VASCO THE AUTHENTICATION COMPANY

UCL

Anonymity & Censorship-free Communication

Steven J. Murdoch
VASCO & University College London

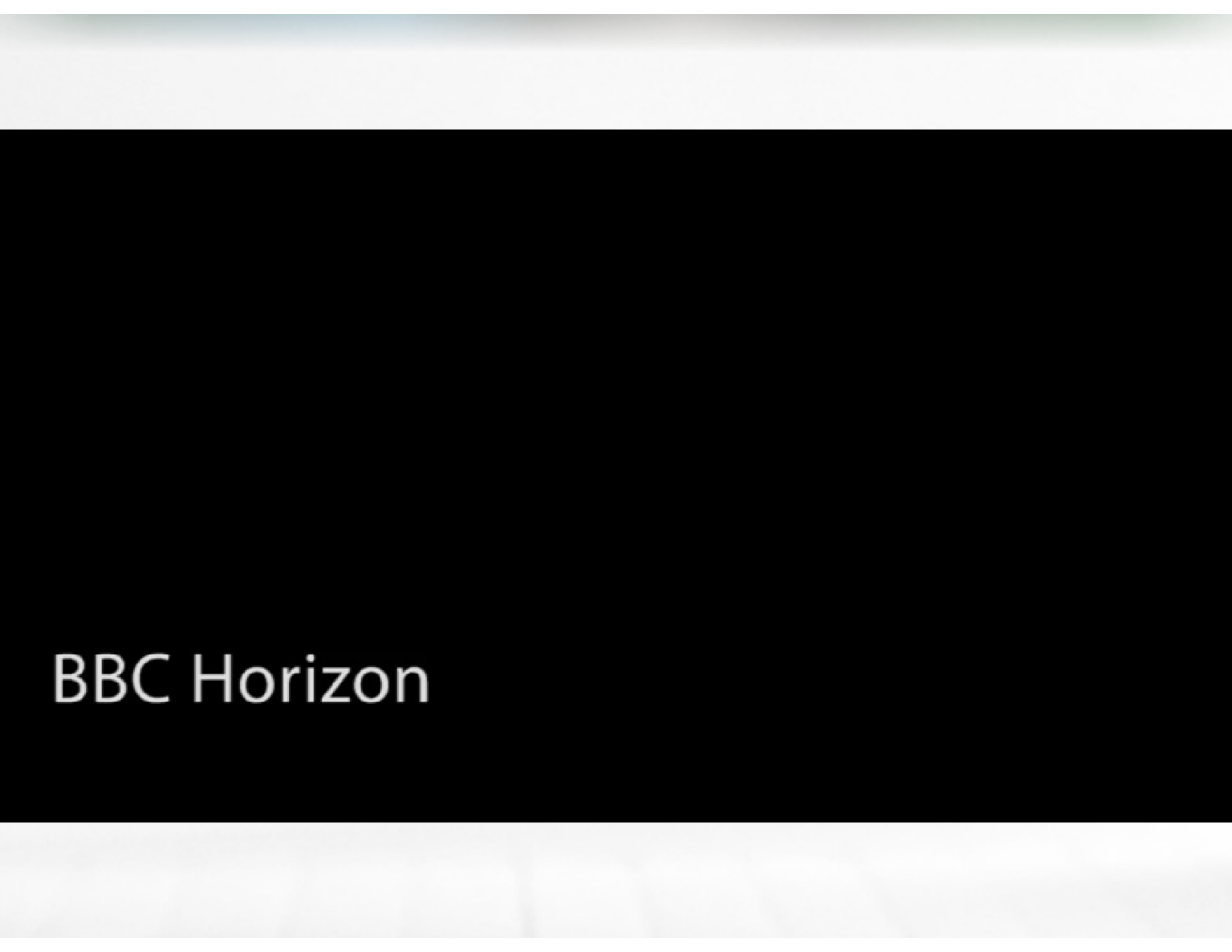
Who needs anonymity?

- 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?


BBC Horizon

Encryption doesn't work

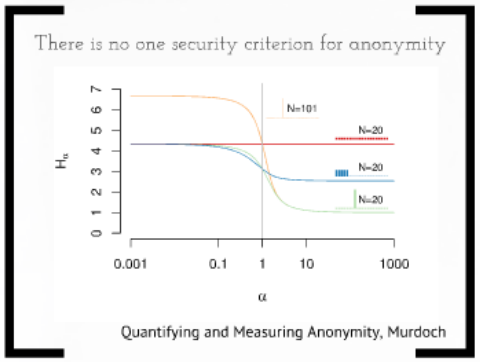
TLS, PGP, S/MIME only hide what is being said

- 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

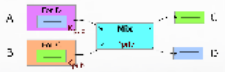
penet.fi (1993-1996)

- 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

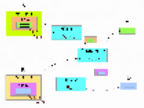


Type-1 (Cypherpunk)

- Mix decrypts messages
- Uses PGP
- CAST5 & ElGamal



Mixmaster (1998-)



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

Mixminion (2002-)

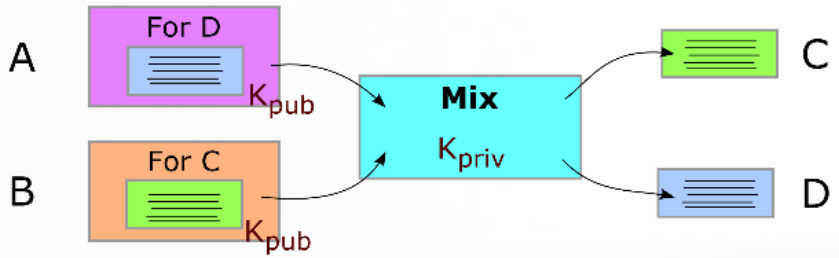
- Fixed many problems
- Introduced replies
- AES, SHA-1, RSA OEAP
- LIONESS wide-block cipher to resist tagging

penet.fi (1993-1996)

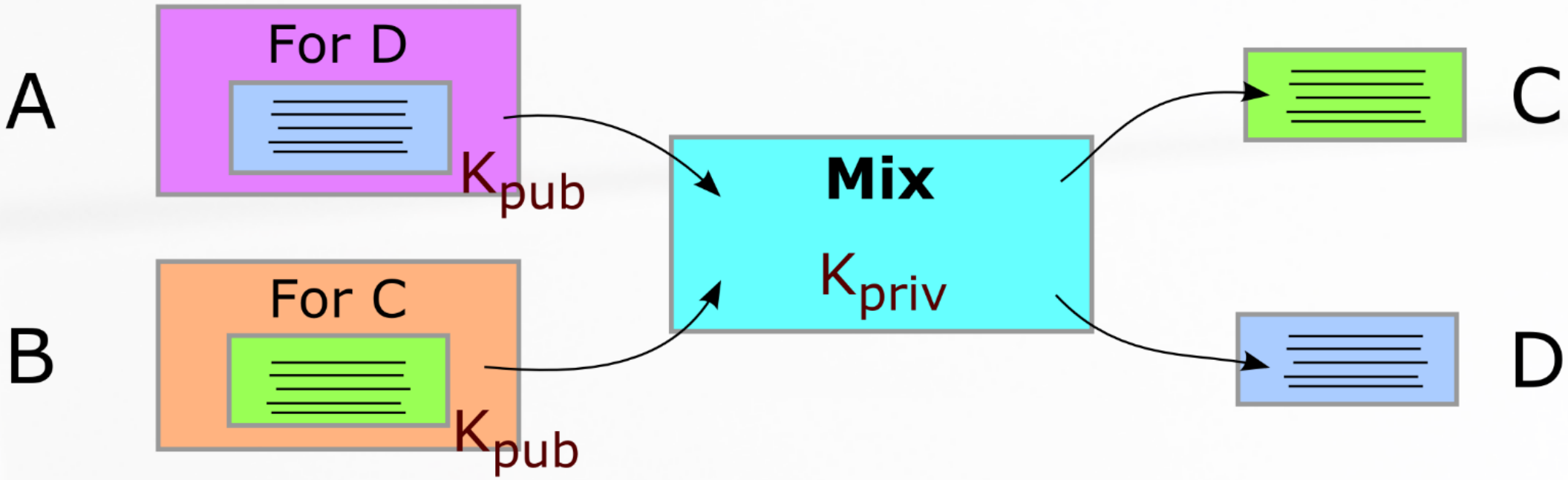
- Simply stripped headers off emails sent via remailer
- Allowed replies to be sent
- Easy to use, but single point of compromise
- Shut down following compromise by CoS

Type-1 (Cypherpunk)

- Mix decrypts messages
- Uses PGP
- CAST5 & ElGamal



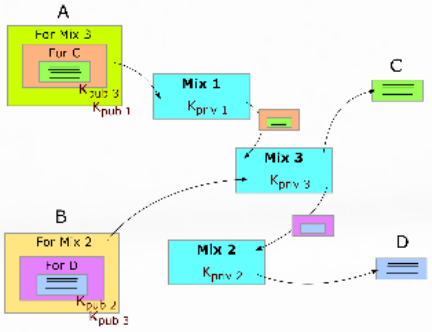
messages



Gamal

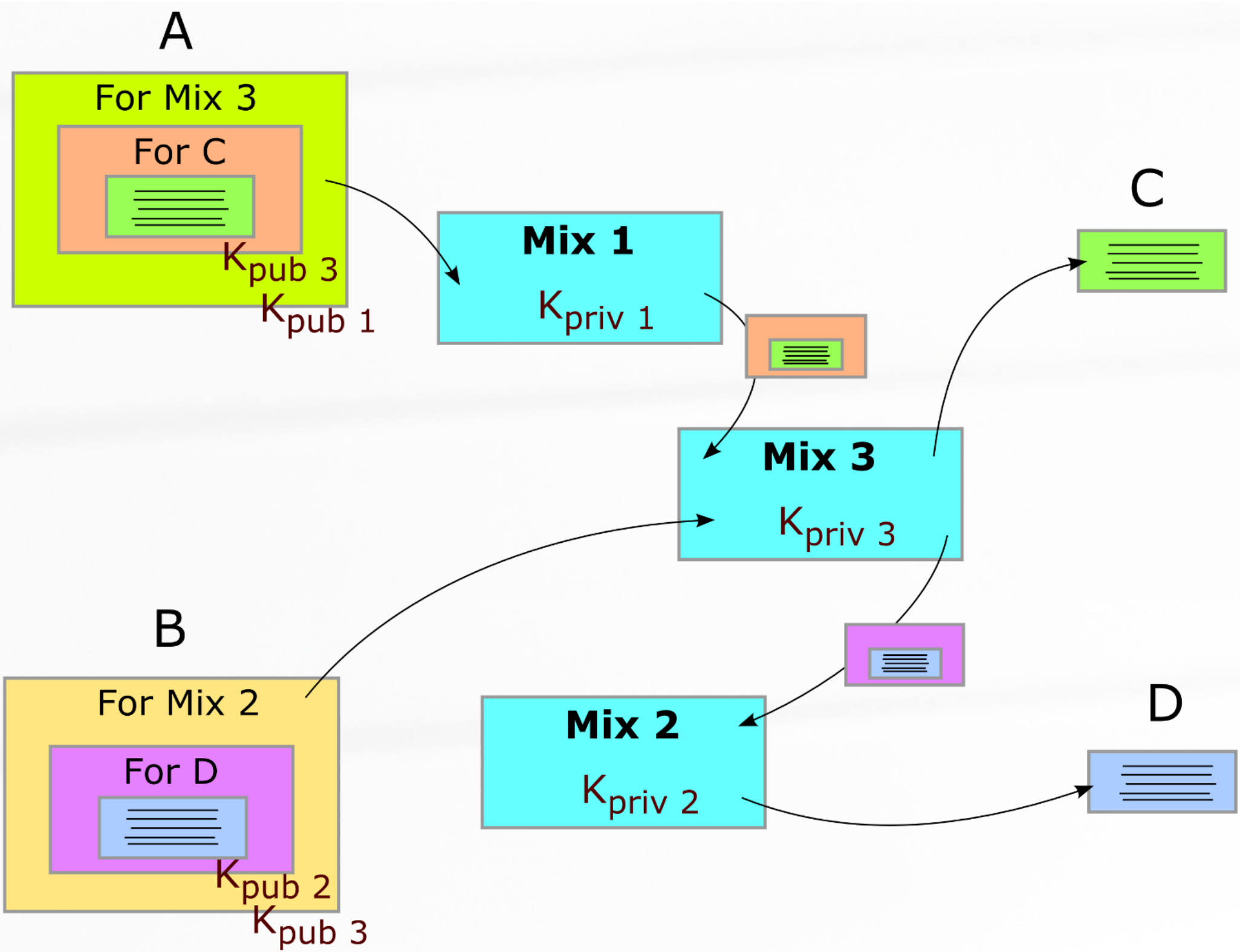
CAST5 & ElGamal

Mixmaster (1998-)



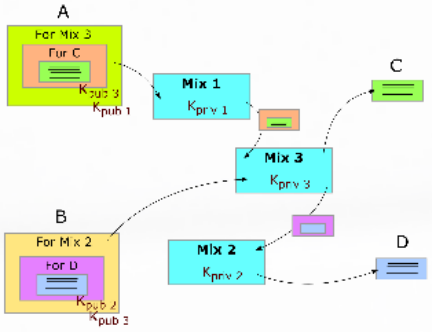
- Layered encryption
- Batching and re-ordering
- Based on Chaum Mix (1981)
- 3DES & RSA (PKCS #1 v1.5)

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

CAST5 & ElGamal

Mixmaster (1998-)



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

Mixminion (2002-)


Senders
Receivers
Mix

- 3DES & RSA (PKCS #1 v1.5

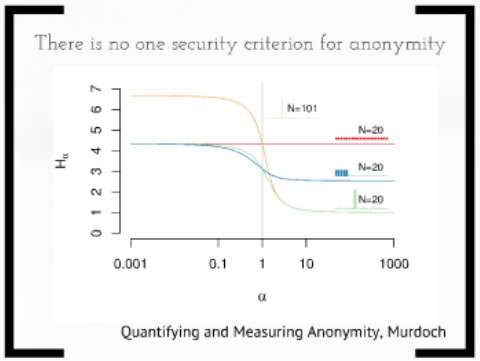
Mixminion (2002-)

- Fixed many problems
- Introduced replies
- AES, SHA-1, RSA OEAP
- LIONESS wide-block cipher to resist tagging

Remailers

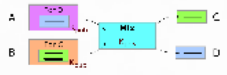
penet.fi (1993–1996)

- 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

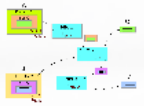


Type-1 (Cypherpunk)

- Mix decrypts messages
- Uses PGP
- CAST5 & ElGamal



Mixmaster (1998–)

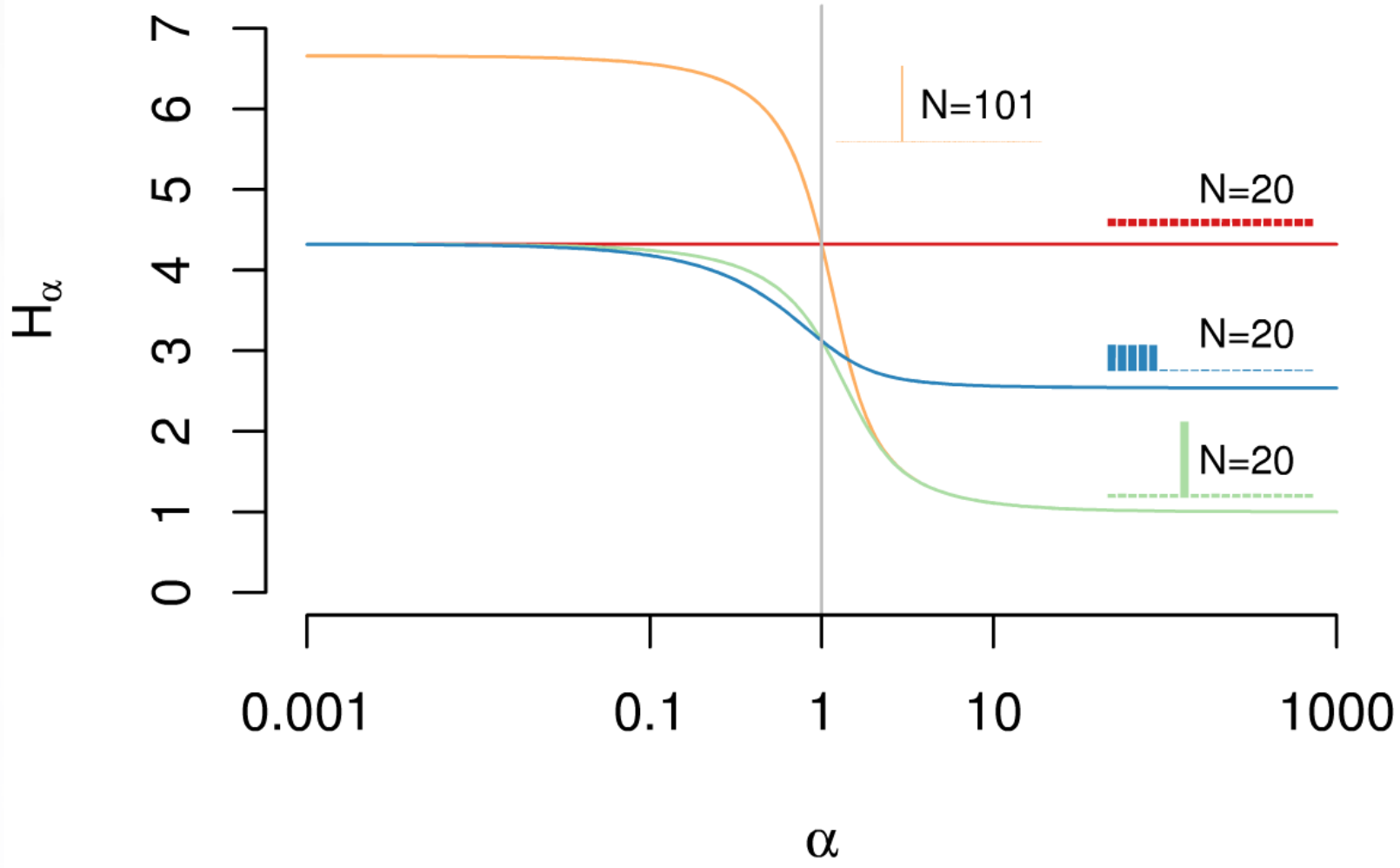


- Layered encryption
- Batching and re-ordering
- Based on Chaum Mix (1981)
- 3DES & RSA (PKCS #1 v1.5)

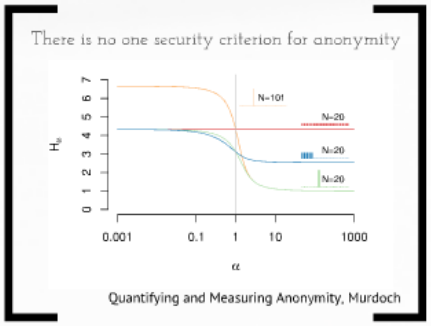
Mixminion (2002–)

- 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

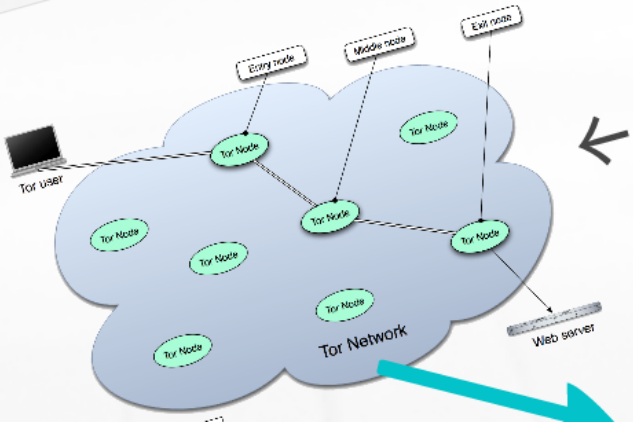


Quantifying and Measuring Anonymity, Murdoch



- Fixed many problems
- Introduced replies
- AES, SHA-1, RSA OEAP
- LIONESS wide-block cipher to resist tagging

Number of users ≈ 0



← 98%

The Web

rd to secure

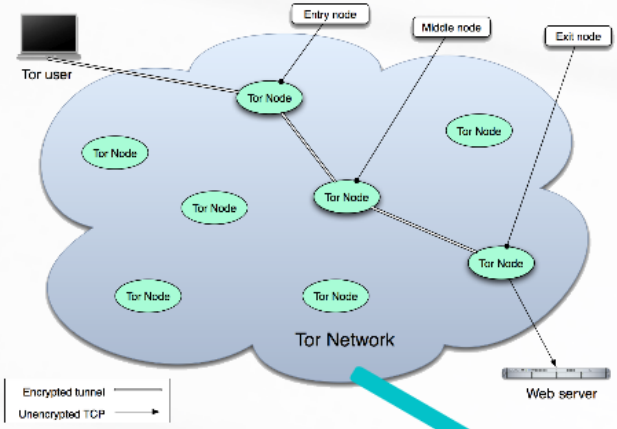
The Web

Web browsing is hard to secure

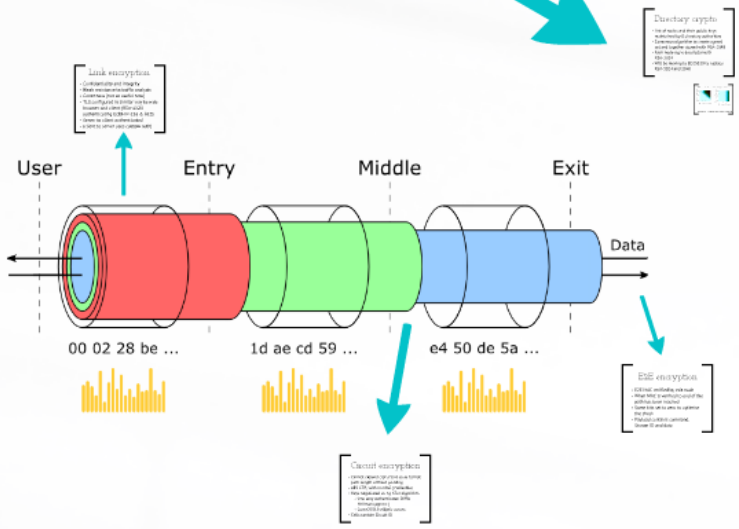
- Requires low latency
- High variability
- Low tolerance to padding

Equivalent systems

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



← 98%



The Web

Web browsing is hard to secure

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

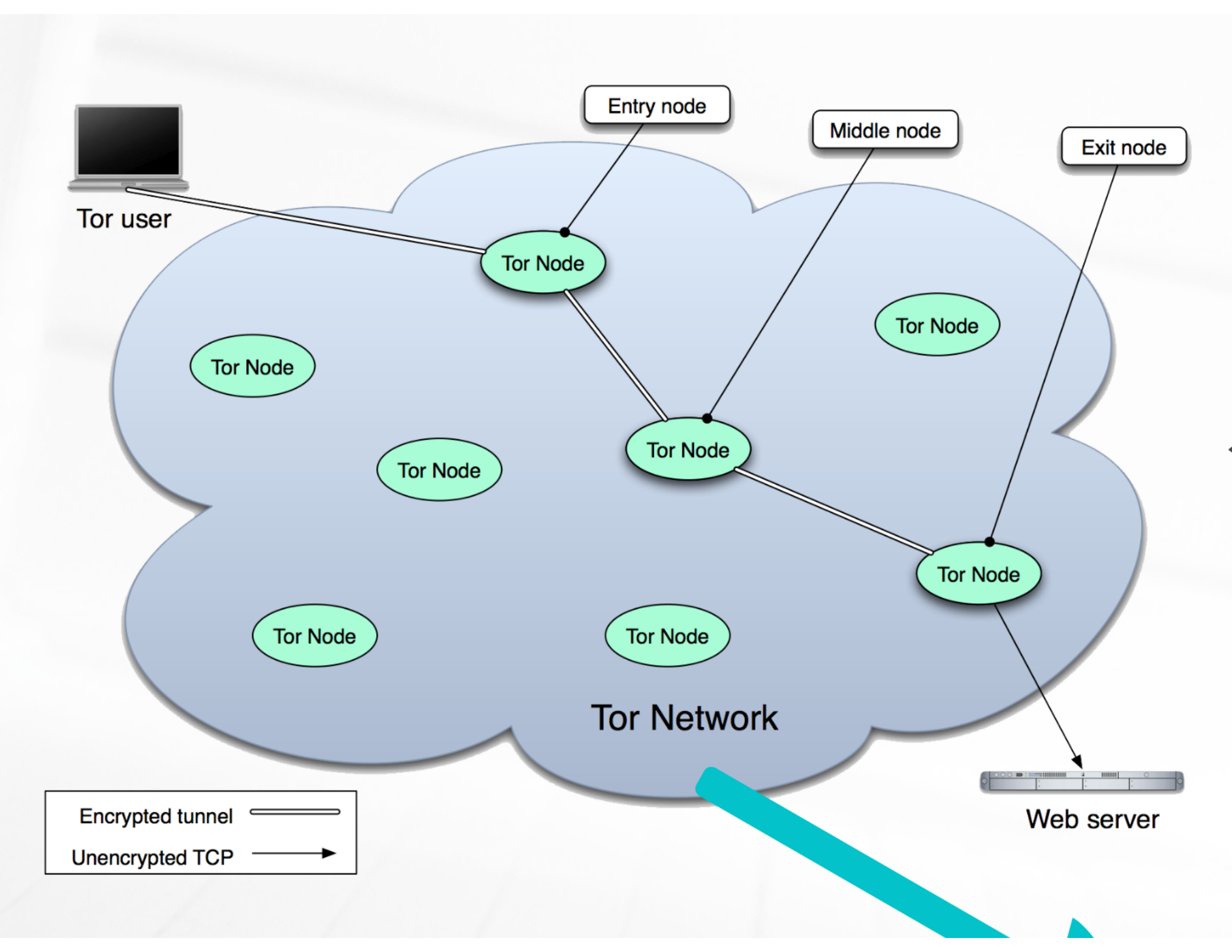
Equivalent systems

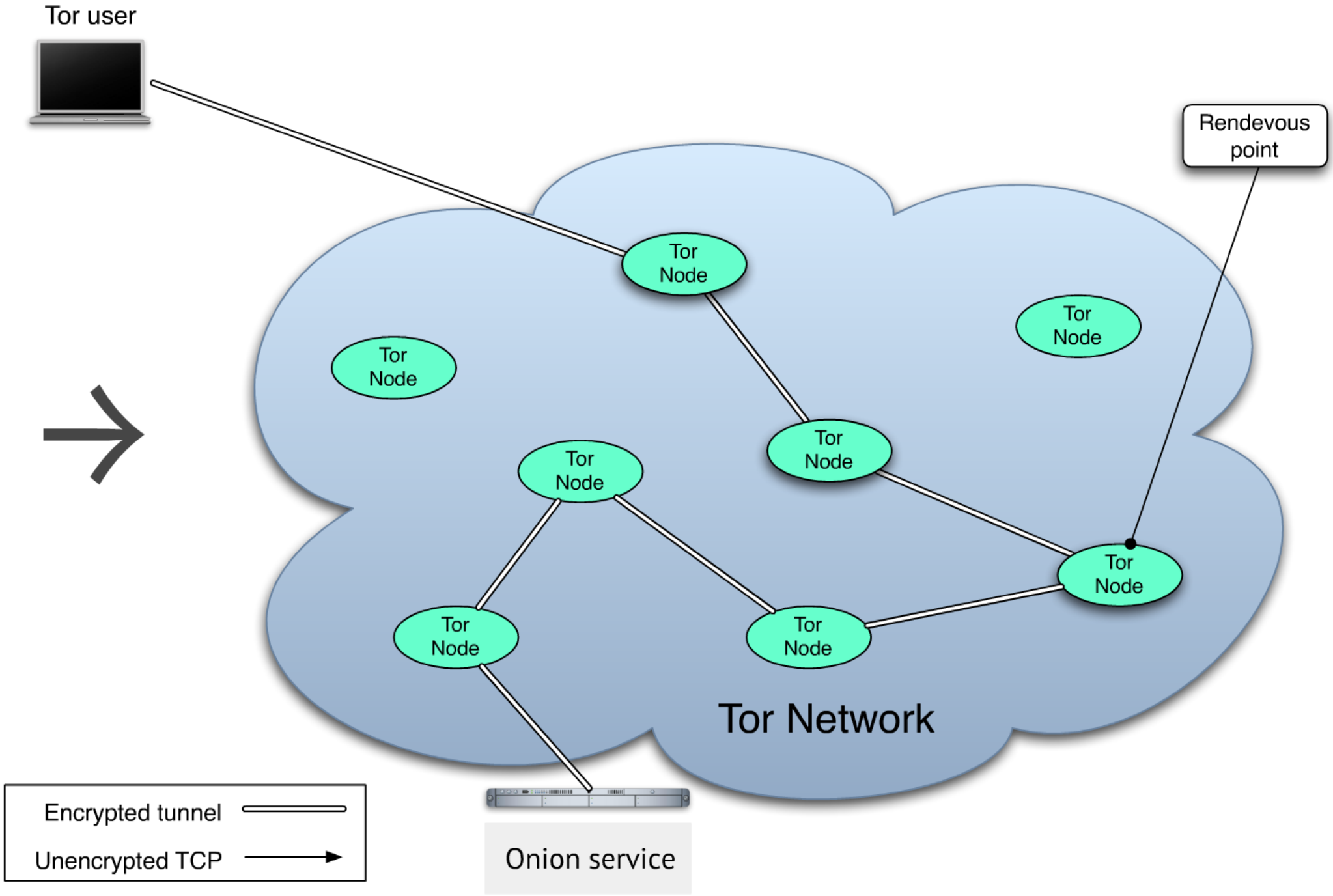
Equivalent systems

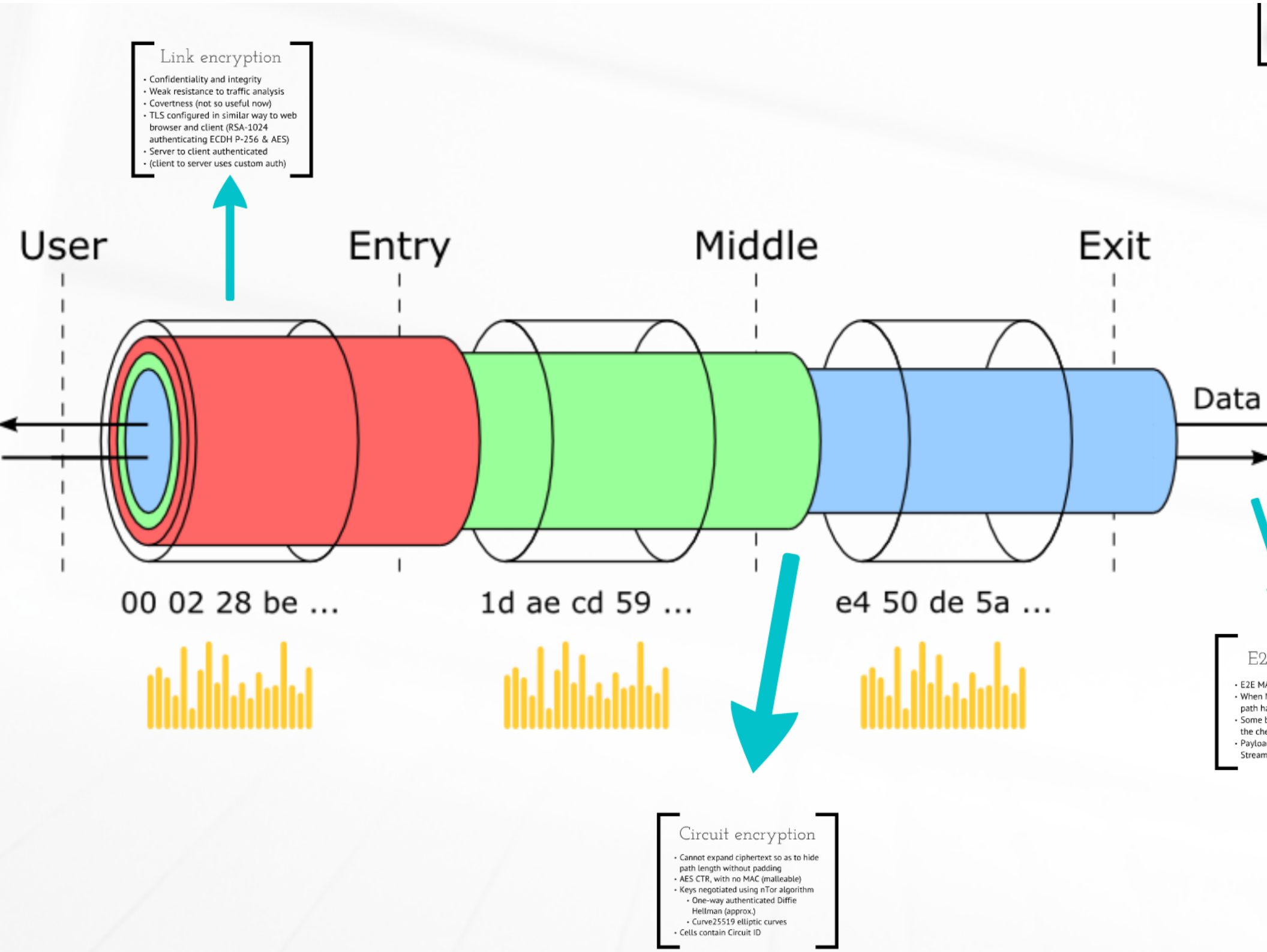
Open proxies ≈ penet.fi

VPN (IPSEC) ≈ Type-0

MixMinion ≈ Tor

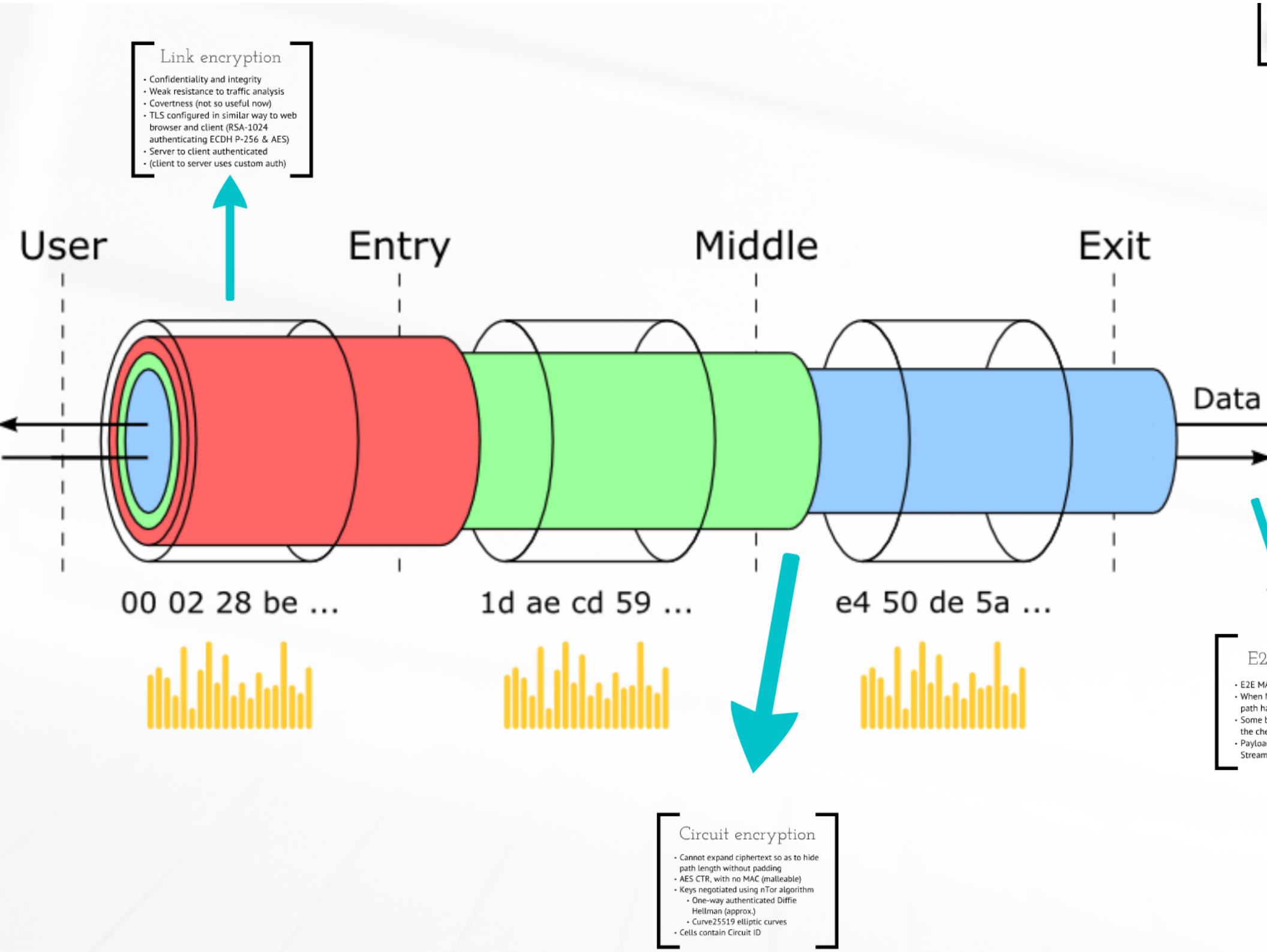

Entry node
Middle node
Exit node
Tor user
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Network
Web server
Encrypted tunnel
Unencrypted TCP


Tor user
Rendevous point
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Network
Encrypted tunnel
Unencrypted TCP
Onion service


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 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

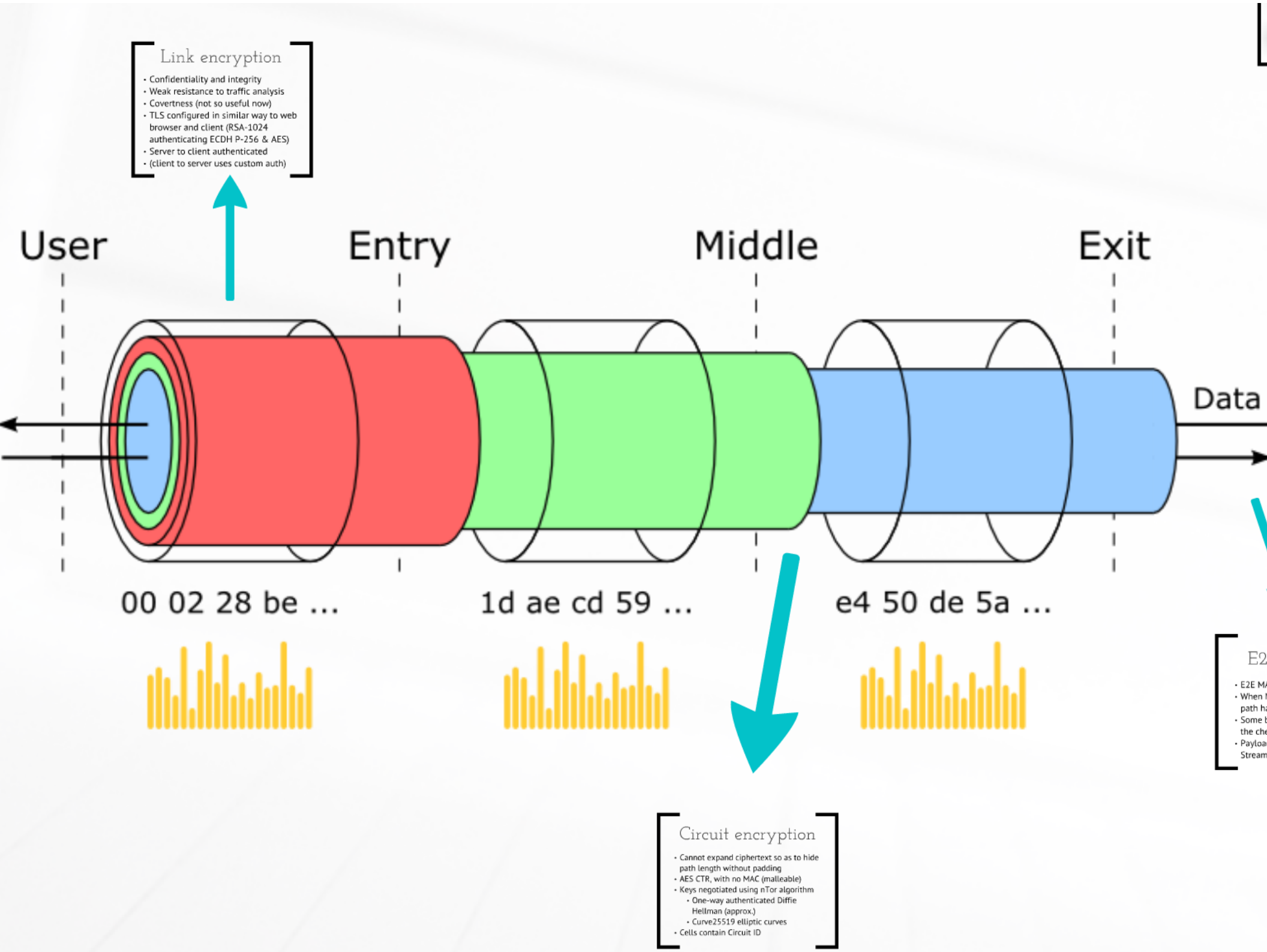
Link encryption

- 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)


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 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

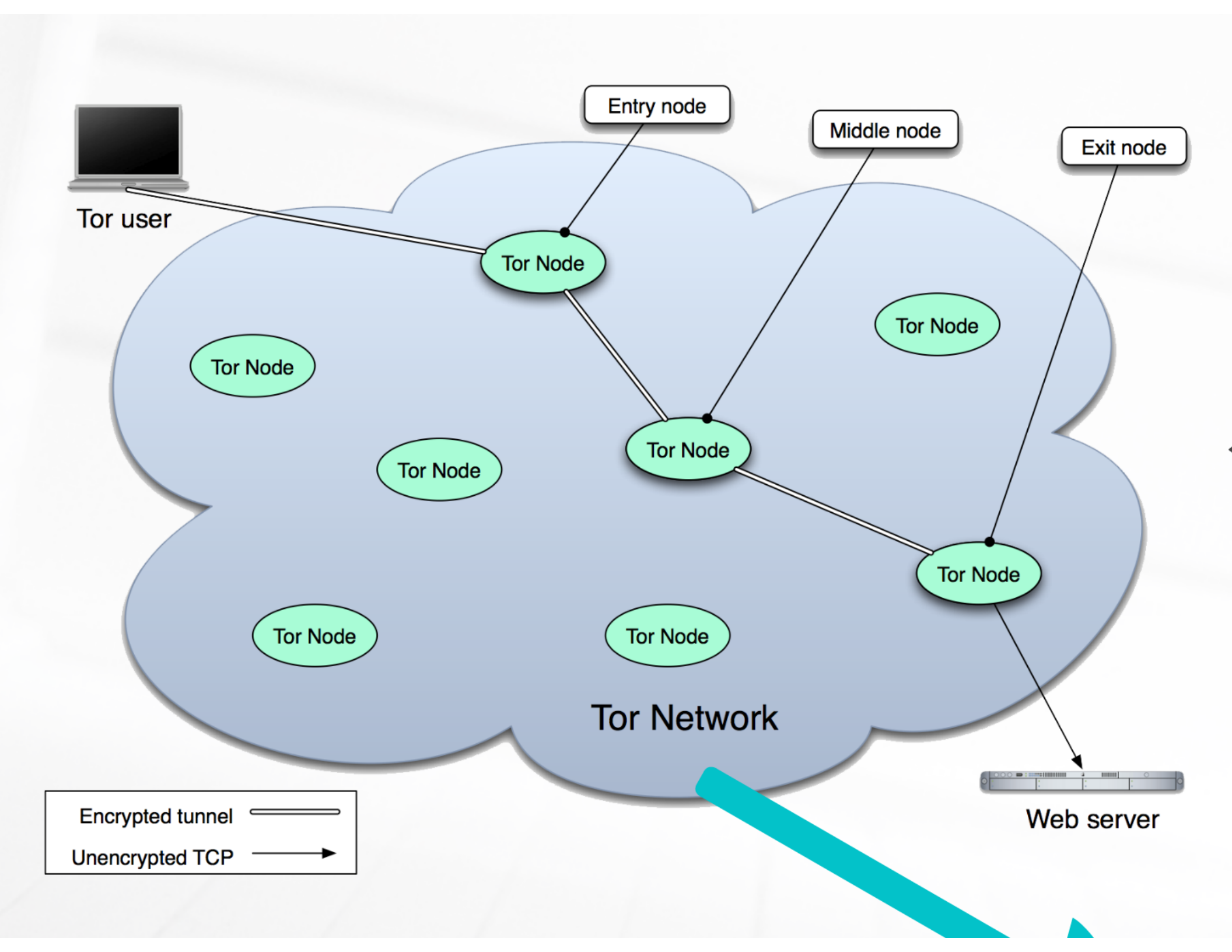
Circuit encryption

- 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 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

E2E encryption

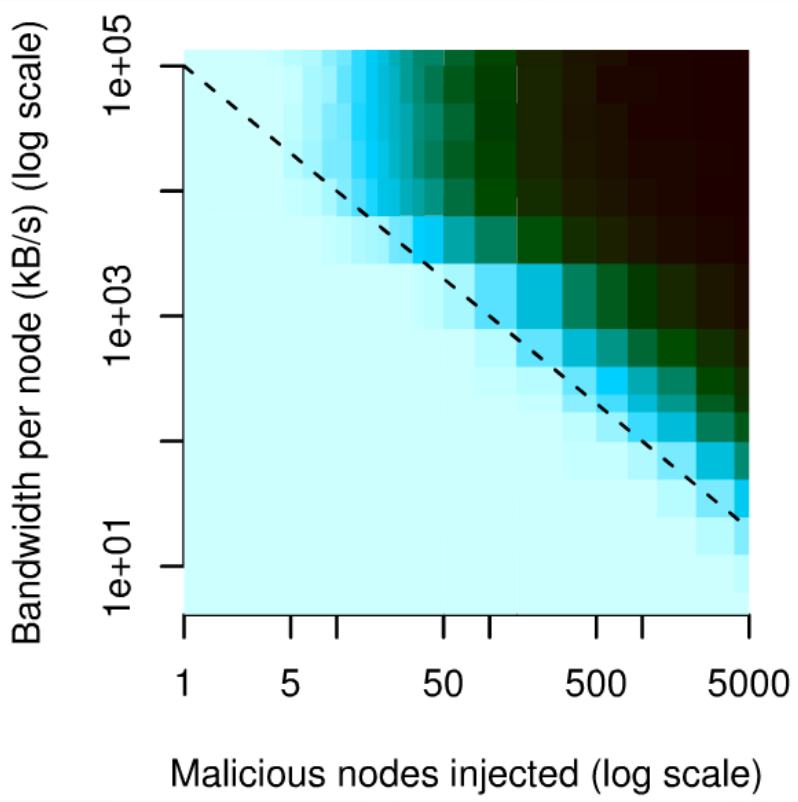
- E2E MAC verified by exit node
- When MAC is verified to end of the path has been reached
- Some bits set to zero to optimise the check
- Payload contains command, Stream ID and data

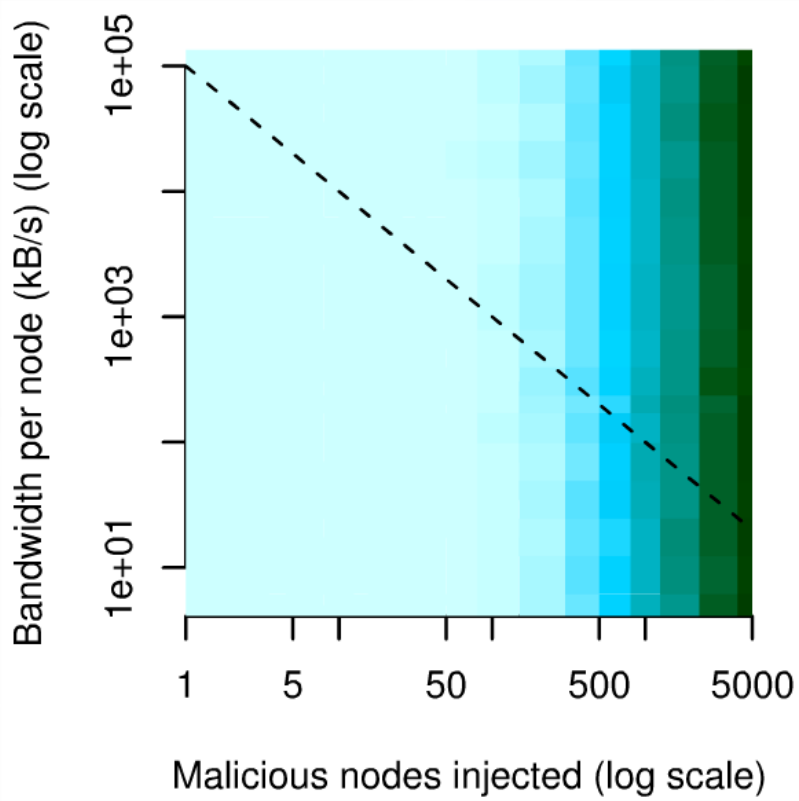

Entry node
Middle node
Exit node
Tor user
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Network
Web server
Encrypted tunnel
Unencrypted TCP

Directory crypto

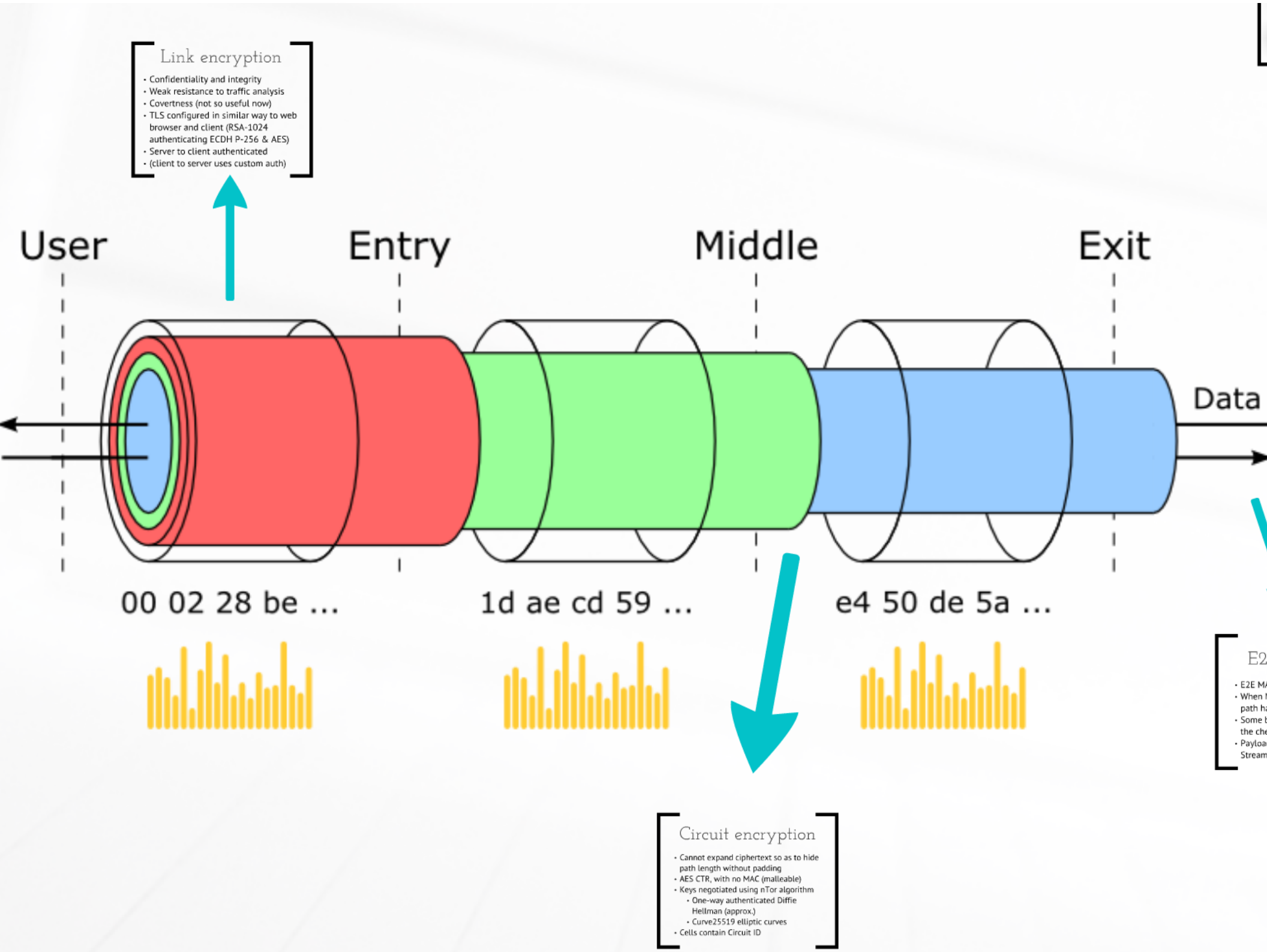
- List of nodes and their public keys maintained by 8 directory authorities
- Consensus algorithm to create agreed set and together signed with RSA-2048
- Each node signs descriptor with RSA-1024
- Will be moving to ED25519 to replace RSA-1024 and 2048

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
• 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 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

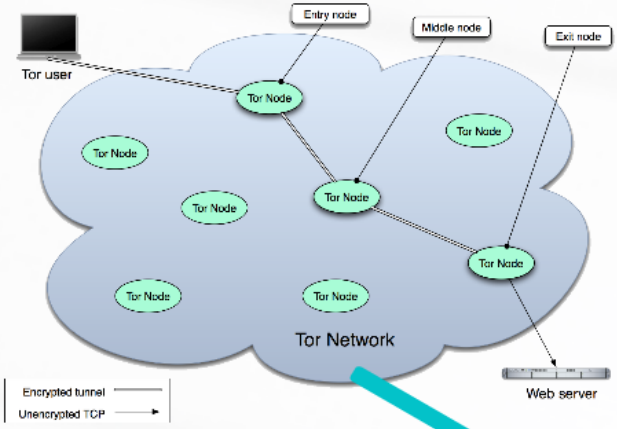
The Web

Web browsing is hard to secure

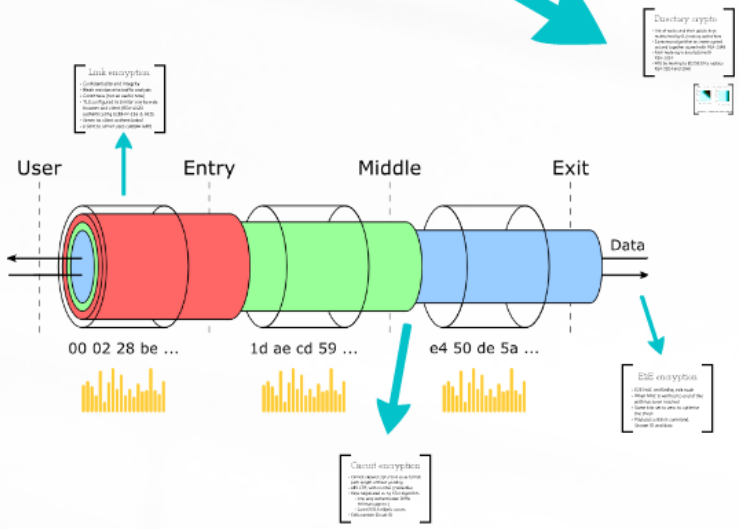
- Requires low latency
- High variability
- Low tolerance to padding

Equivalent systems

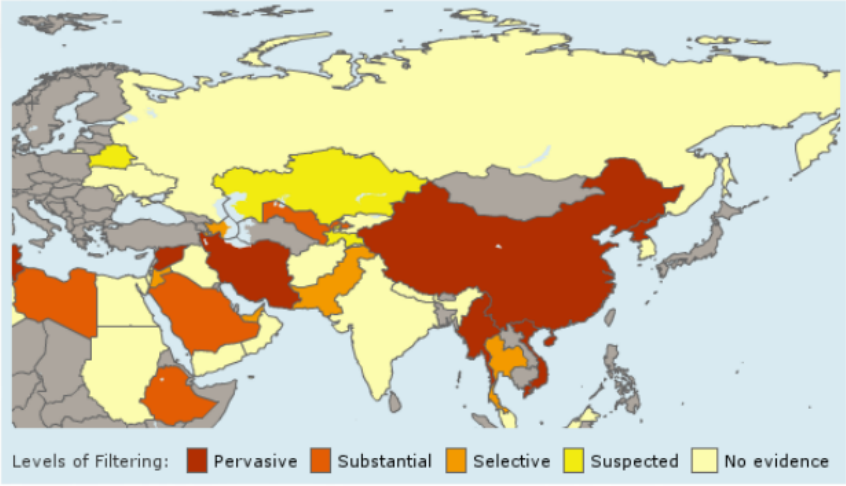
Open proxies ≈ penet.fi
VPN (IPSEC) ≈ Type-0
MixMinion ≈ Tor

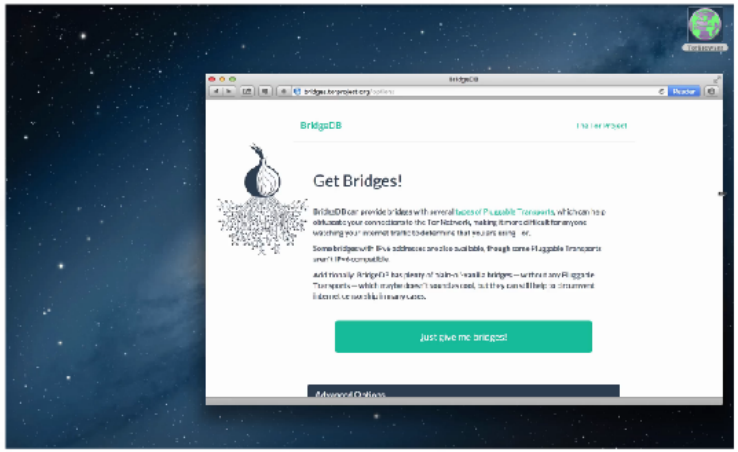


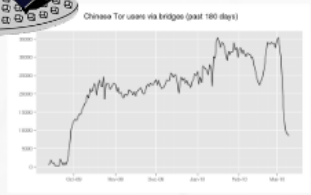
← 98%

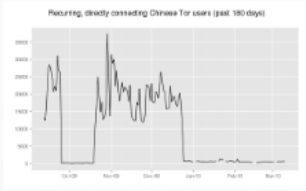


Censorship resistance

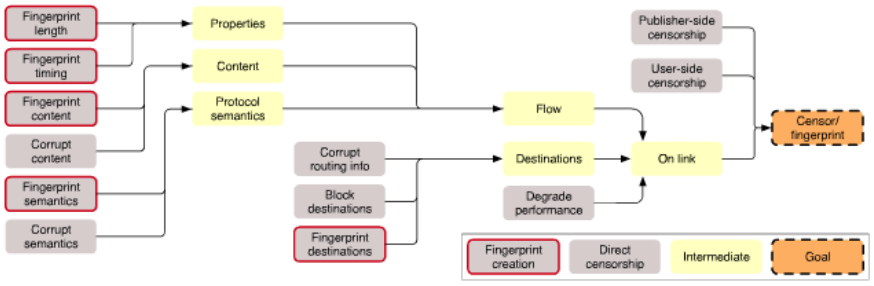




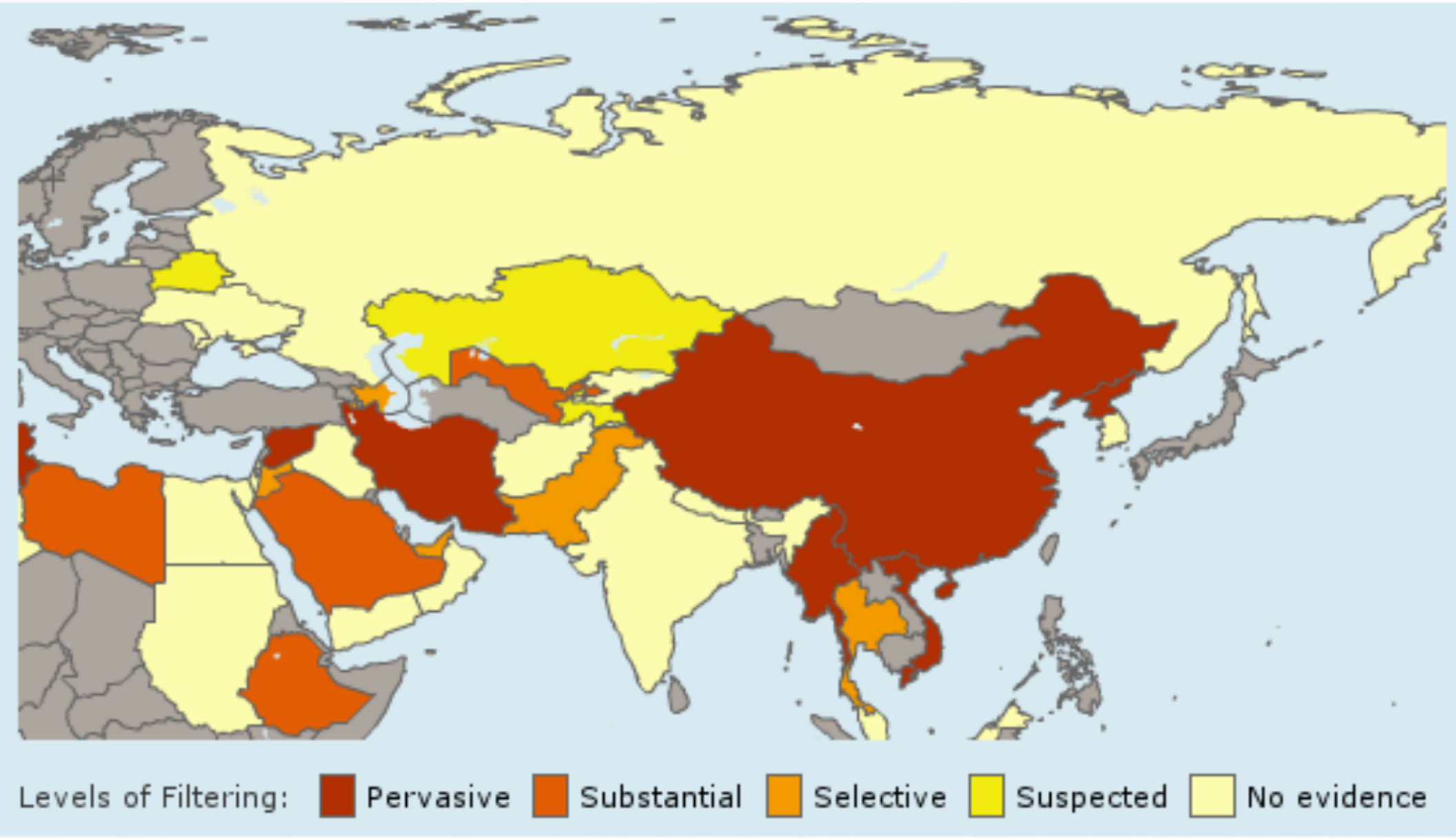




Fingerprinting and developing blocking rules

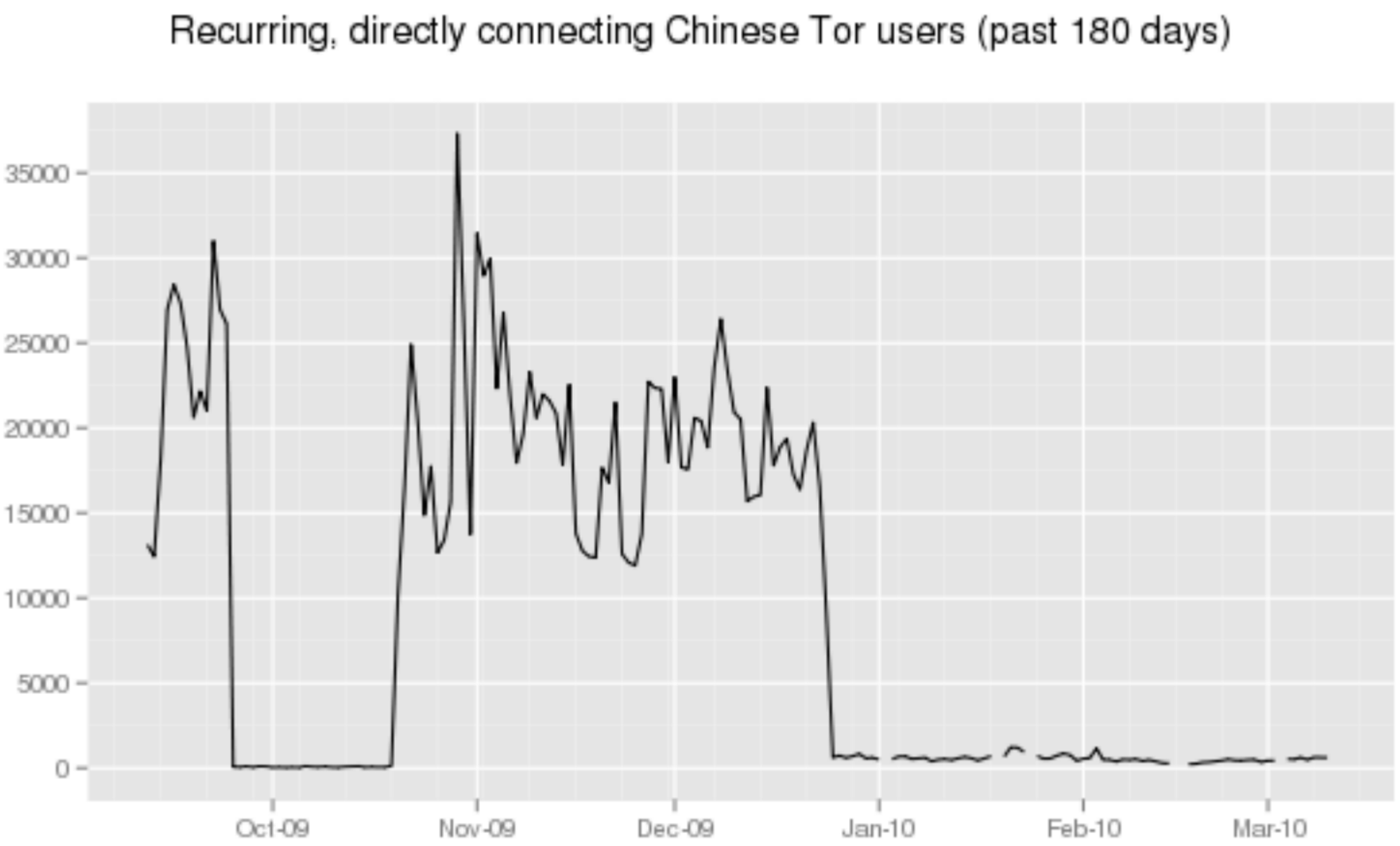


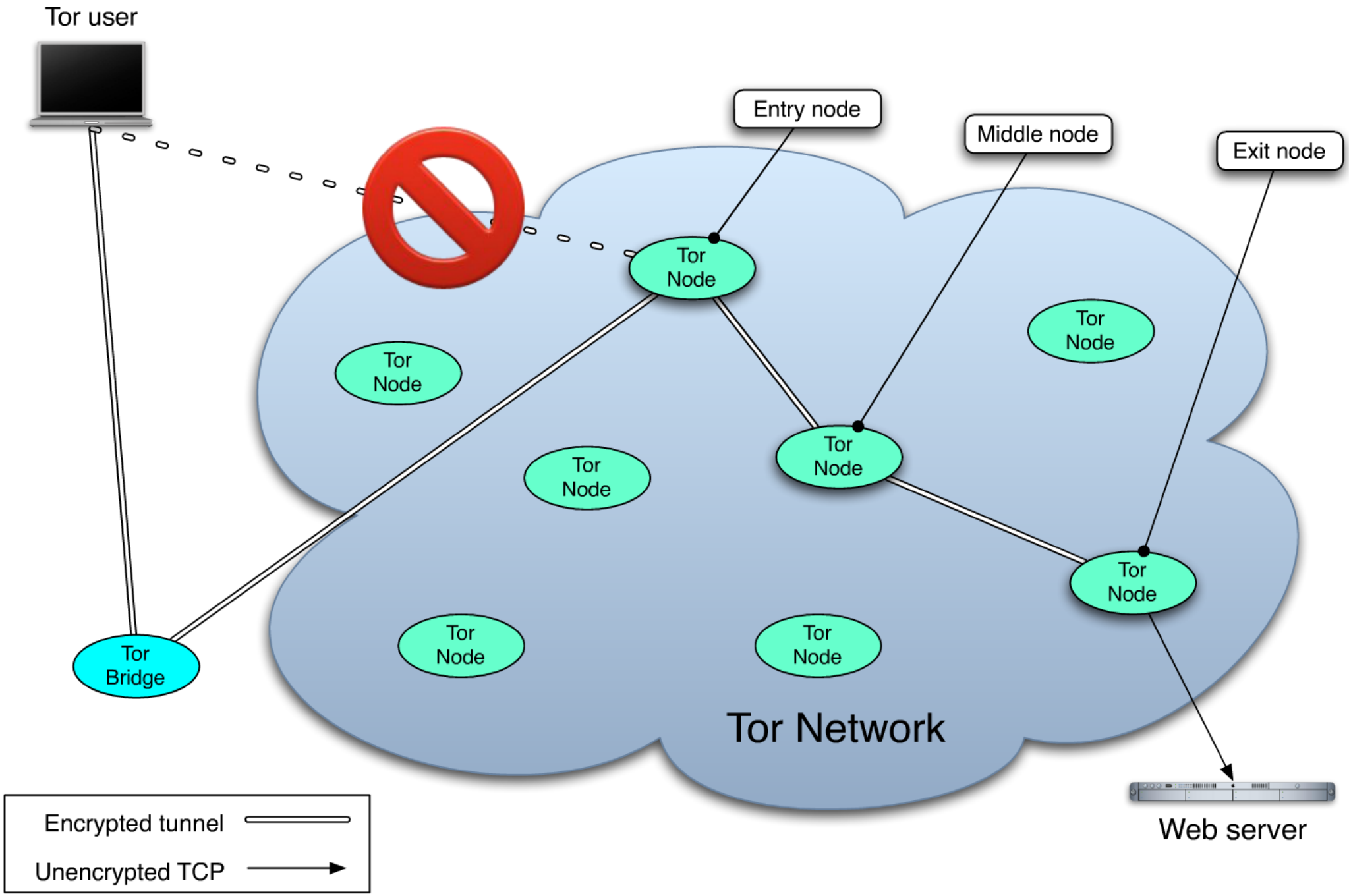
SoK: Making Sense of Censorship Resistance Systems, Khattak et al.

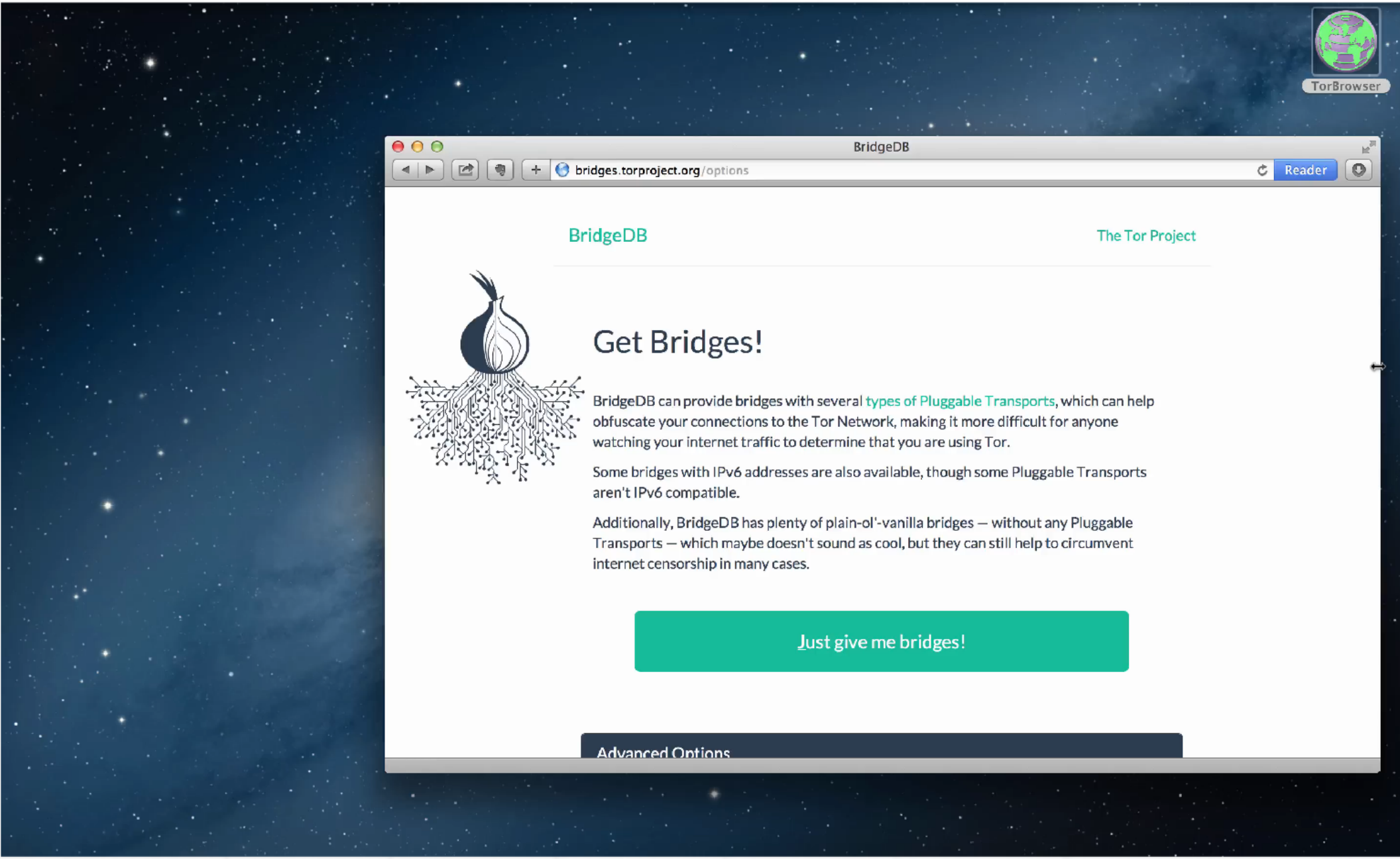

Levels of Filtering:
Pervasive
Substantial
Selective
Suspected
No evidence

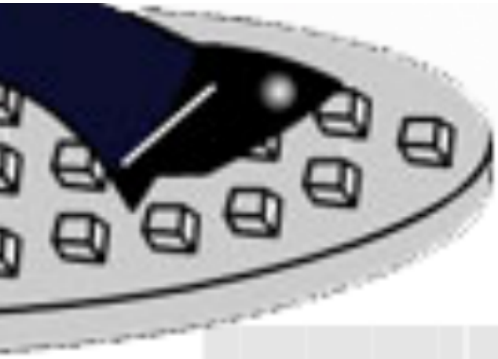
Levels of Filtering: Pervasive Substantia

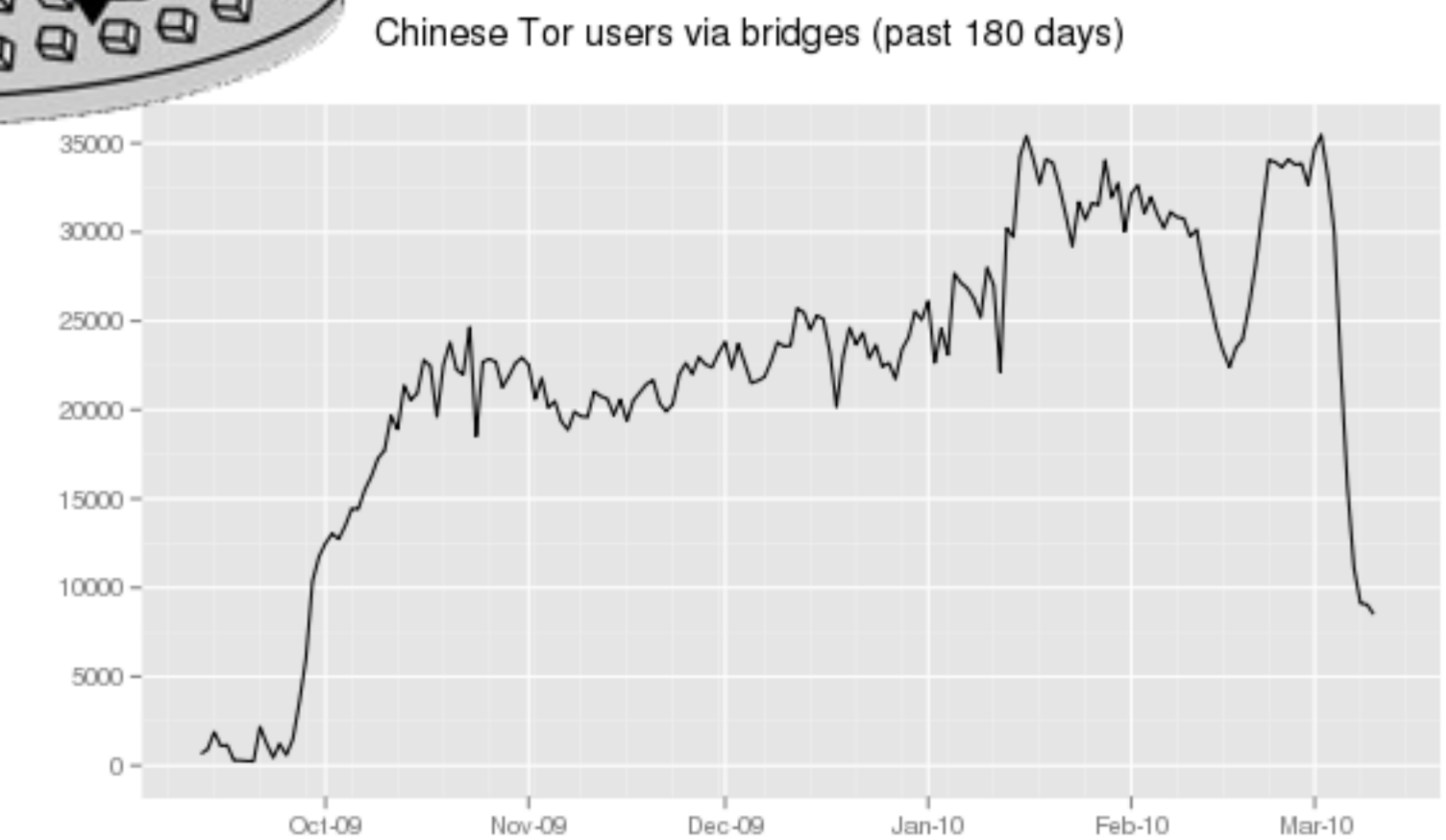
Chin


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

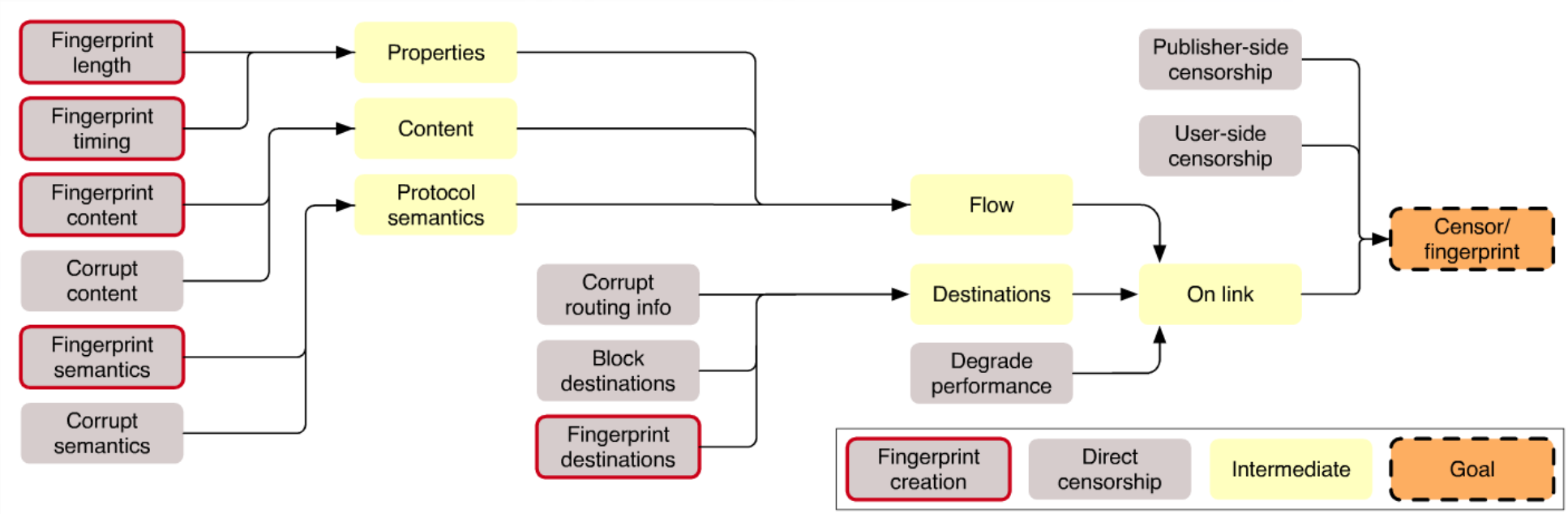

Tor user
Entry node
Middle node
Exit node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Bridge
Tor Network
Web server
Encrypted tunnel
Unencrypted TCP


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



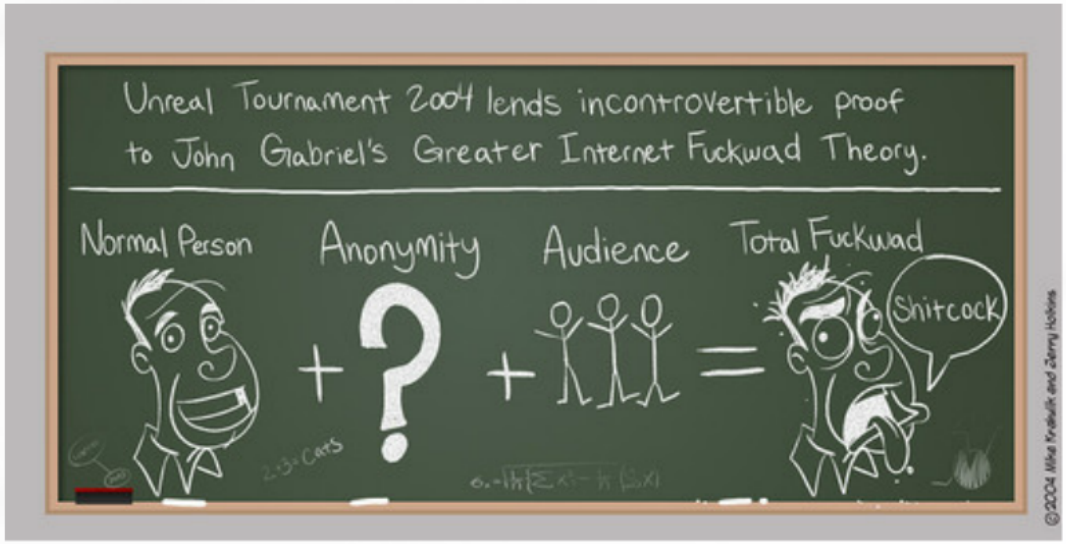

Chinese Tor users via bridges (past 180 days)
35000
30000
25000
20000
15000
10000
5000
0
Oct-09
Nov-09
Dec-09
Jan-10
Feb-10
Mar-10

Fingerprinting and developing blocking rules

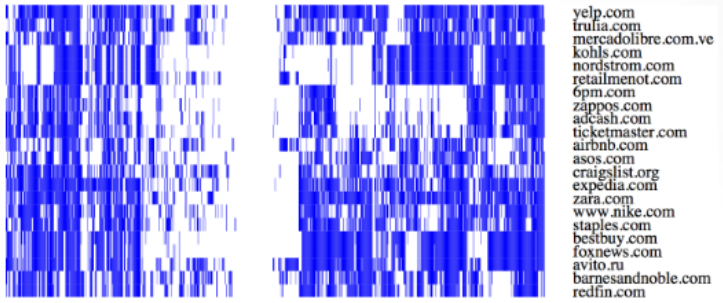


SoK: Making Sense of Censorship Resistance Systems, Khattak et al.

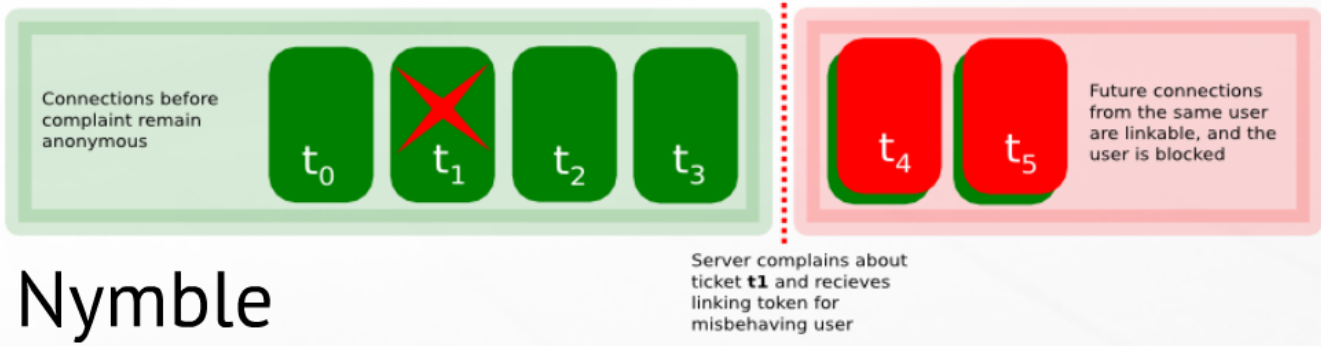
Abuse



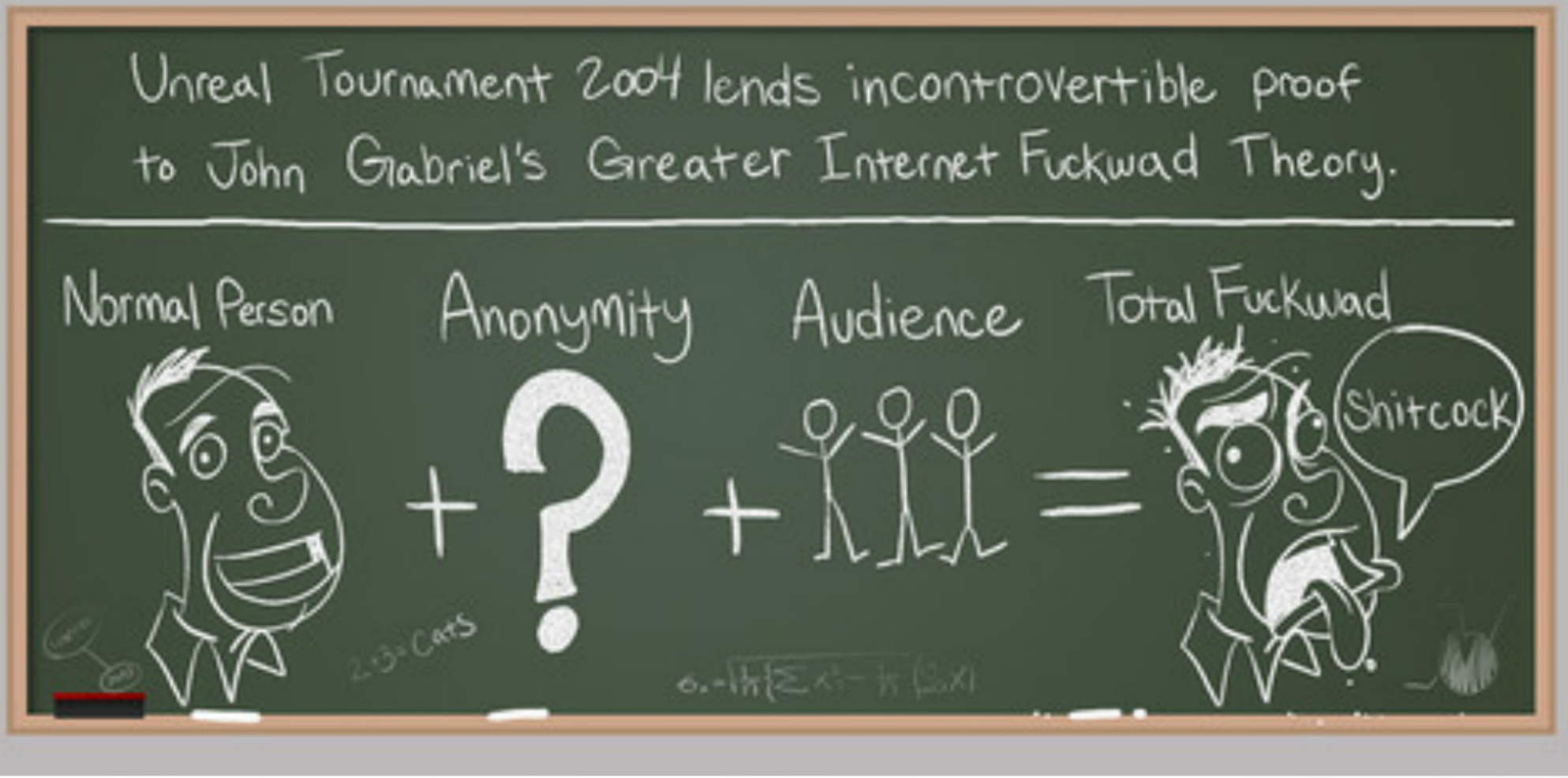
3.67% of the most popular 1,000 websites block Tor



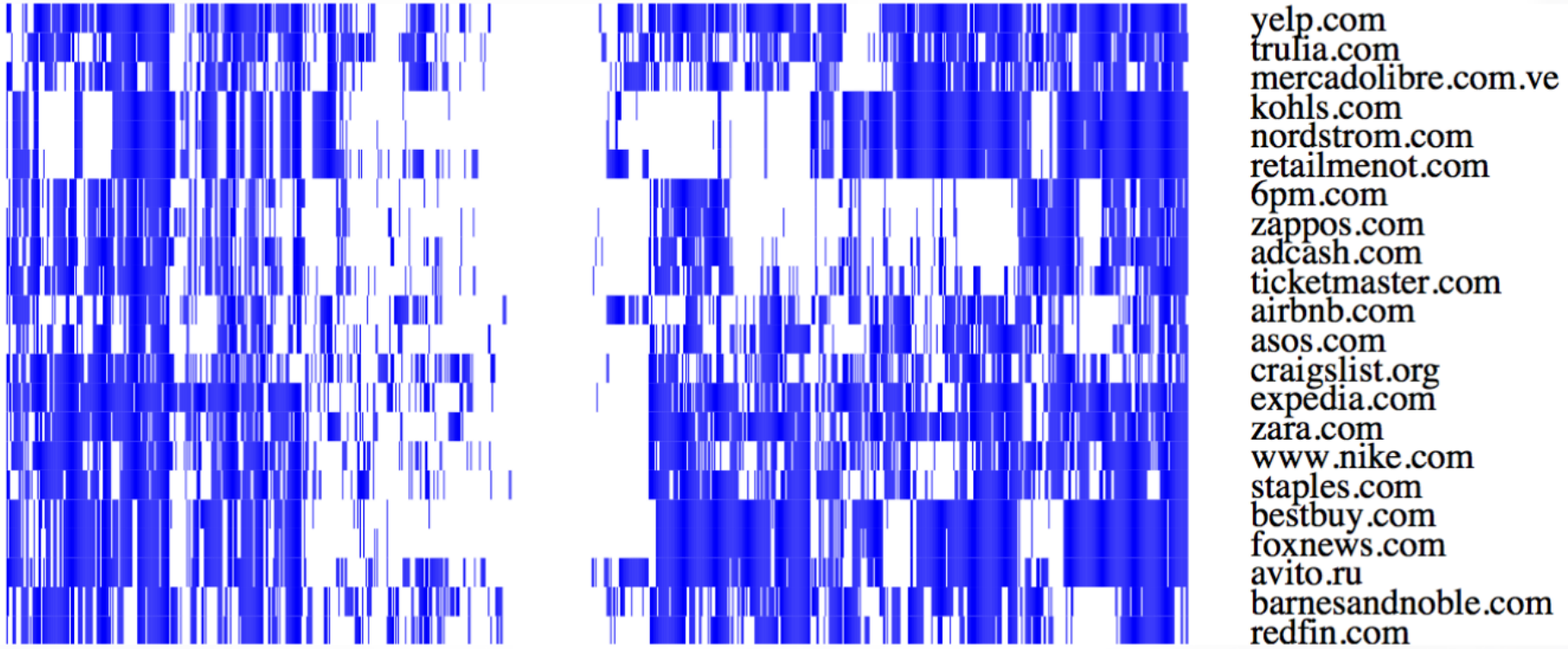
Do You See What I See? Differential Treatment of Anonymous Users, Khattak et al.



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

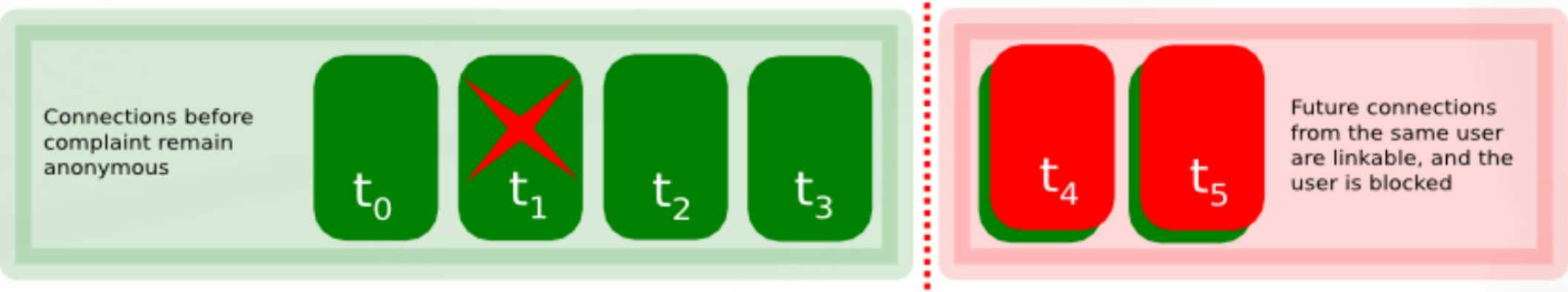
3.67% of the most popular 1,000 websites block Tor



Do You See What I See? Differential Treatment of Anonymous Users, Khattak et al.

foxnews.com
avito.ru
barnesandnoble.com
redfin.com

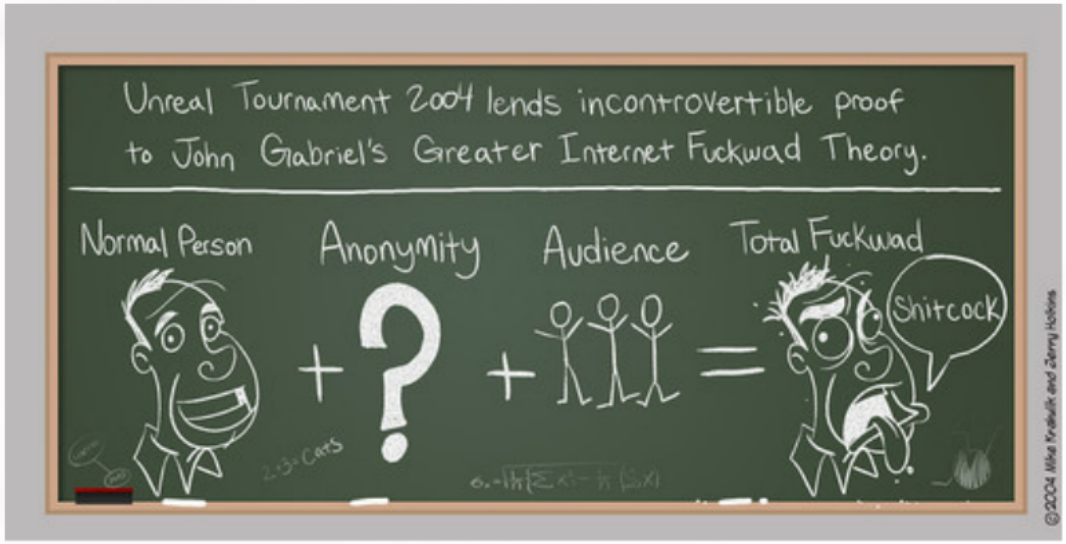
Do You See What I See? Differential Treatment of Anonymous Users, Khattak et al.



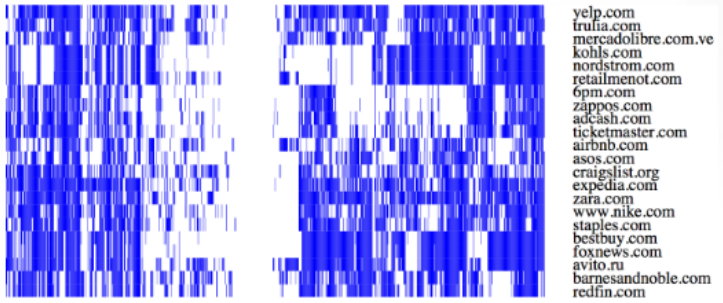
Server complains about ticket **t1** and recieves linking token for misbehaving user

Nymble

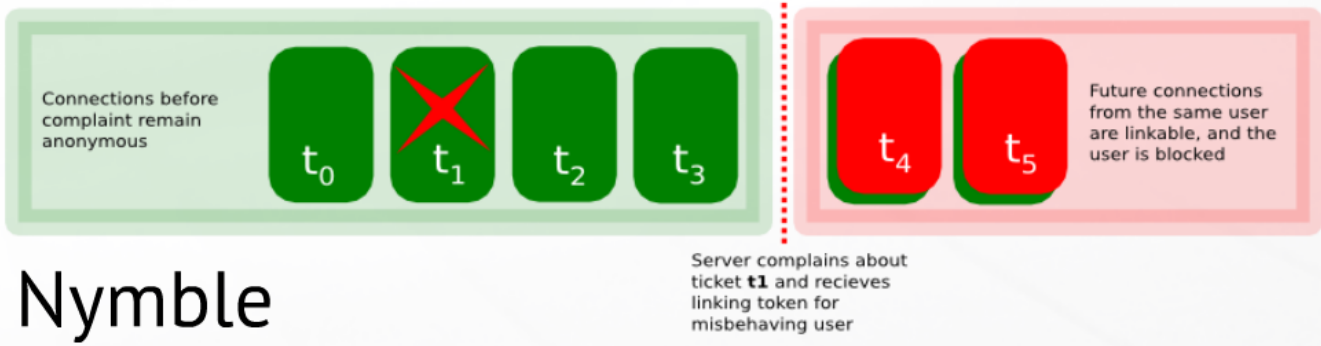
Abuse



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

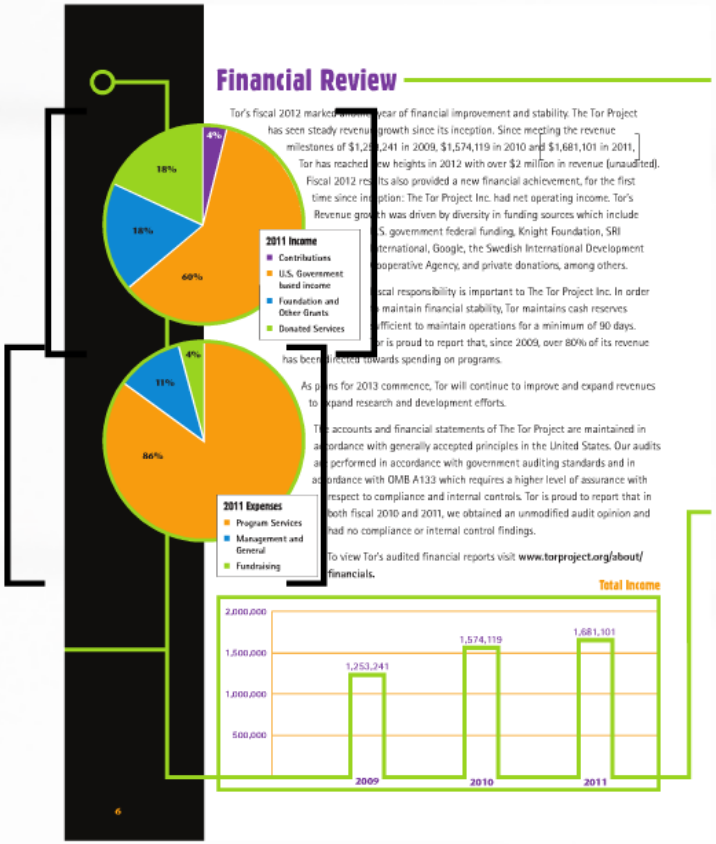


Do You See What I See? Differential Treatment of Anonymous Users, Khattak et al.



Nymble

Sustainability

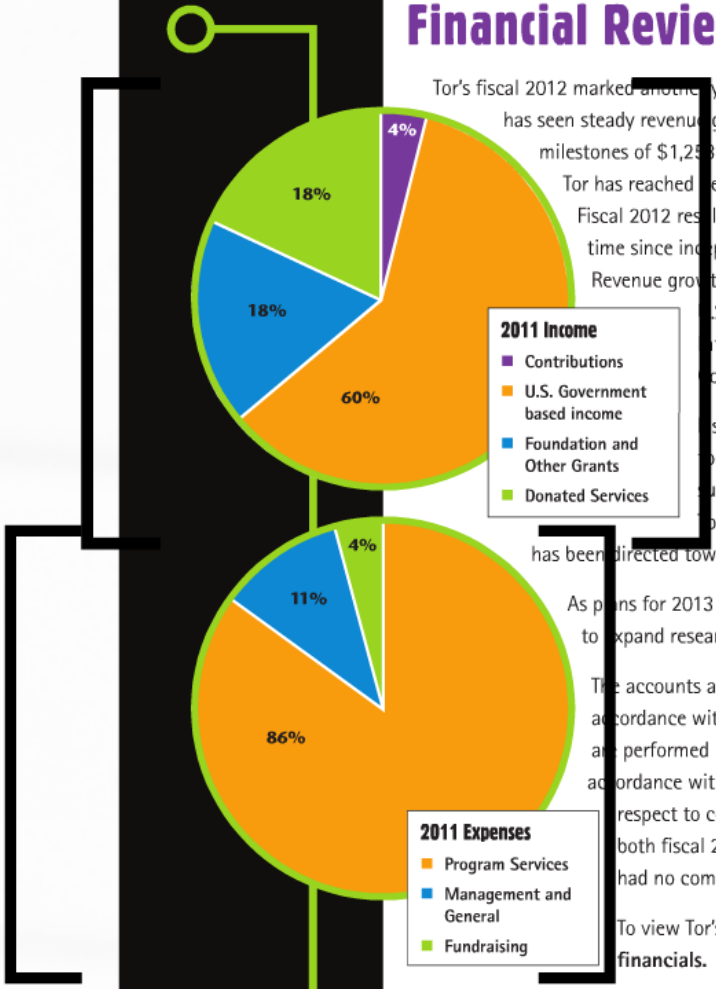


Incentives

- 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

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.

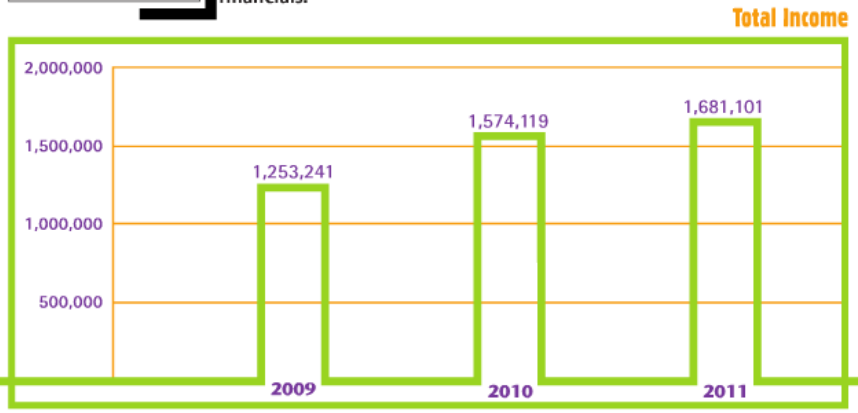


Fiscal responsibility is important to The Tor Project Inc. In order to maintain financial stability, Tor maintains cash reserves sufficient to maintain operations for a minimum of 90 days. Tor is proud to report that, since 2009, over 80% of its revenue has been directed towards spending on programs.

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

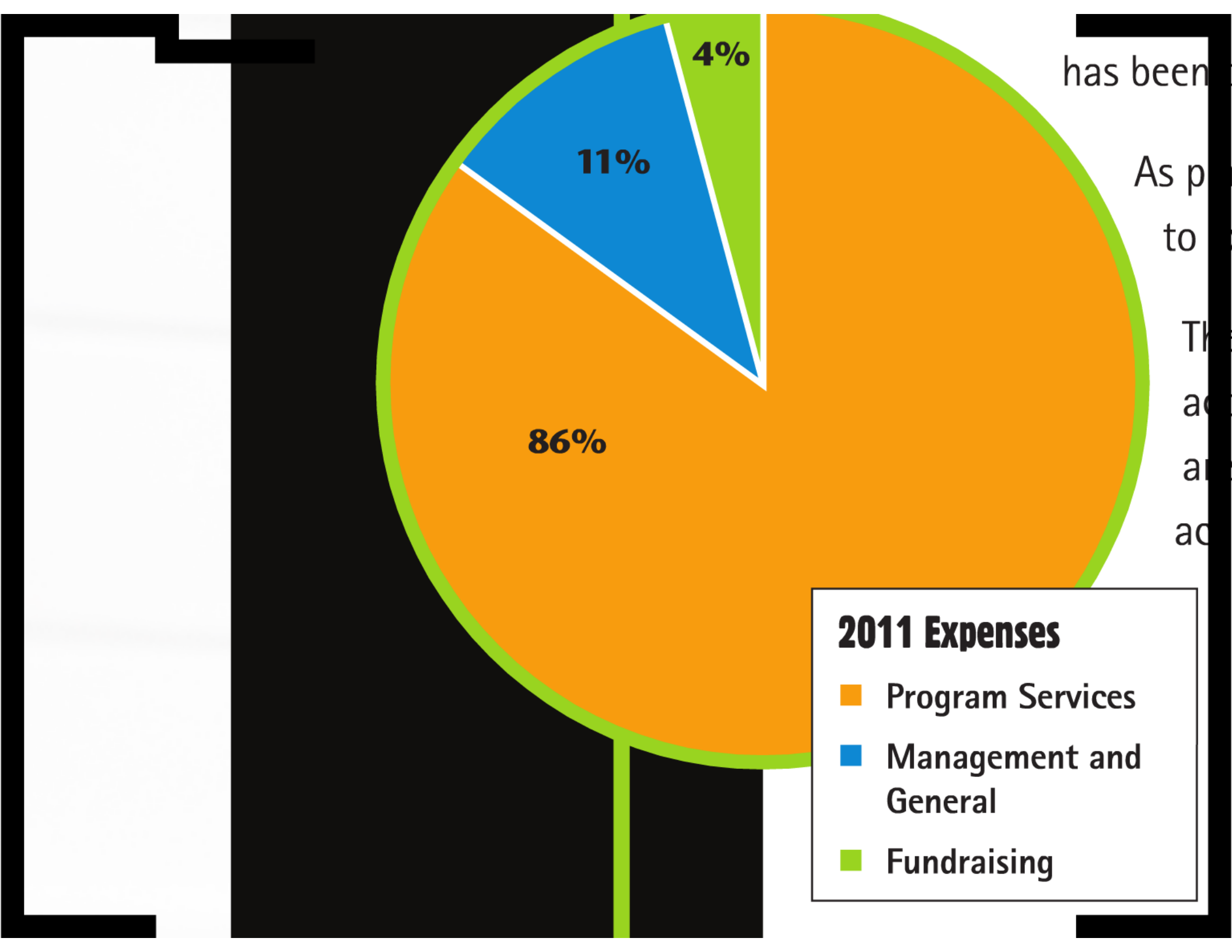
to

Th

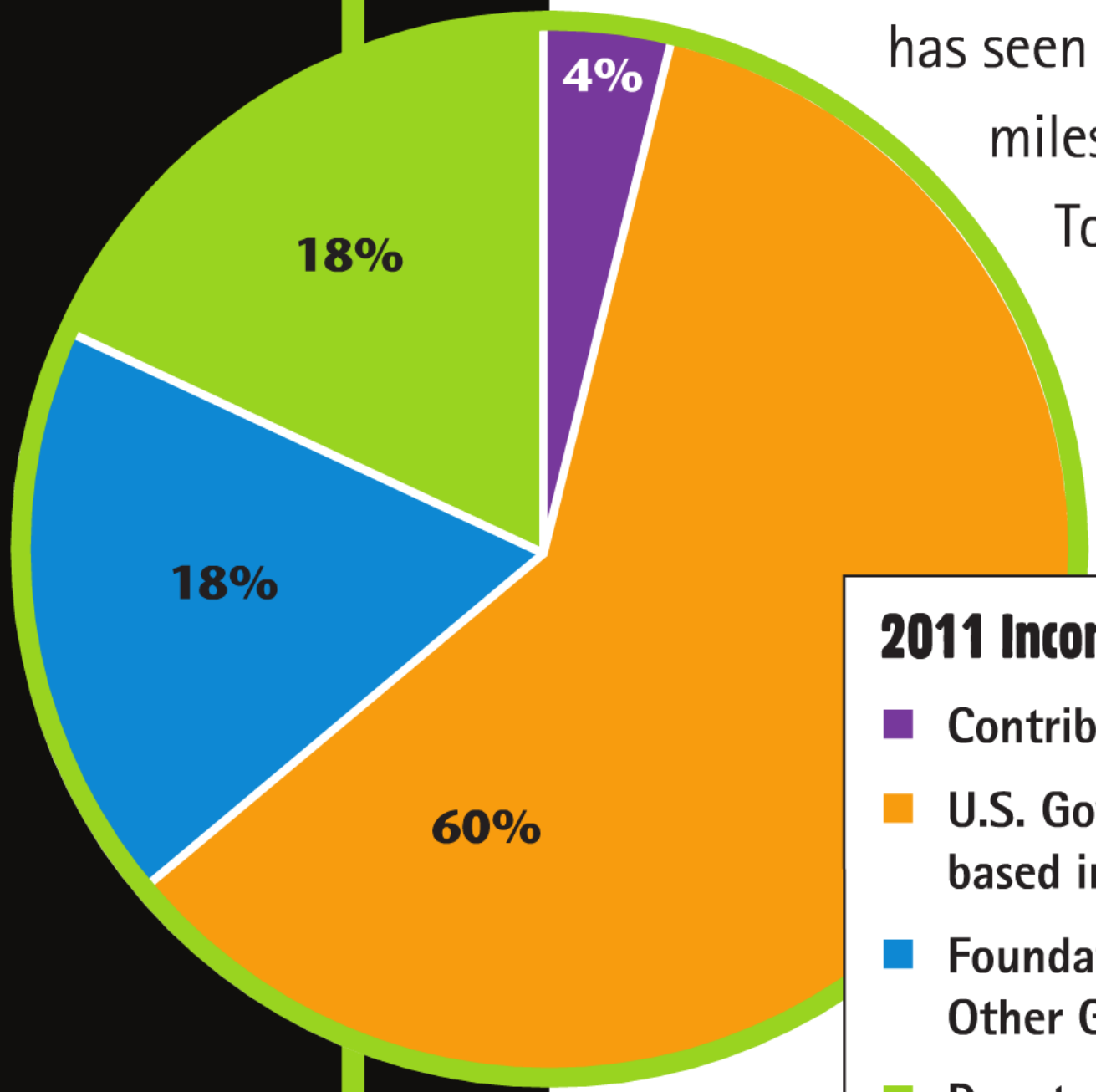
a

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



2011 Income

- Contributions
- U.S. Government based income
- Foundation and Other Grants
- Donated Services

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

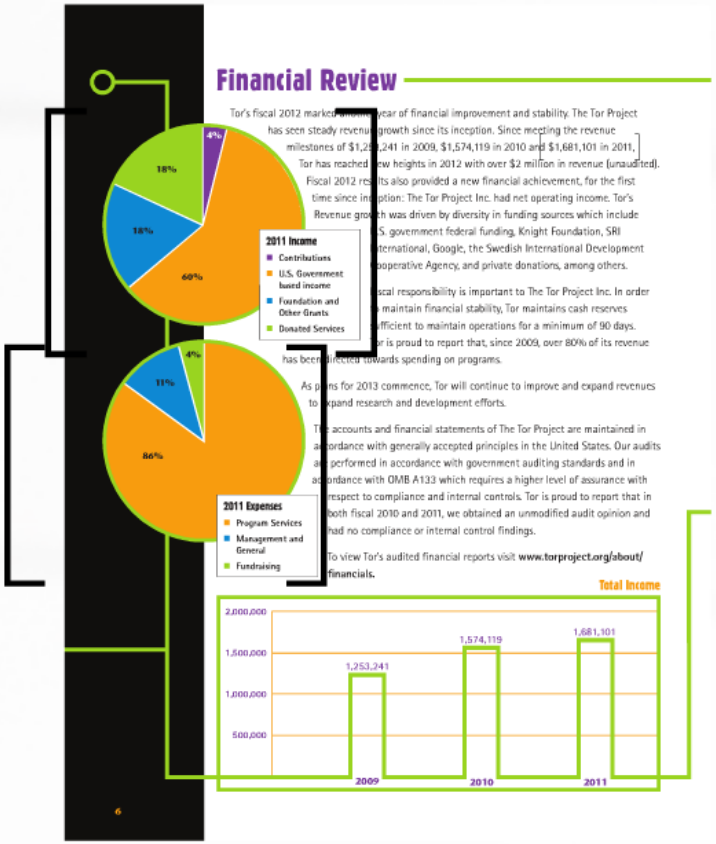
THIS IS WHAT A Tor

DAN ELLSBERG AND PATRICIA MARX ELLSBERG, *PRIVACY ACTIVISTS*

SUPPORTER LOOKS LIKE

#SUPPORT Tor

Sustainability



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