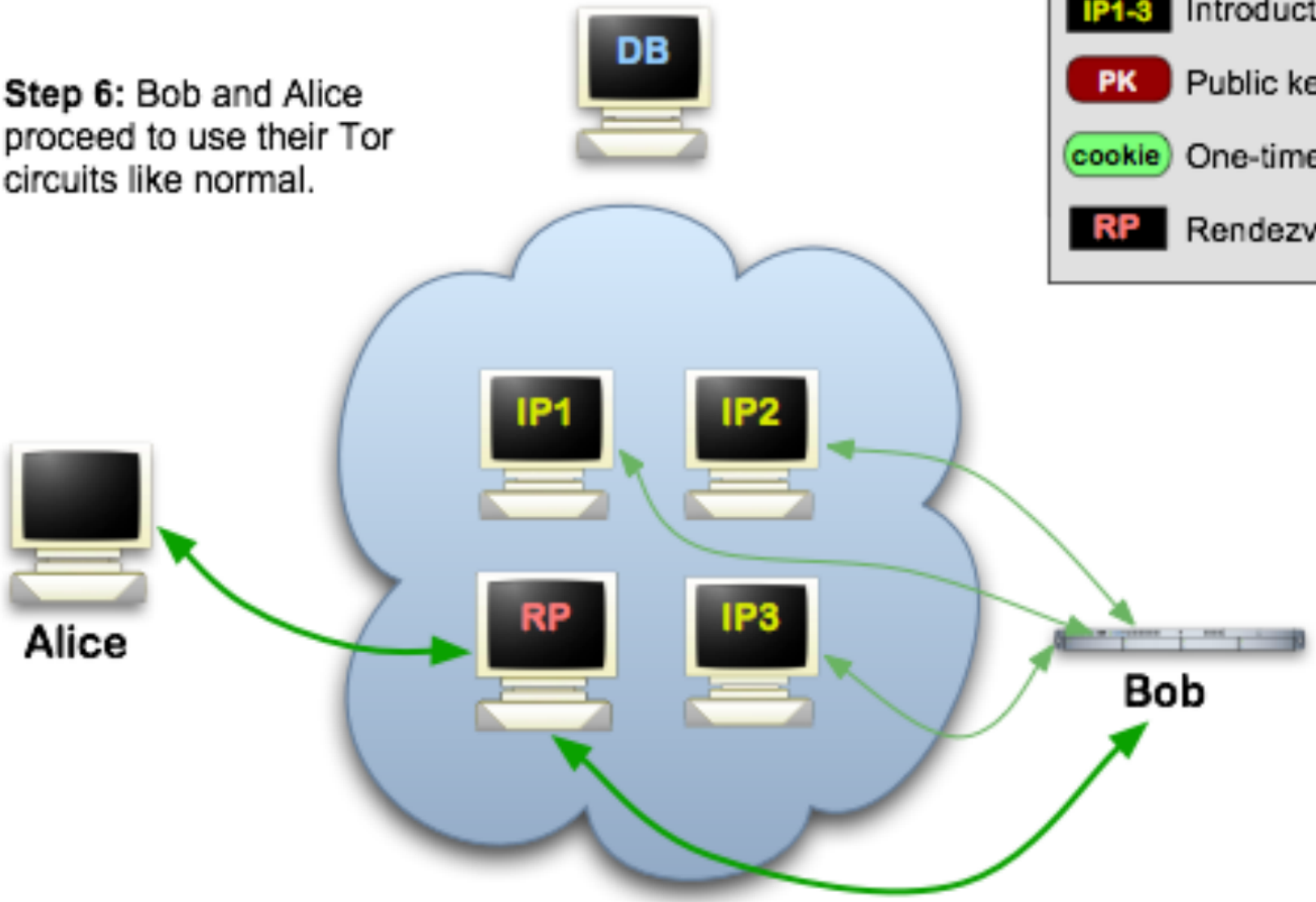
... but your computer or network may be sending automated queries. To protect our users, we can't process your request right now.

To continue searching, please type the characters you see below: I'm human!

See Google Help for more information.

Hidden Services: 6

Step 6: Bob and Alice proceed to use their Tor circuits like normal.



Tor cloud

Tor circuit

IP1-3 Introduction points

PK Public key

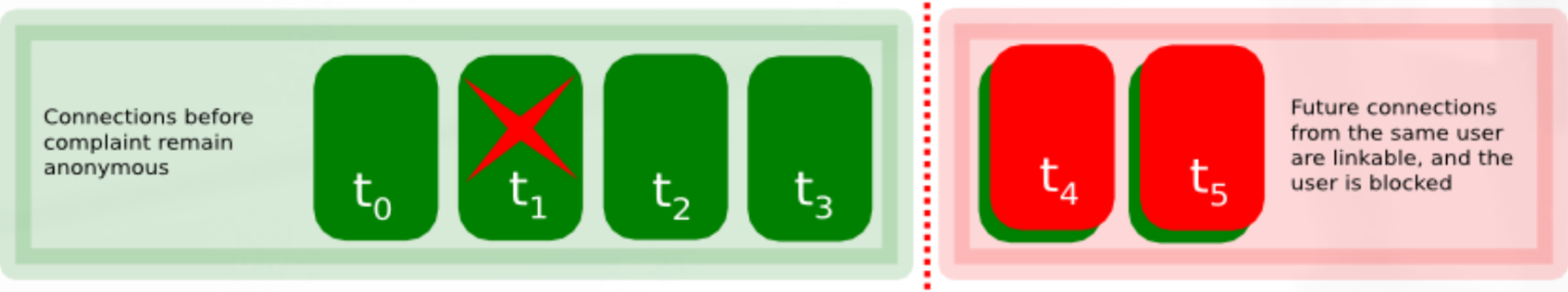
cookie One-time secret

RP Rendezvous point

Submit

See Google Help for more information.

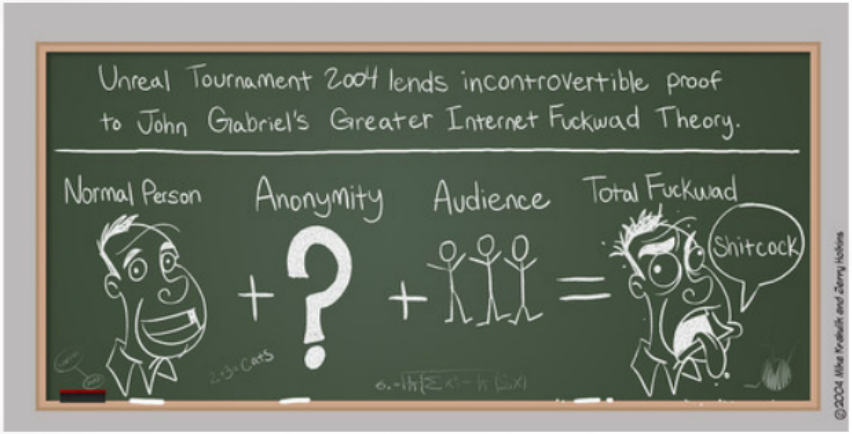
Alice

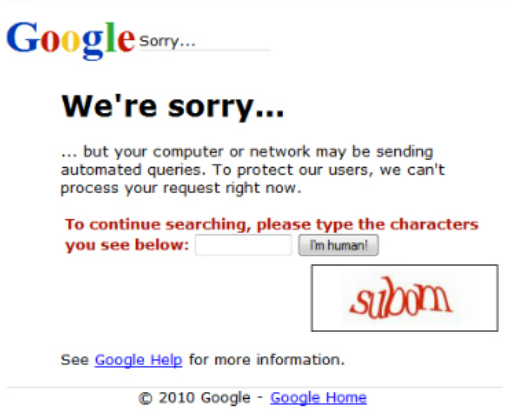


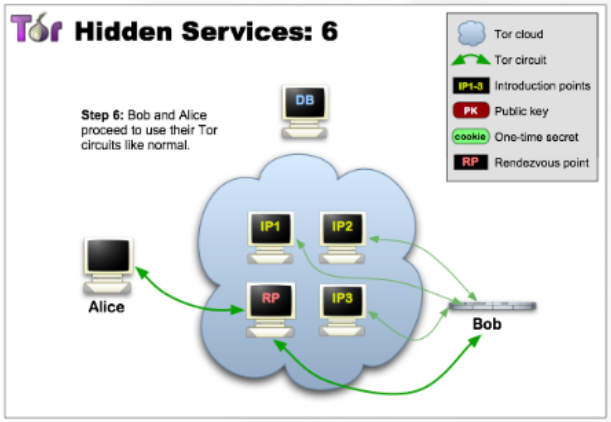
Server complains about ticket **t1** and recieves linking token for misbehaving user

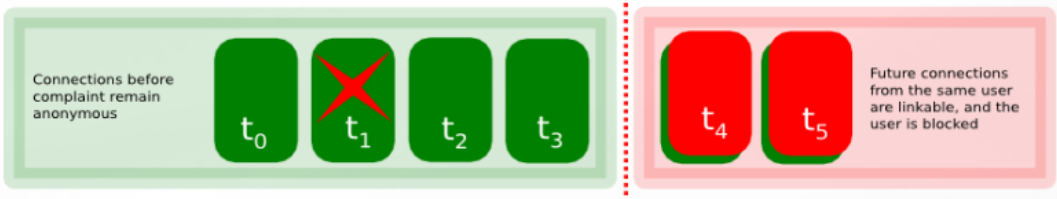
Nymble

Abuse





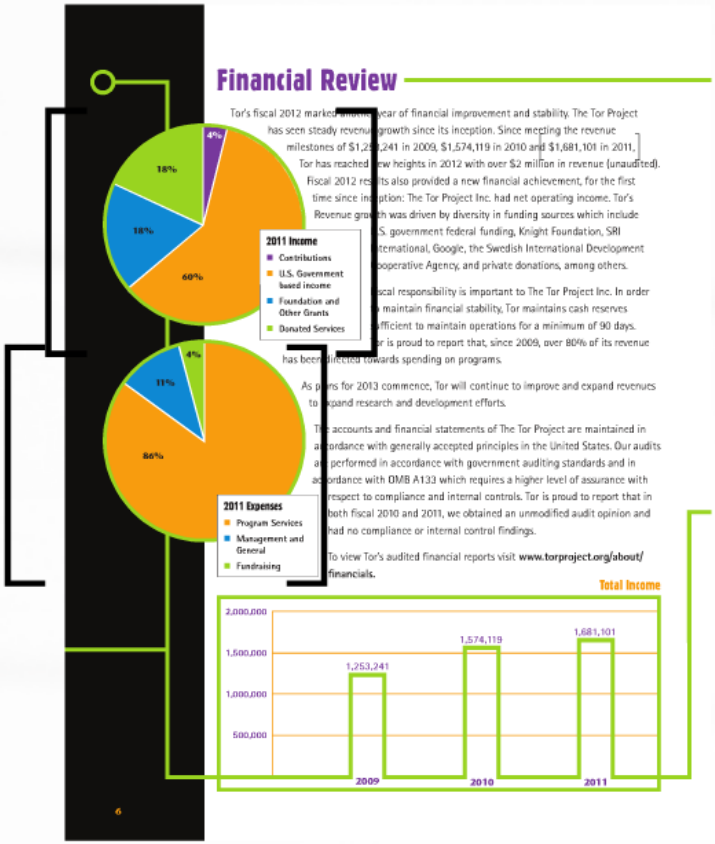




Server complains about ticket **t1** and recieves linking token for misbehaving user

Nymble

Sustainability



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.

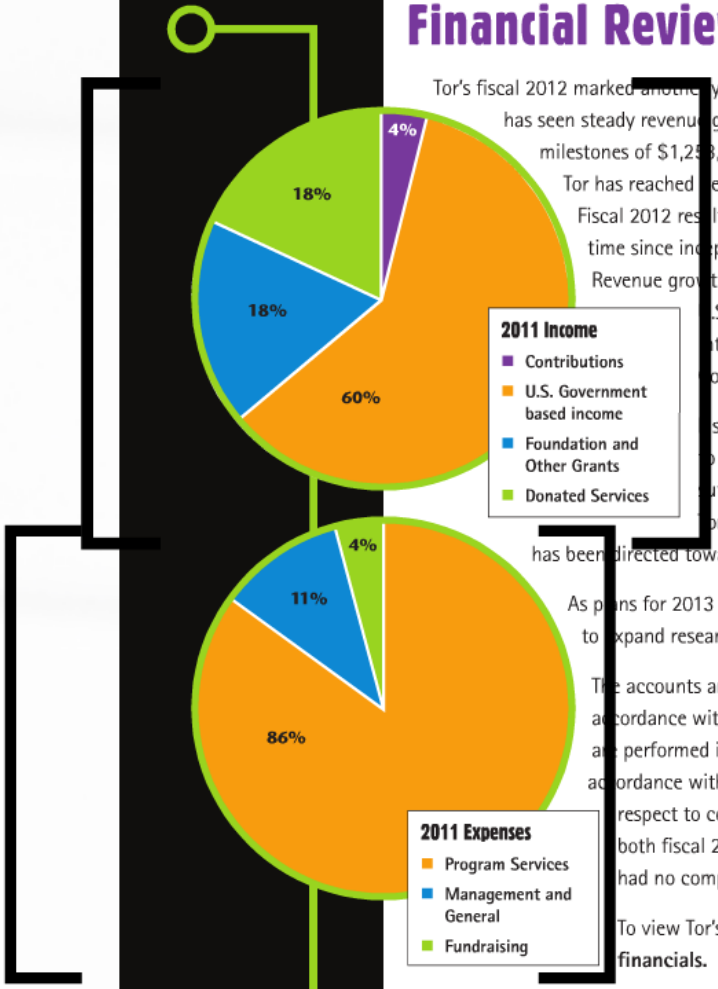
To view Tor's audited financial reports visit **www.torproject.org/about/financials.**

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.

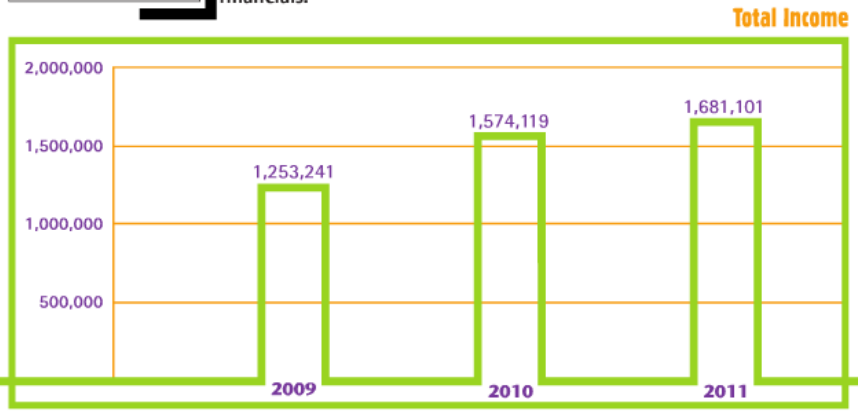


Fiscal responsibility is important to The Tor Project Inc. In order to maintain financial stability, Tor maintains cash reserves sufficient to maintain operations for a minimum of 90 days. Tor is proud to report that, since 2009, over 80% of its revenue has been directed towards spending on programs.

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.**



tability. The Ior Project

eting the revenue

d $1,681,101 in 2011,

tion in revenue (unaudi

ievement. for the first

has been

As p

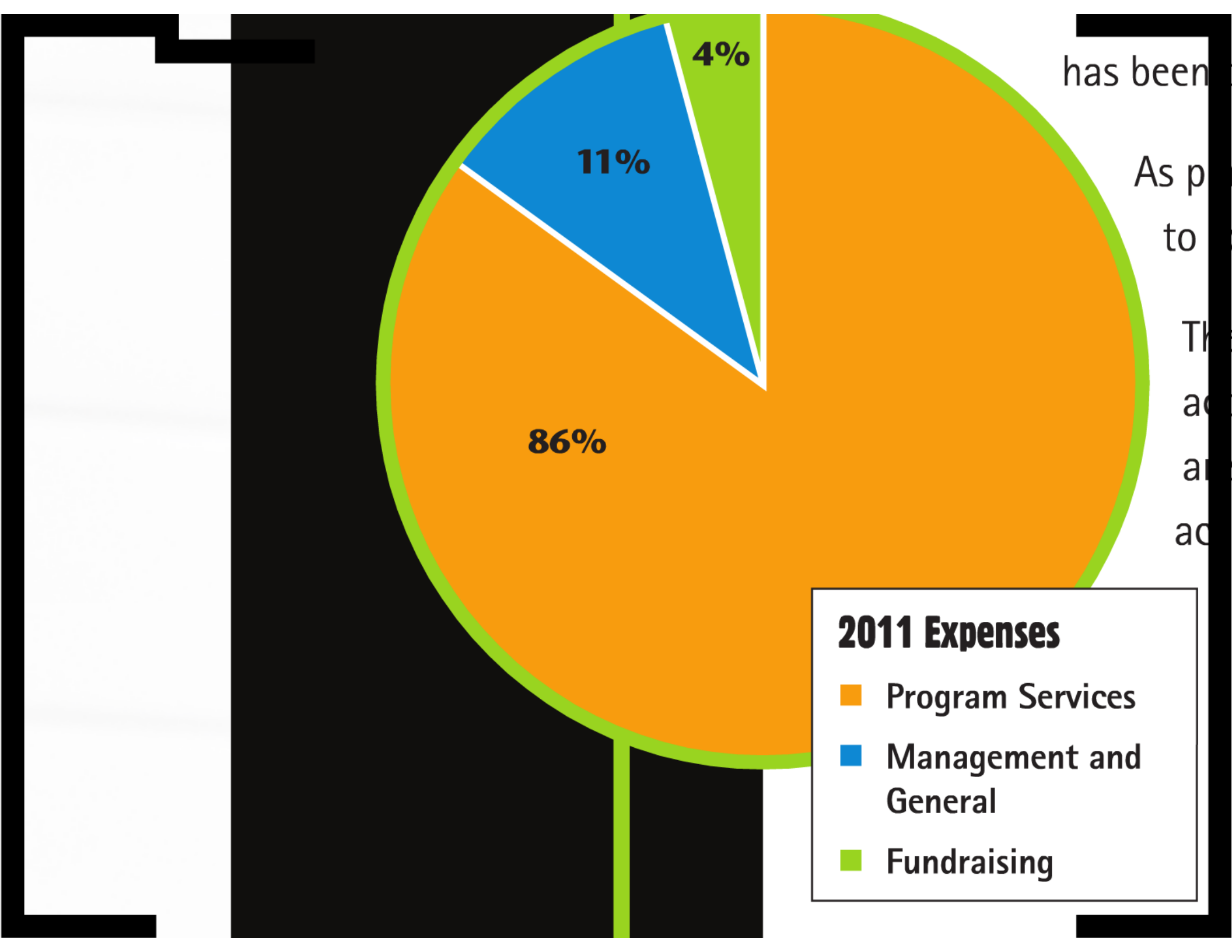
to

Th

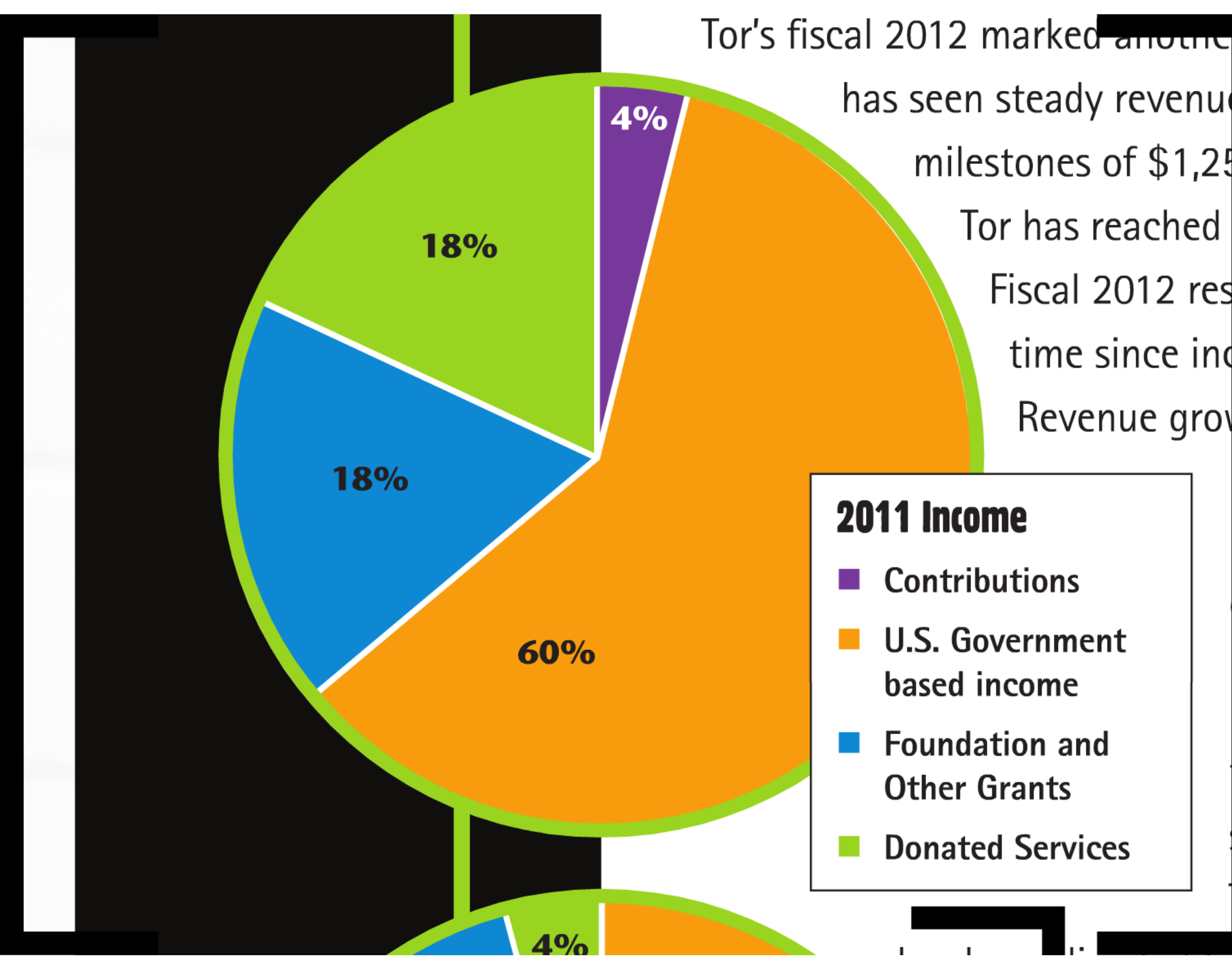
a

a

a



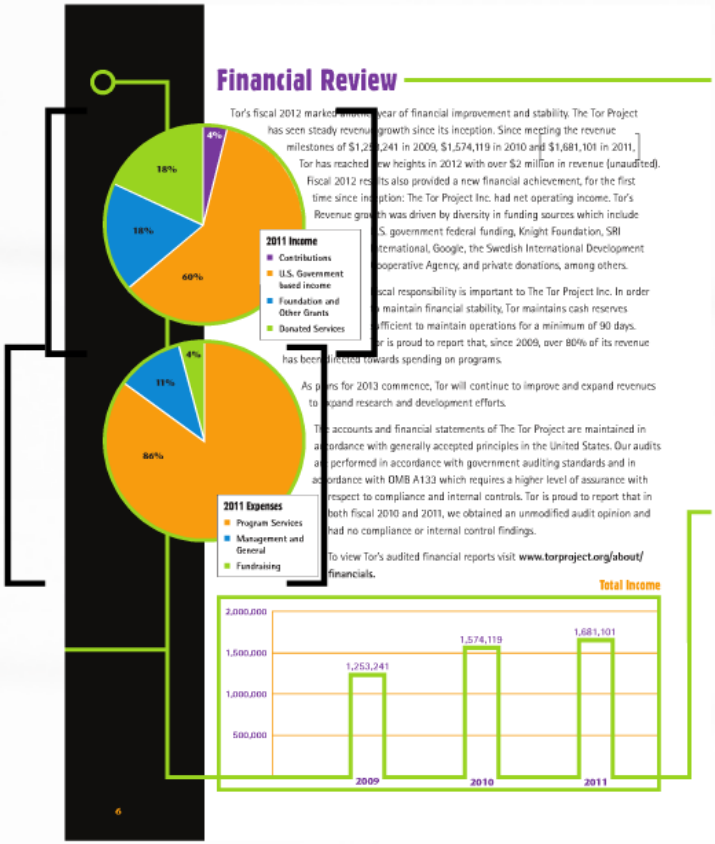
Tor's fiscal 2012 marked another
has seen steady revenue
milestones of $1,25
Tor has reached
Fiscal 2012 res
time since inc
Revenue grow



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

Sustainability



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.**

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