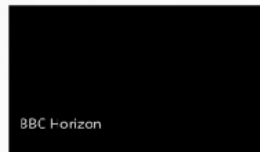


Who needs anonymity?

- 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?

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?

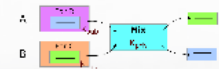
Remailers

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

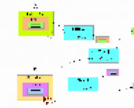
Type-1 (Cypherpunk)

- Mix decrypts messages
- Uses PGP



Mixmaster (1998-)

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



Mixminion (2002-)

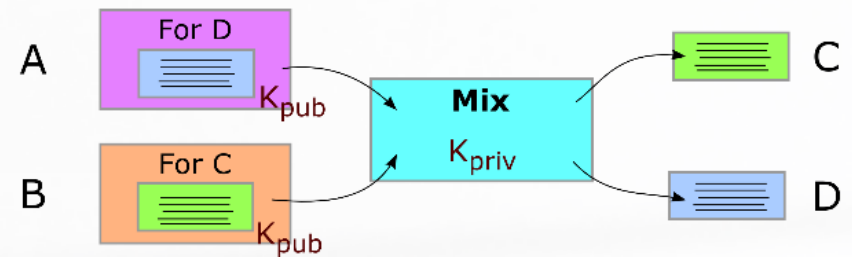
- Fixed many problems
- Introduced replies

penet.fi (1993-1996)

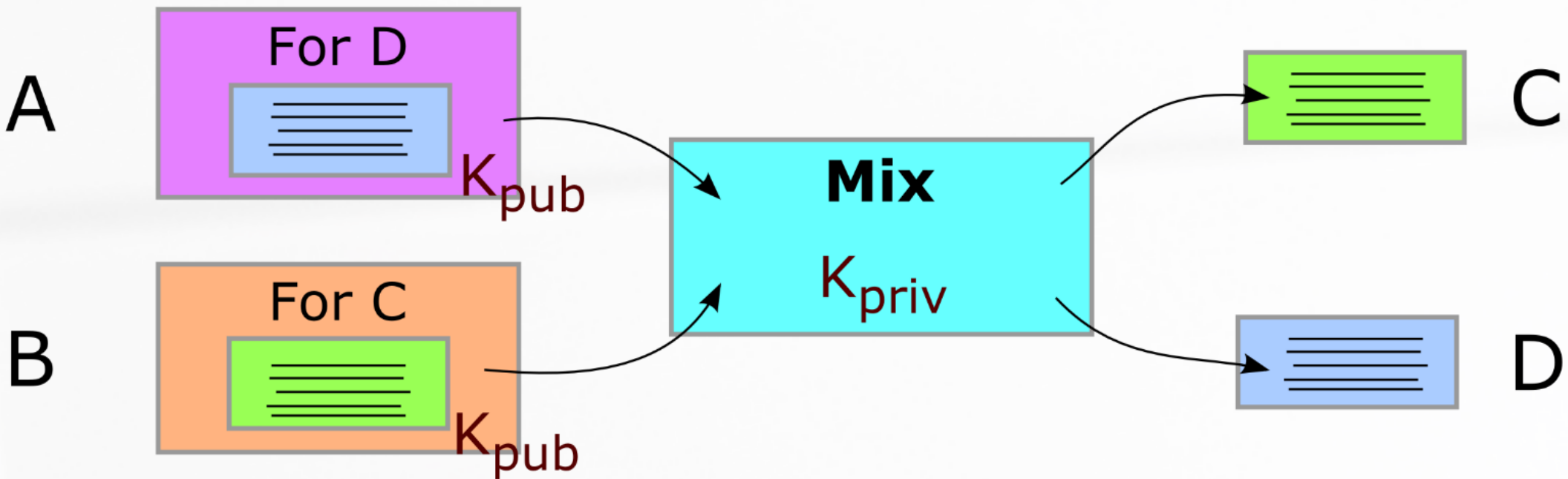
- Simply stripped headers off emails sent via remailer
- Allowed replies to be sent
- Easy to use, but single point of compromise
- Shut down following compromise by CoS

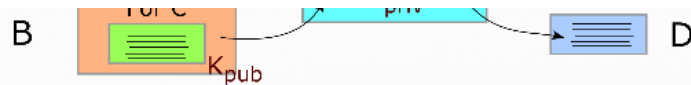
Type-1 (Cypherpunk)

- Mix decrypts messages
- Uses PGP



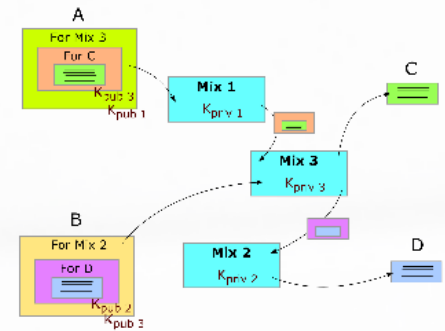
messages





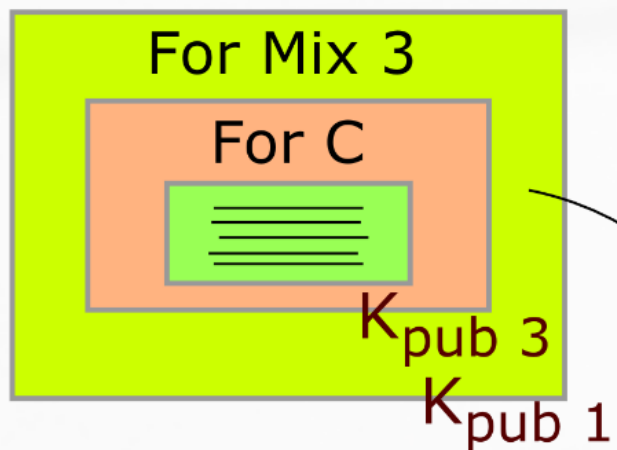
Mixmaster (1998-)

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

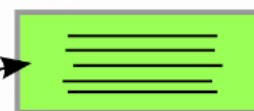


Mixminion (2002-)

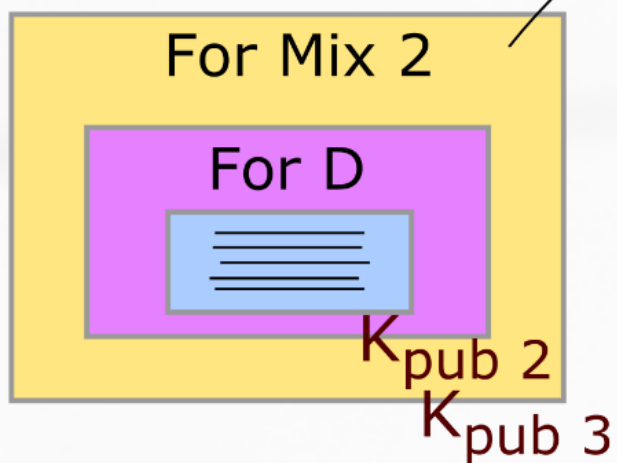
A



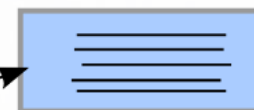
C

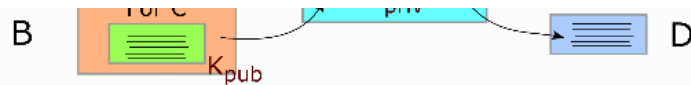


B



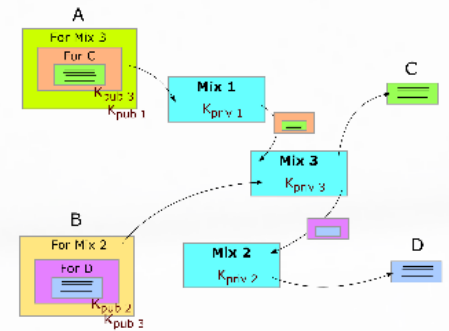
D





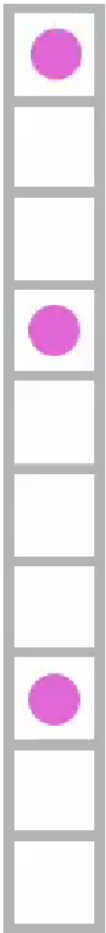
Mixmaster (1998-)

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

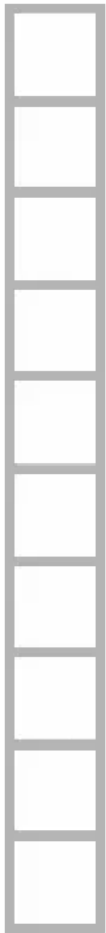


Mixminion (2002-)

Senders



Receivers



Mix

Mixminion (2002-)

- Fixed many problems
- Introduced replies

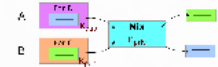
Remailers

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)

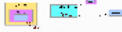


Mixminion (2002-)

- Fixed many problems
- Introduced replies

Number of users ≈ 0

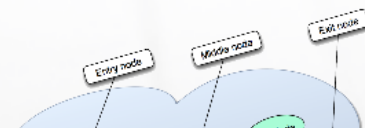
- Simply stripped headers off emails sent via remailer
- Allowed replies to be sent
- Easy to use, but single point of compromise
- Shut down following compromise by CoS

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

Mixminion (2002-)

- Fixed many problems
- Introduced replies

Number of users ≈ 0



98%

The Web

Web browsing is hard to secure

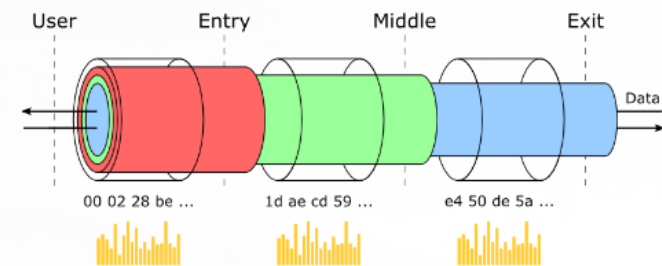
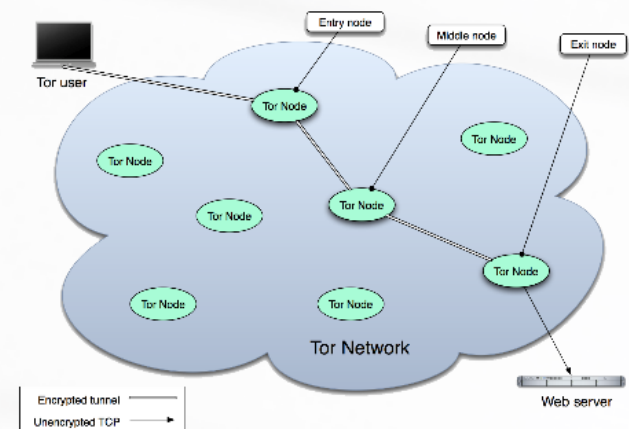
- Requires low latency
- High variability
- Low tolerance to padding

Equivalent systems

Open proxies \approx penet.fi

VPN \approx Type-0

MixMinion \approx Tor



The 'Web

Web browsing is hard to secure

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

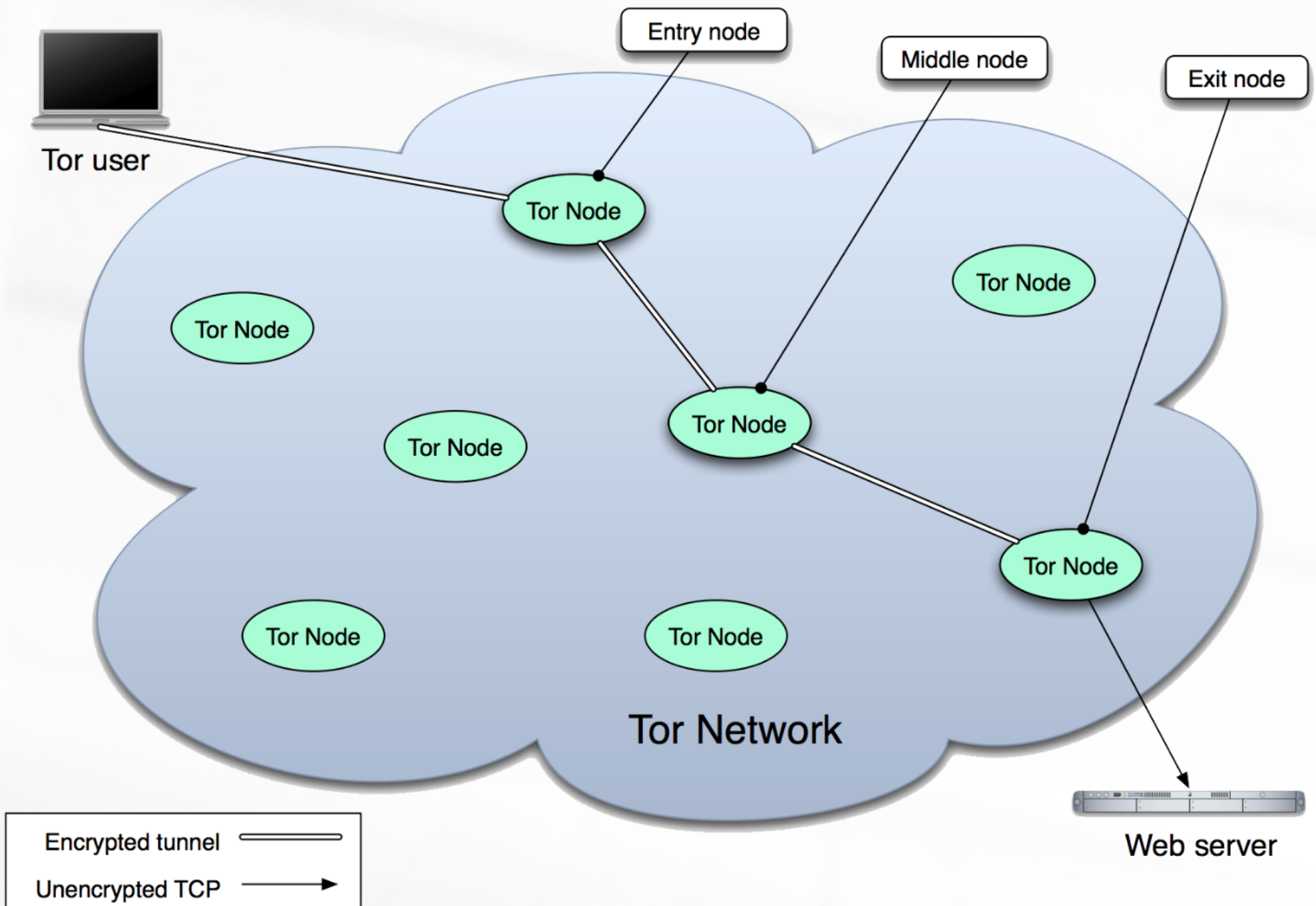
Equivalent systems

Equivalent systems

Open proxies \approx penet.fi

VPN \approx Type-0

MixMinion \approx Tor



Tor user



Rendevous point



Tor Node

Tor Node

Tor Node

Tor Node

Tor Node

Tor Node

Tor Node

Tor Node

Tor Network



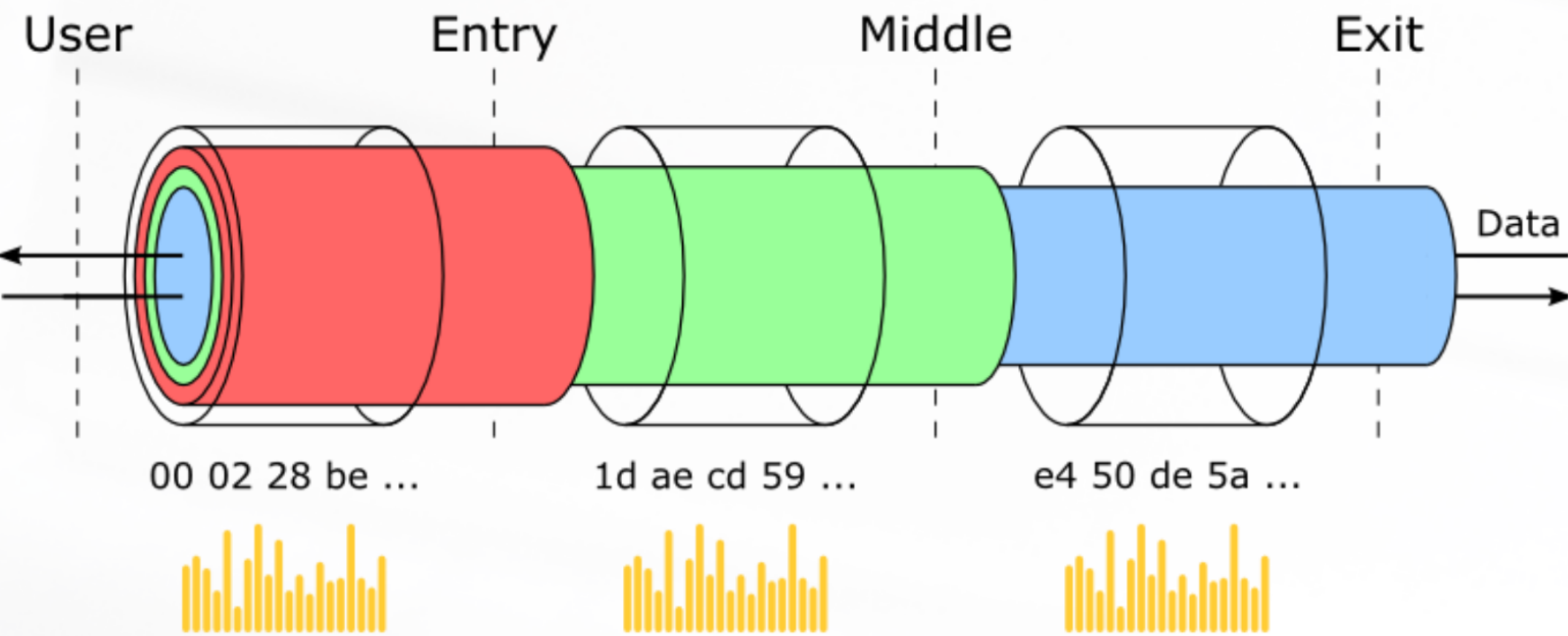
Hidden
web server

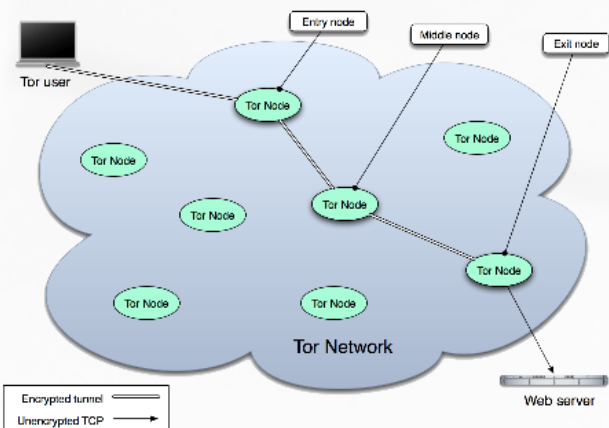
Encrypted tunnel



Unencrypted TCP

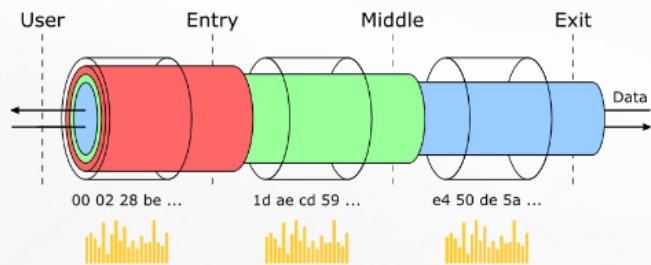
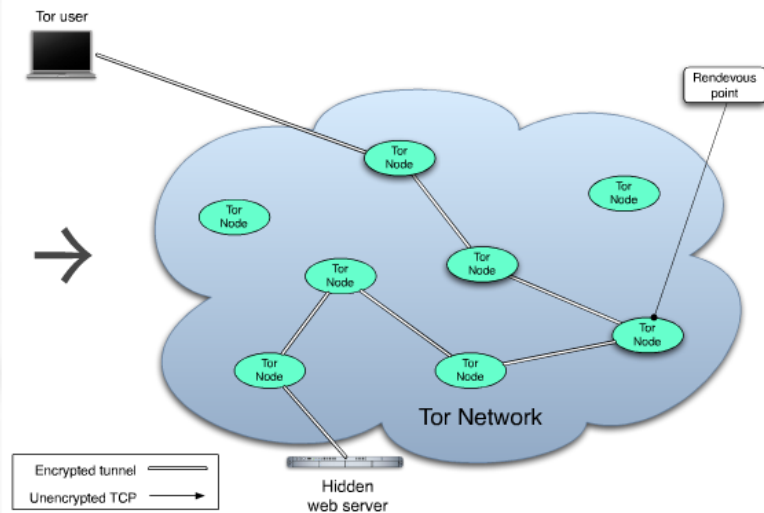






← 98%

2% →



The Web

Web browsing is hard to secure

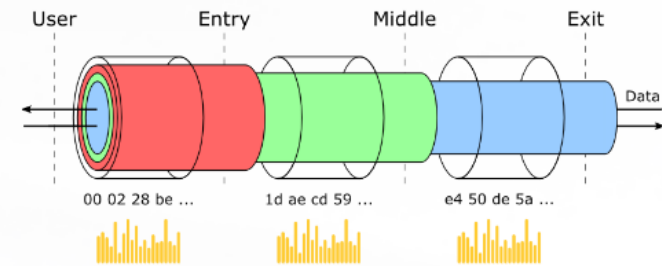
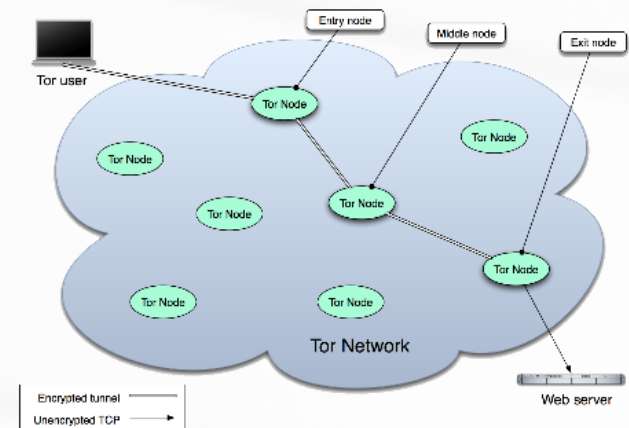
- Requires low latency
- High variability
- Low tolerance to padding

Equivalent systems

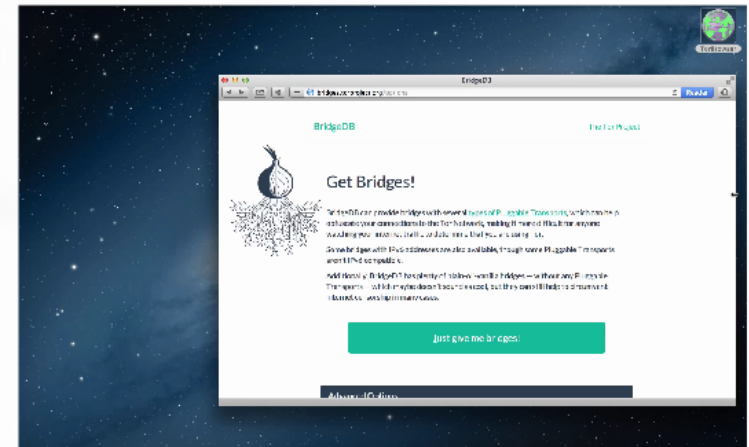
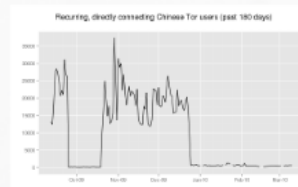
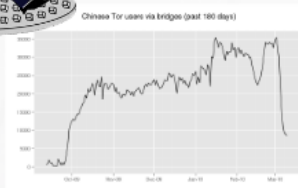
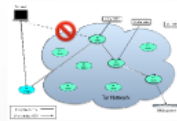
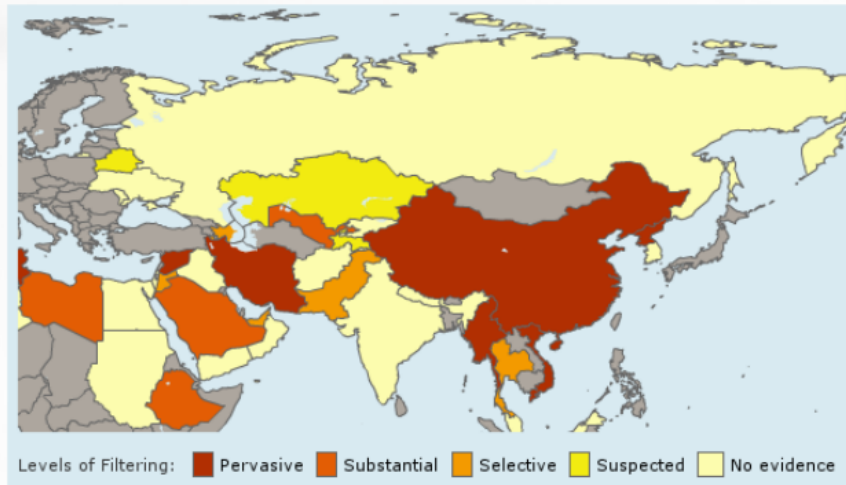
Open proxies \approx penet.fi

VPN \approx Type-0

MixMinion \approx Tor



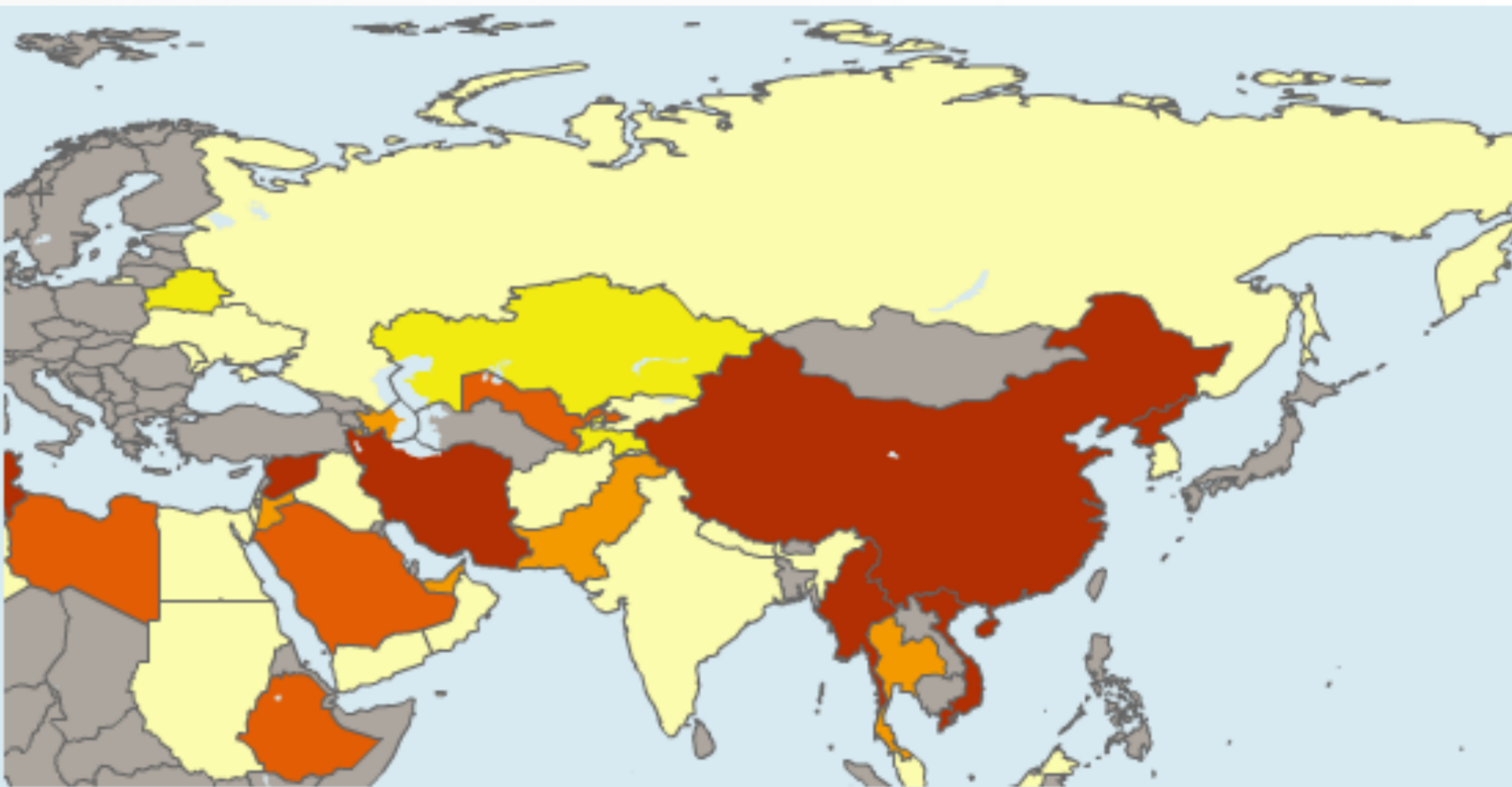
Censorship resistance



Open problems for bridges

- Protocol obfuscation
- Scanning resistance
- Distribution mechanisms

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



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



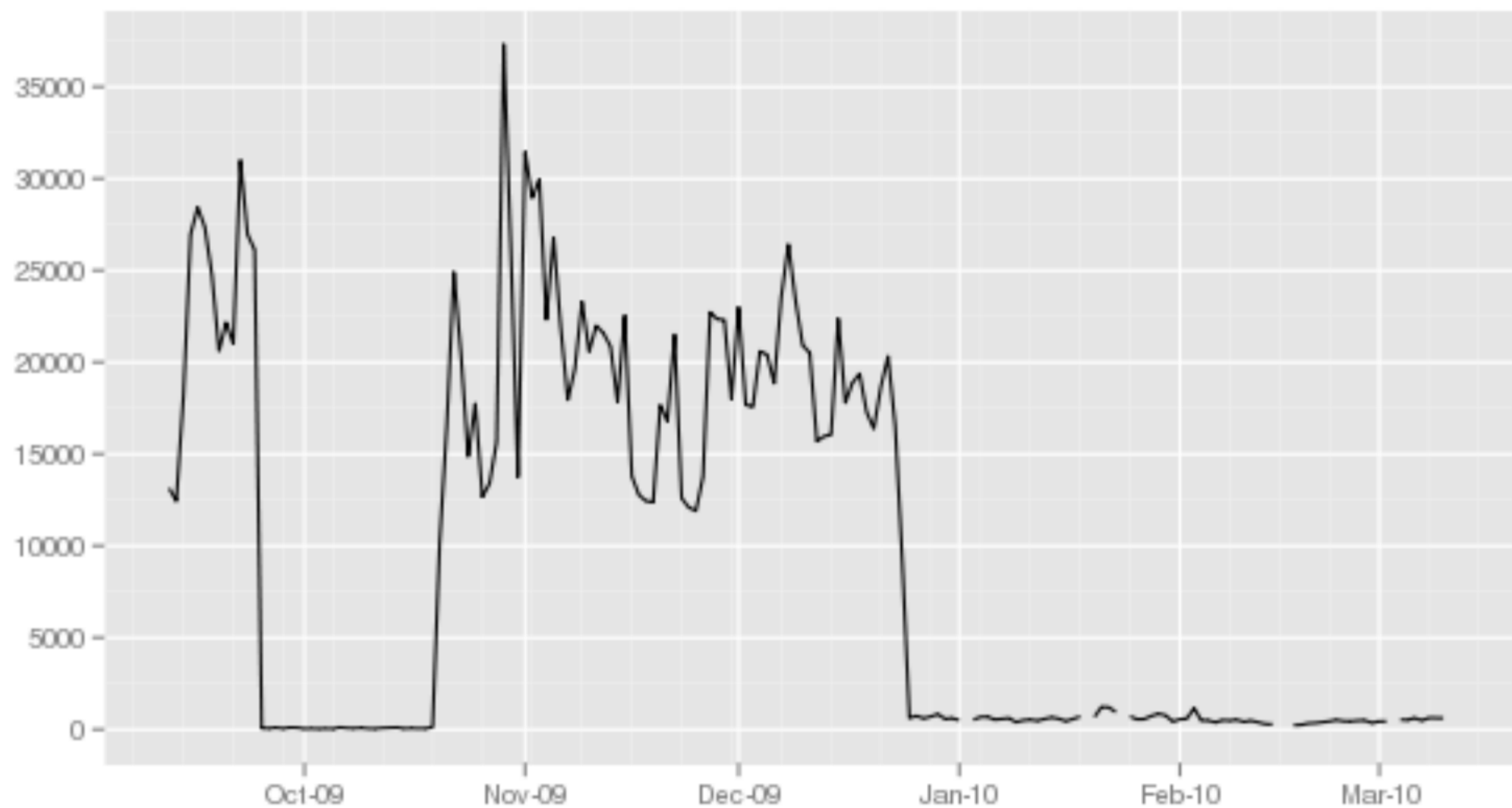
Levels of Filtering: ■ Pervasive ■ Substantia

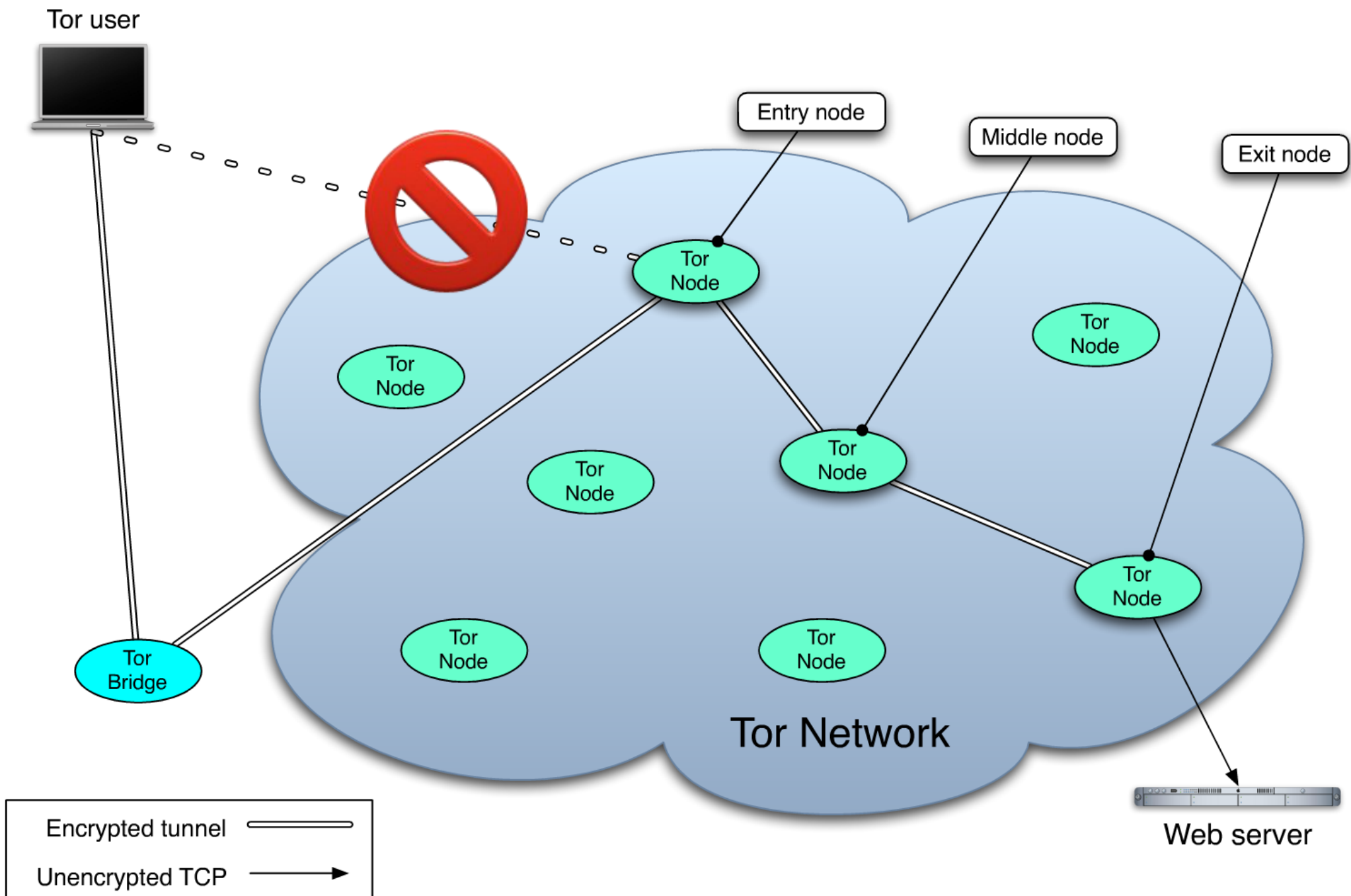


China

35000
30000
25000
20000

Recurring, directly connecting Chinese Tor users (past 180 days)



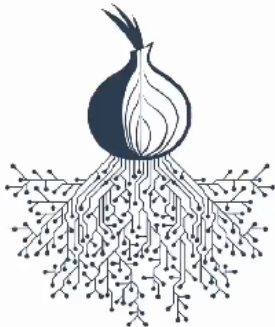




TorBrowser

BridgeDB

The Tor Project



Get Bridges!

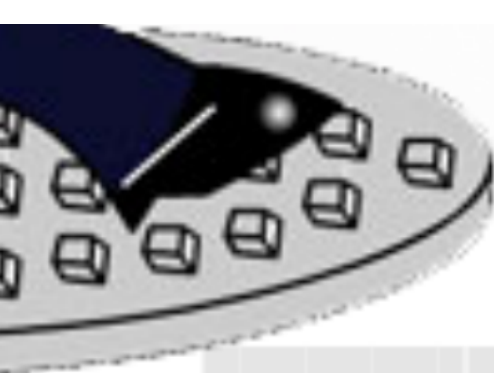
BridgeDB can provide bridges with several [types of Pluggable Transports](#), which can help obfuscate your connections to the Tor Network, making it more difficult for anyone watching your internet traffic to determine that you are using Tor.

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

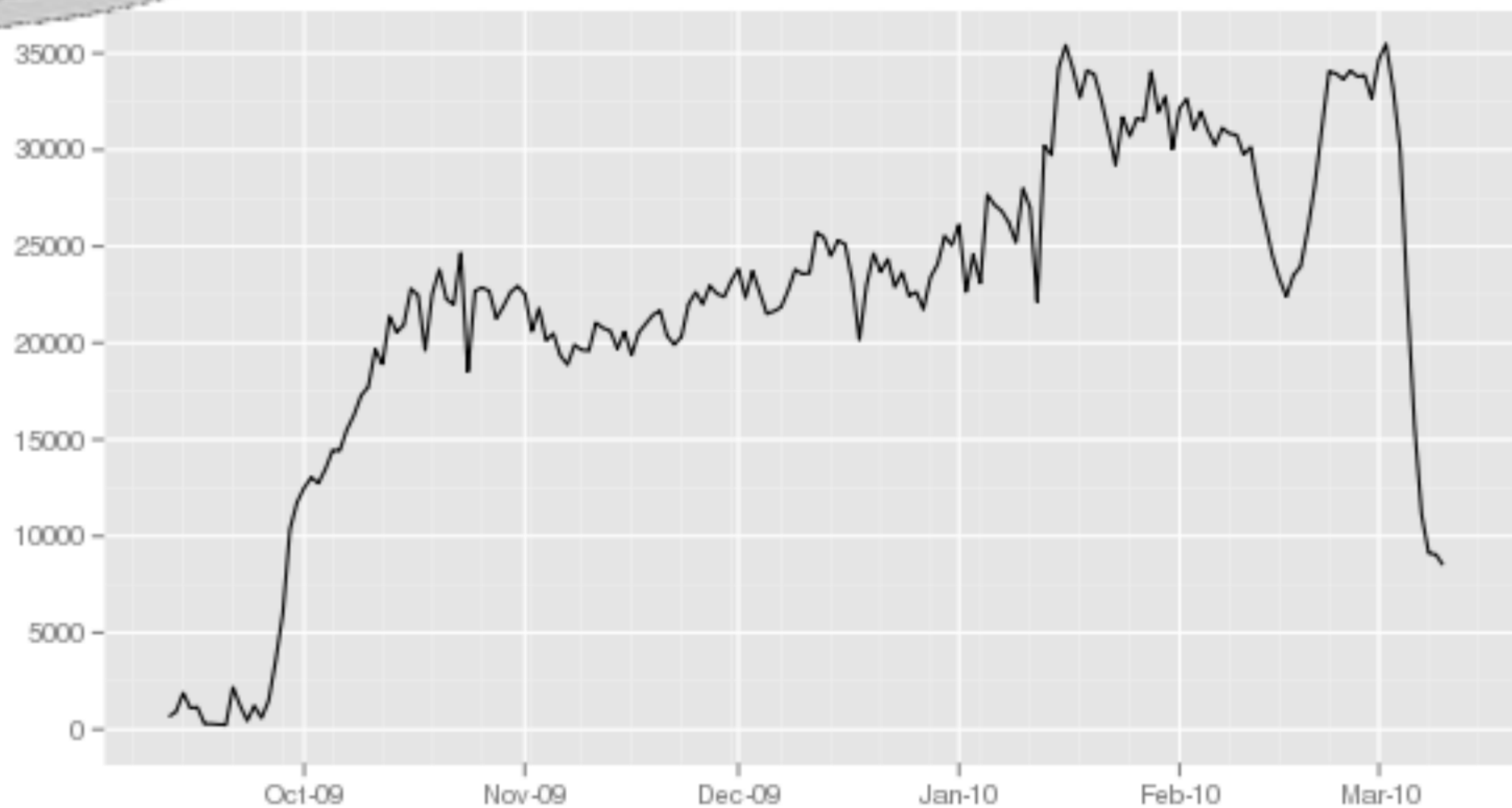
Additionally, BridgeDB has plenty of plain-ol'-vanilla bridges — without any Pluggable Transports — which maybe doesn't sound as cool, but they can still help to circumvent internet censorship in many cases.

Just give me bridges!

Advanced Options



Chinese Tor users via bridges (past 180 days)

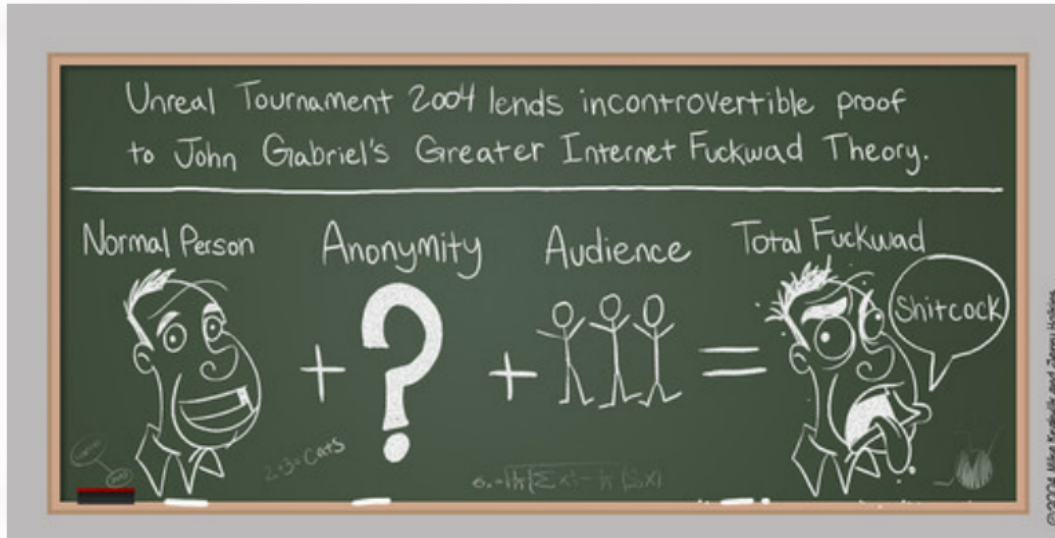


Open problems for bridges

- Protocol obfuscation
- Scanning resistance
- Distribution mechanisms

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

Abuse



Google Sorry...

We're sorry...

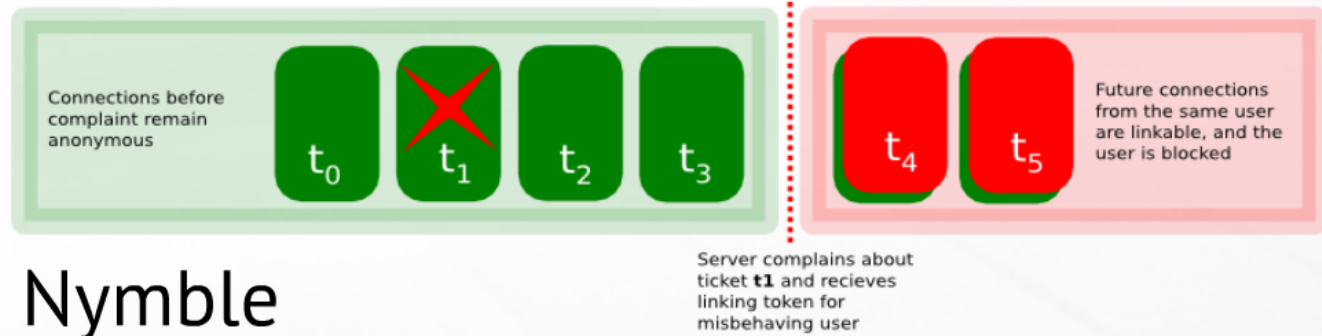
... but your computer or network may be sending automated queries. To protect our users, we can't process your request right now.

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

subom

See [Google Help](#) for more information.

© 2010 Google - [Google Home](#)



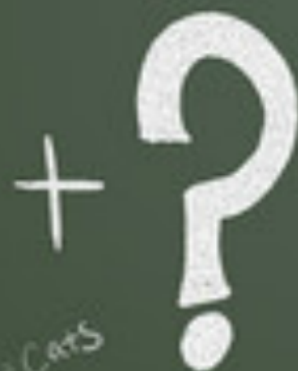
Nymble

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

Normal Person



Anonymity



$2+3=5$ Cats

Audience



$\sigma = \sqrt{\frac{1}{n}(\sum x_i^2 - \frac{(\sum x_i)^2}{n})}$

Total Fuckwad





We're sorry...

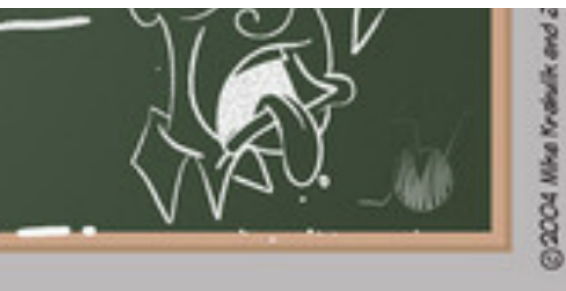
... but your computer or network may be sending automated queries. To protect our users, we can't process your request right now.

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

I'm human!

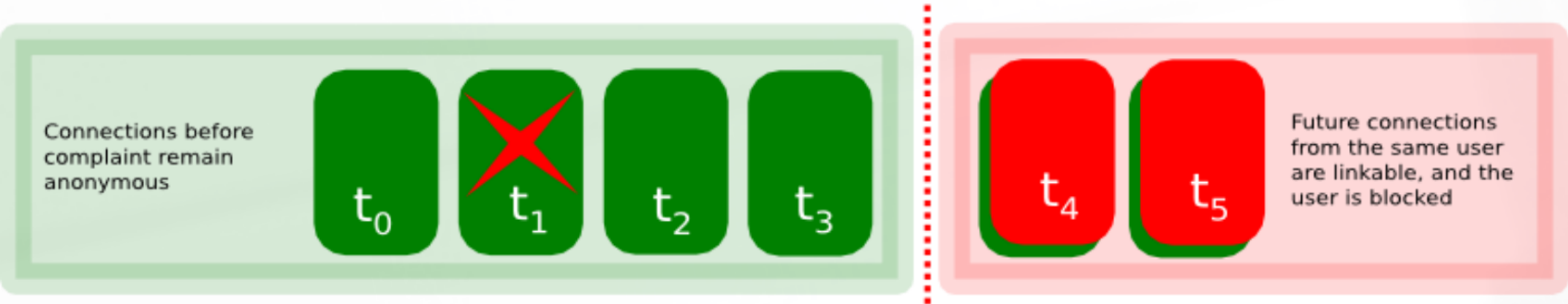
A rectangular box containing the word "suborn" written in a red, cursive, handwritten-style font.

See [Google Help](#) for more information.



See [Google Help](#) for more information.

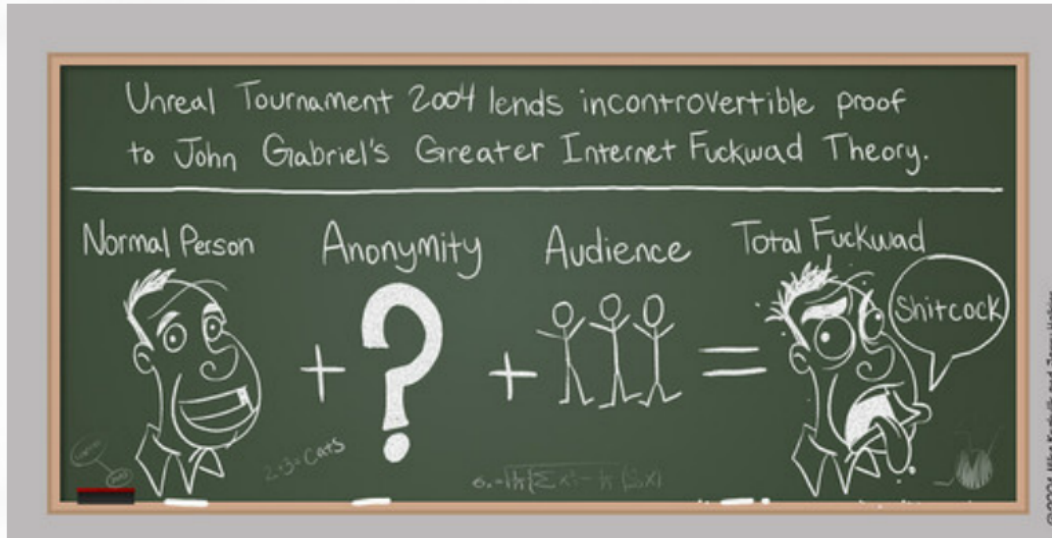
© 2010 Google - [Google Home](#)



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

Nymble

Abuse



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.

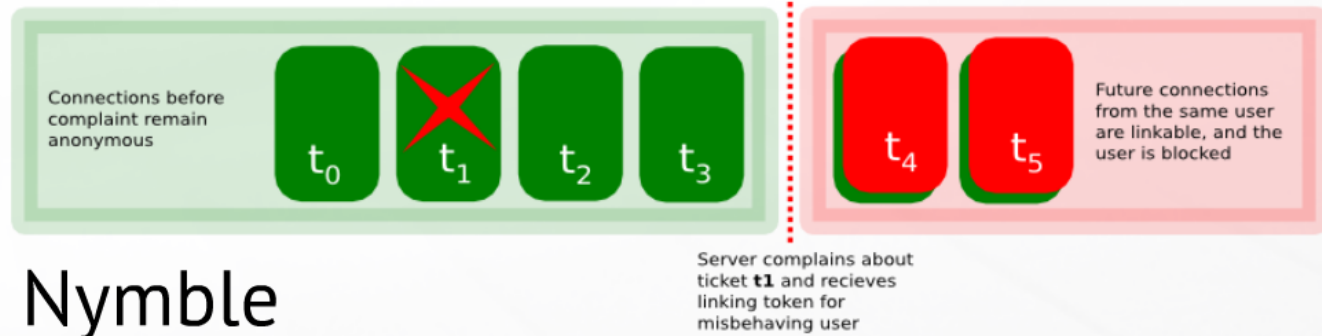
To continue searching, please type the characters you see below:

I'm human!

subom

See [Google Help](#) for more information.

© 2010 Google - [Google Home](#)



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 \$1,241,241 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).

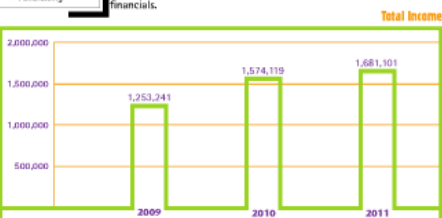
Fiscal 2012 results also provided a new financial achievement, for the first time since inception: The Tor Project Inc. had net operating income. Tor's Revenue growth was driven by diversity in funding sources which include U.S. government federal funding, Knight Foundation, SRI International, Google, the Swedish International Development Co-operative Agency, and private donations, among others.

Financial 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 Co-operative Agency, and private donations, among others.

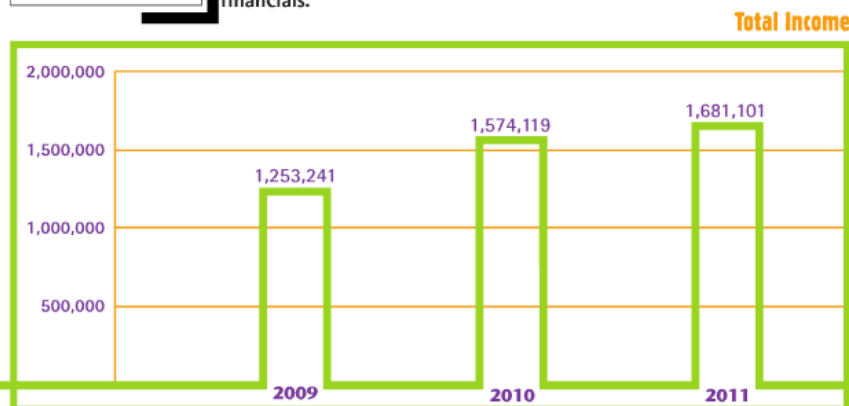
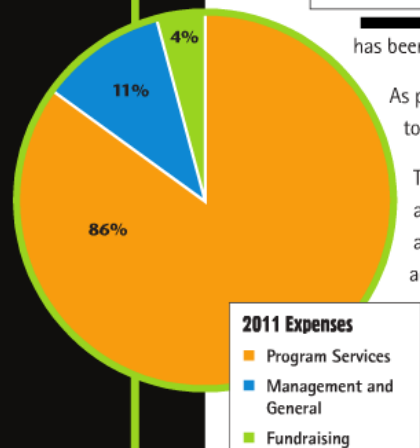
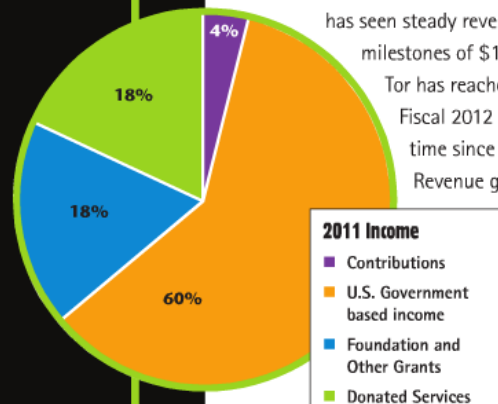
Financial responsibility is important to The Tor Project Inc. In order to maintain financial stability, Tor maintains cash reserves sufficient to maintain operations for a minimum of 90 days.

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.



ability. The Ior Project

eting the revenue

d \$1,681,101 in 2011,

tion in revenue (unaudited)

ievement, for the first

has been

As p

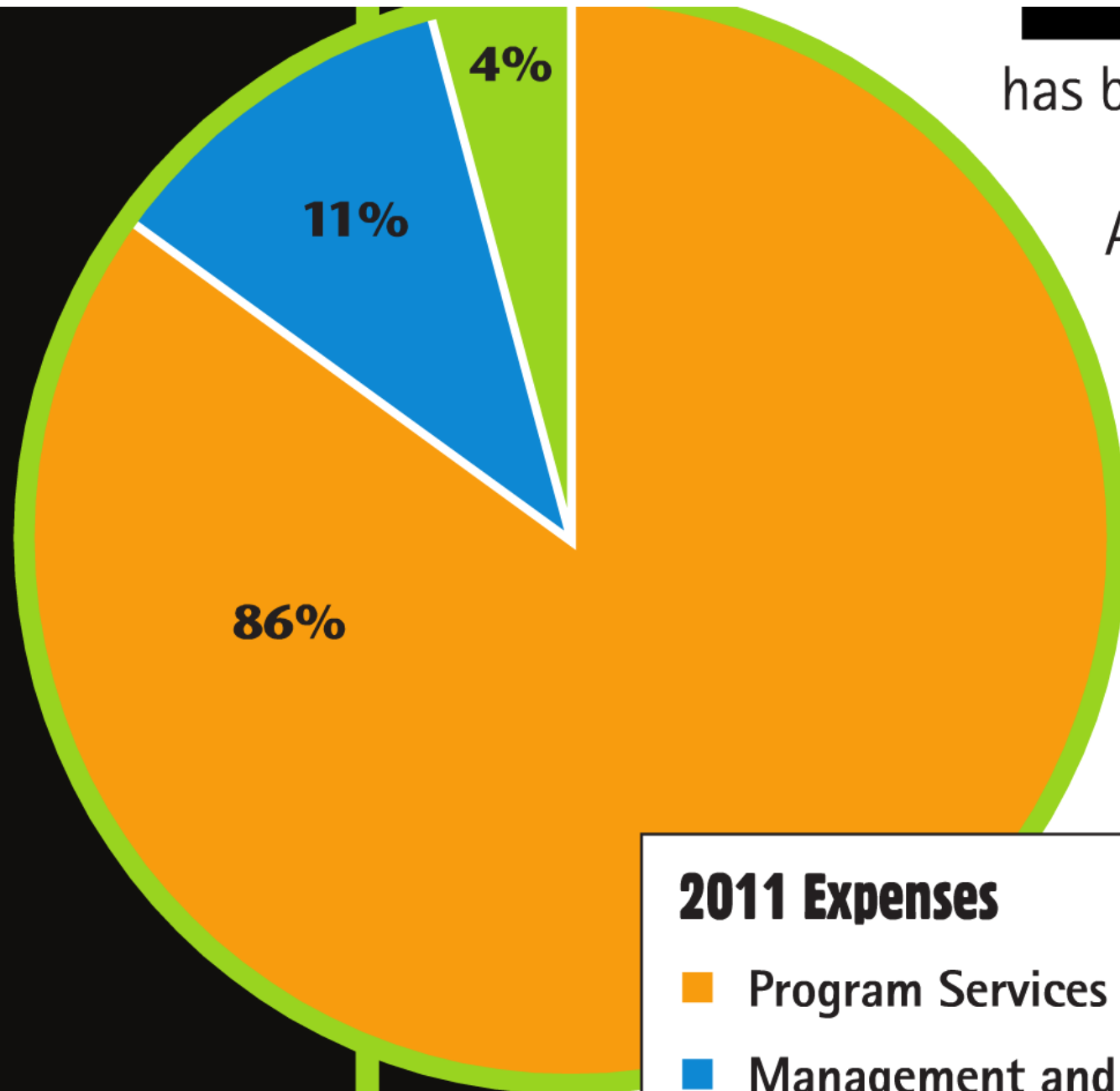
to

Th

ac

an

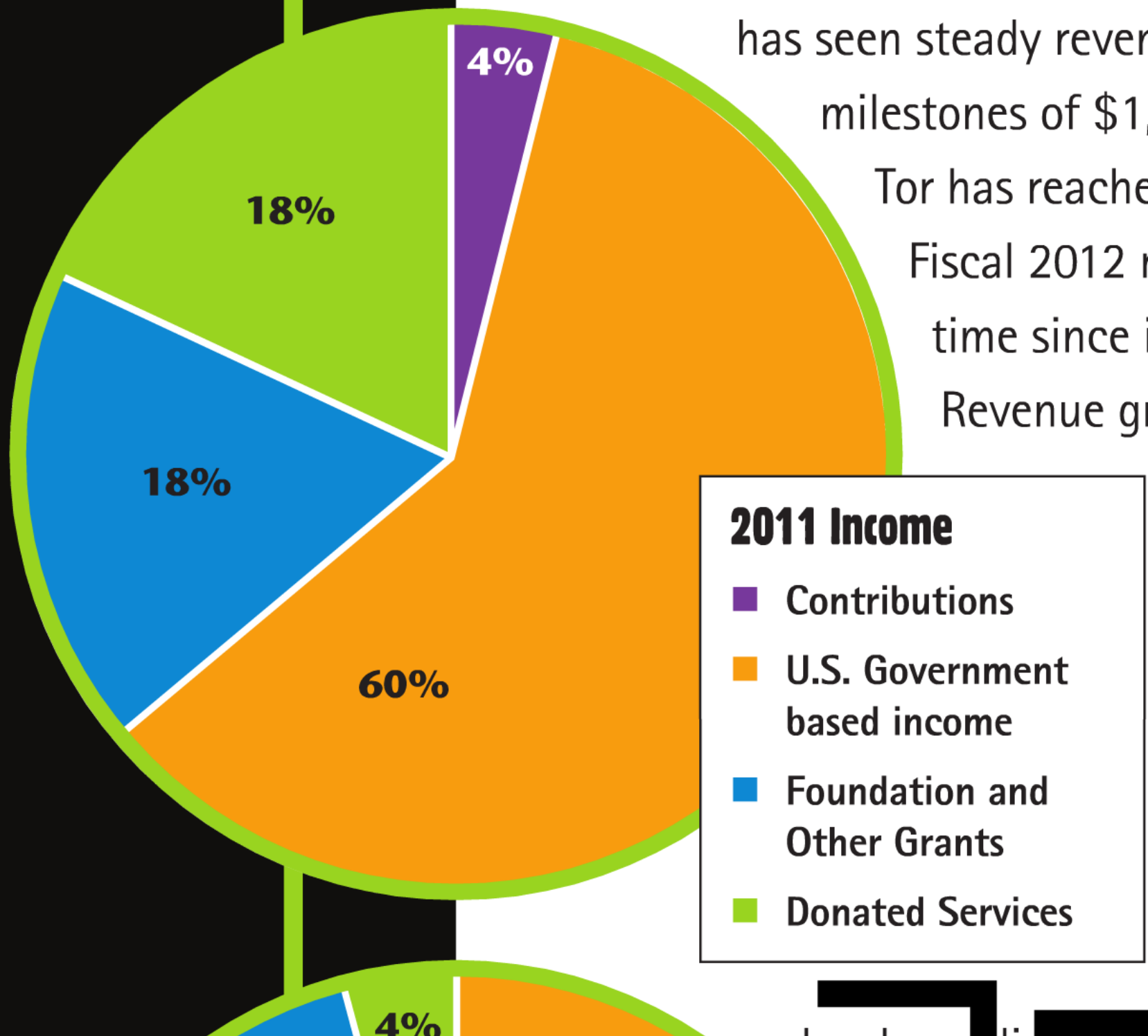
ac



2011 Expenses

- Program Services
- Management and General
- Fundraising

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

Juice Media Rap News
September 2012

THIS IS WHAT A
Tor



DAN ELLSBERG AND PATRICIA MARX ELLSBERG, PRIVACY ACTIVISTS

SUPPORTER
LOOKS LIKE

#SUPPORT**Tor**

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 \$1,241,241 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).

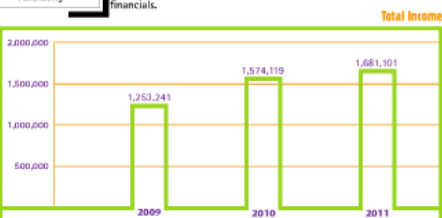
Fiscal 2012 results also provided a new financial achievement, for the first time since inception: The Tor Project Inc. had net operating income. Tor's Revenue growth was driven by diversity in funding sources which include U.S. government federal funding, Knight Foundation, SRI International, Google, the Swedish International Development Co-operative Agency, and private donations, among others.

Financial 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