TorProject.org

Andrew Lewman
andrew@torproject.org

The Tor Project, Inc.

501(c)(3) non-profit organization dedicated to the research and development of technologies for online anonymity and privacy

Topics

- Anonymous Communications
- Tor Overview
- The Future

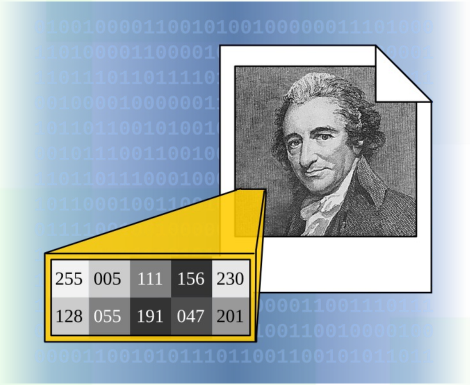
What is Anonymity?

Anonymity isn't:

- Cryptography

Anonymity isn't:

- Cryptography
- **Stenography**



Anonymity isn't:

- Cryptography
- Stenography
- **Wishful Thinking**

Examples of Wishful Thinking

- “They can't prove it was me.”
- “Promise you won't tell.”
- “Well, I didn't sign it.”
- “The Internet is already anonymous, right?”

- *“They can't prove it was me.”*
- “Promise you won't tell.”
- “Well, I didn't sign it.”
- “The Internet is already anonymous, right?”

- *“They can't prove it was me.”*
- “Promise you won't tell.”
- “Well, I didn't sign it.”
- “The Internet is already anonymous, right?”

Proof is a very strong word. Statistical analysis allows suspicion to become certainty.

- “They can't prove it was me.”
- *“Promise you won't tell.”*
- “Well, I didn't sign it.”
- “The Internet is already anonymous, right?”

- “They can't prove it was me.”
- *“Promise you won't tell.”*
- “Well, I didn't sign it.”
- “The Internet is already anonymous, right?”

Will other parties have the abilities and incentives to keep these promises?

- “They can't prove it was me.”
- “Promise you won't tell.”
- *“Well, I didn't sign it.”*
- “The Internet is already anonymous, right?”

- “They can't prove it was me.”
- “Promise you won't tell.”
- *“Well, I didn't sign it.”*
- “The Internet is already anonymous, right?”

Not what we're talking about.

- “They can't prove it was me.”
- “Promise you won't tell.”
- “Well, I didn't sign it.”
- *“The Internet is already anonymous, right?”*

- “They can't prove it was me.”
- “Promise you won't tell.”
- “Well, I didn't sign it.”
- *“The Internet is already anonymous, right?”*

Nope!

Anonymous Communication

People need to hide in a crowd of other people.

"Anonymity loves company."

Anonymous Communication

The goal of the system is to make all users look as similar as possible.

Anonymous Communication

Hide who is communicating with whom.

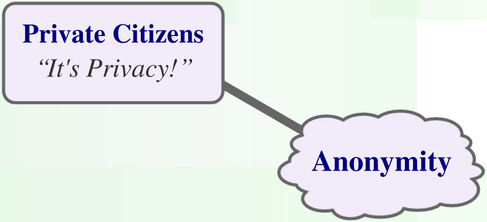
Anonymous Communication

Layered encryption and random delays hide correlation between input traffic and output traffic.

Anonymity serves different interests for different user groups:

Anonymity

Anonymity serves different interests for different user groups:

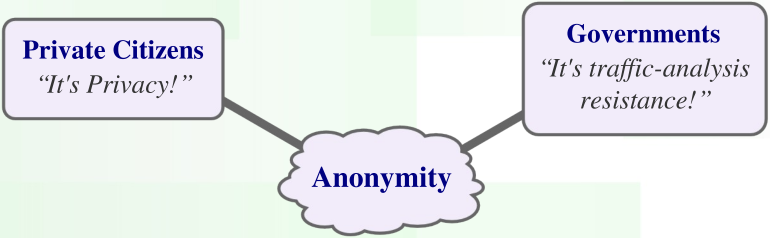


Private Citizens

"It's Privacy!"

Anonymity

Anonymity serves different interests for different user groups:



Private Citizens

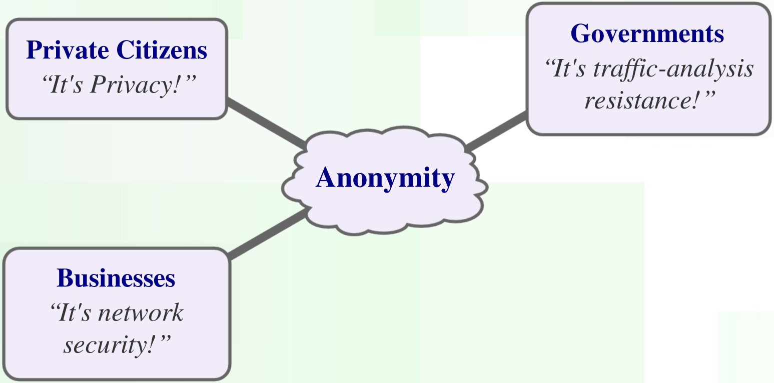
“It's Privacy!”

Governments

“It's traffic-analysis resistance!”

Anonymity

Anonymity serves different interests for different user groups:



Private Citizens

"It's Privacy!"

Governments

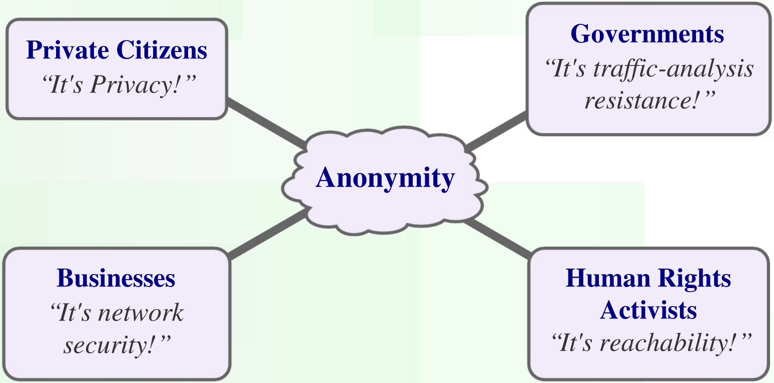
"It's traffic-analysis resistance!"

Anonymity

Businesses

"It's network security!"

Anonymity serves different interests for different user groups:



Anonymity

Private Citizens
“It's Privacy!”

Governments
“It's traffic-analysis resistance!”

Businesses
“It's network security!”

Human Rights Activists
“It's reachability!”

Tor is not the first system: ZKS, mixmaster, single-hop proxies, Crowds, Java Anon Proxy, VPNs.

Low Latency Systems

Low-latency systems are vulnerable to end-to-end correlation attacks.

High Latency Systems

High-latency systems are more resistant to end-to-end correlation attacks, but by definition, are less interactive.

Low Latency Systems

- Low-latency systems are generally more attractive to today's user:

  Interactive apps: web, instant messaging, VOIP, ssh, X11, cifs/nfs, video streaming (millions of users)

What is Tor?

- Online anonymity software and network

What is Tor?

Open source, freely available, 3-clause BSD licensed

What is Tor?

Active research environment:

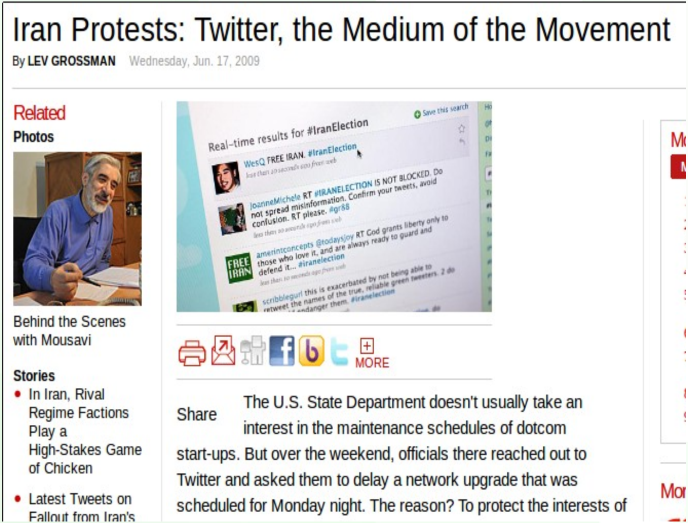
Rice, UMN, NSF, NRL, Drexel, Waterloo, Cambridge UK, Bamberg Germany, Boston Univ, Harvard, MIT, RPI, Georgia Tech

What is Tor?

Increasingly diverse toolset:

Tor, Torbutton, Tor Browser Bundle, TA(I)LS LiveCD, Tor Weather, Tor auto-responder, Secure Updater, Orbot, Torora, Tor Check, Arm, Nymble, Tor Control, Tor Wall, TorVM

Twitter In Iran: Good



Iran Protests: Twitter, the Medium of the Movement

By LEV GROSSMAN Wednesday, Jun. 17, 2009

Related

Photos

Behind the Scenes with Mousavi

Stories

- In Iran, Rival Regime Factions Play a High-Stakes Game of Chicken
- Latest Tweets on Fallout from Iran's

Real-time results for #IranElection

Save this search

WesQ FREE IRAN. #IranElection
less than 20 seconds ago from web

JoanneMichele RT #IRANELECTION IS NOT BLOCKED. Do not spread misinformation. Confirm your tweets, avoid confusion. RT please. #gr88
less than 20 seconds ago from web

amerintconcepts @todaysjoy RT God grants liberty only to those who love it, and are always ready to guard and defend it... #iranelection
less than 10 seconds ago from web

scribblegurl this is exacerbated by not being able to retweet the names of the true, reliable green tweeters. 2 do endanger them. #iranelection

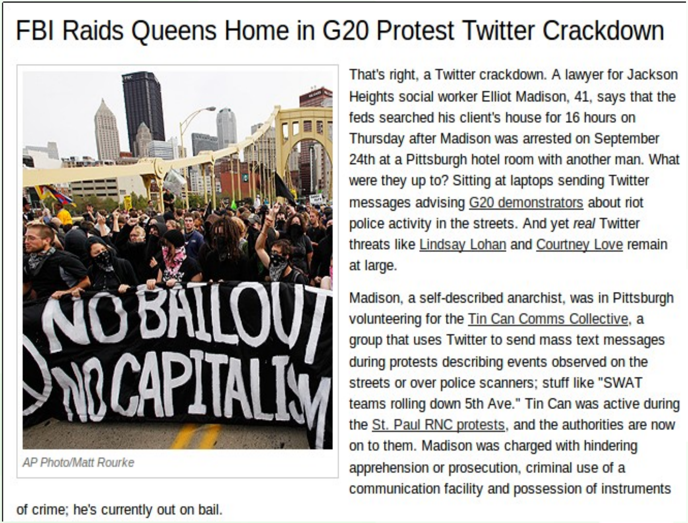
MORE

Share

The U.S. State Department doesn't usually take an interest in the maintenance schedules of dotcom start-ups. But over the weekend, officials there reached out to Twitter and asked them to delay a network upgrade that was scheduled for Monday night. The reason? To protect the interests of

From http://www.time.com/time/world/article/0,8599,1905125,00.html

Twitter In USA: Bad



FBI Raids Queens Home in G20 Protest Twitter Crackdown

AP Photo/Matt Rourke

That's right, a Twitter crackdown. A lawyer for Jackson Heights social worker Elliot Madison, 41, says that the feds searched his client's house for 16 hours on Thursday after Madison was arrested on September 24th at a Pittsburgh hotel room with another man. What were they up to? Sitting at laptops sending Twitter messages advising G20 demonstrators about riot police activity in the streets. And yet *real* Twitter threats like Lindsay Lohan and Courtney Love remain at large.

Madison, a self-described anarchist, was in Pittsburgh volunteering for the Tin Can Comms Collective, a group that uses Twitter to send mass text messages during protests describing events observed on the streets or over police scanners; stuff like "SWAT teams rolling down 5th Ave." Tin Can was active during the St. Paul RNC protests, and the authorities are now on to them. Madison was charged with hindering apprehension or prosecution, criminal use of a communication facility and possession of instruments of crime; he's currently out on bail.

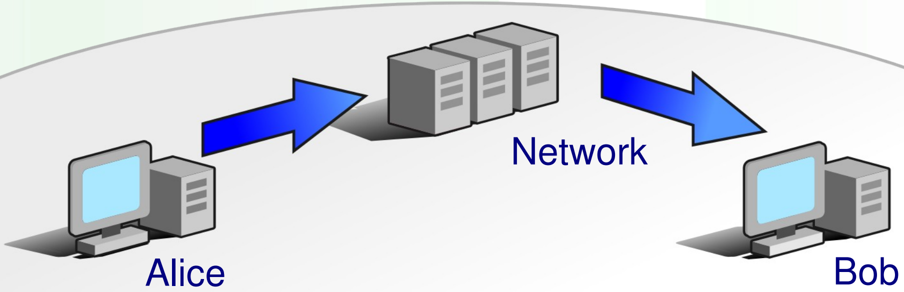
From http://gothamist.com/2009/10/05/fbi_raids_queens_home_in_g20_protes.php

Who Uses Tor?

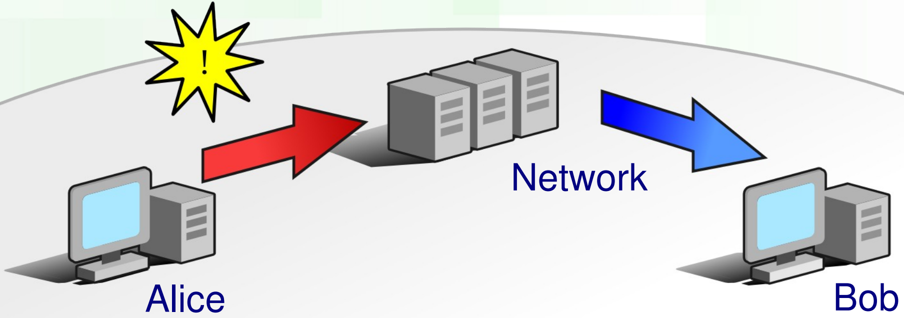
- Law Enforcement
- Human Rights Activists
- Business Executives
- Abuse Victims
- Militaries
- Normal People

Estimated 300k to 800k daily users worldwide

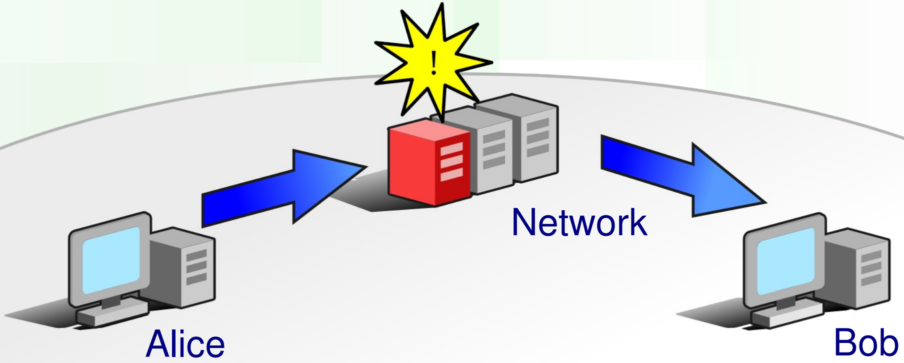
A Typical Internet Connection



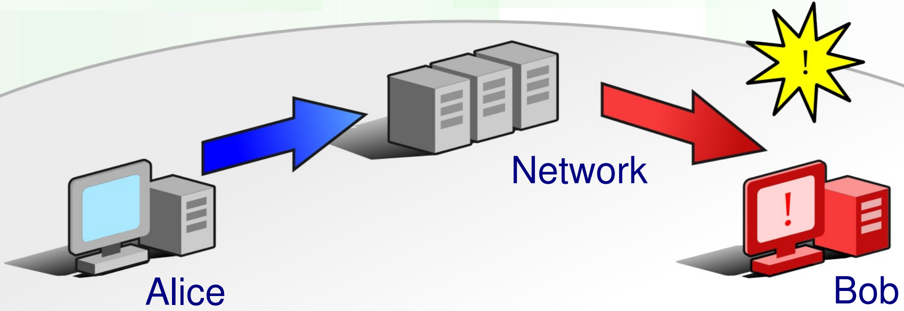
Alice might be watched.



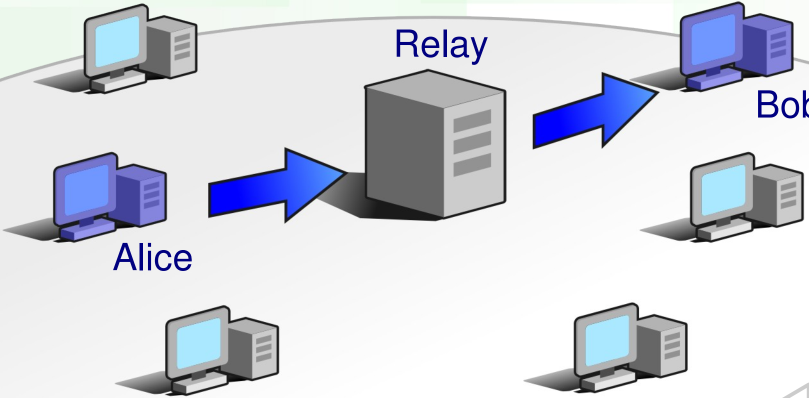
Parts of the network could be monitored.



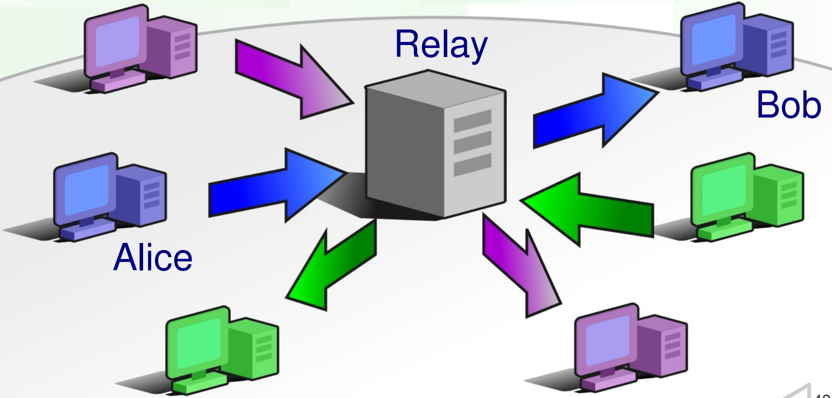
Bob could be compromised.



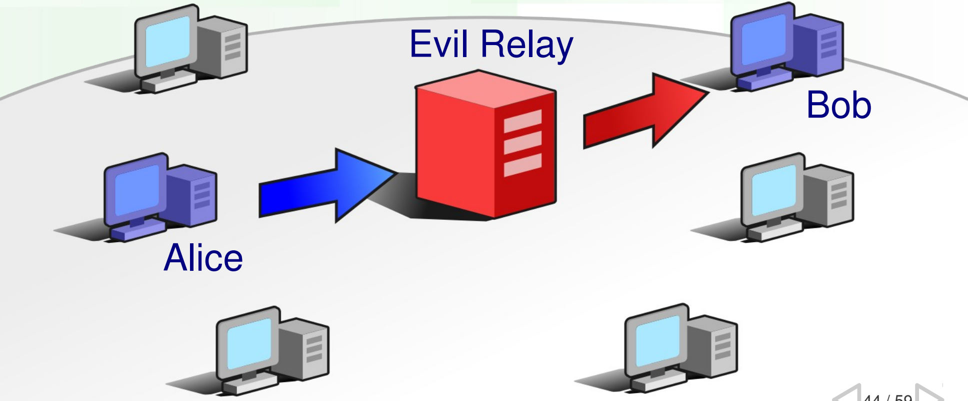
How is Tor Different?



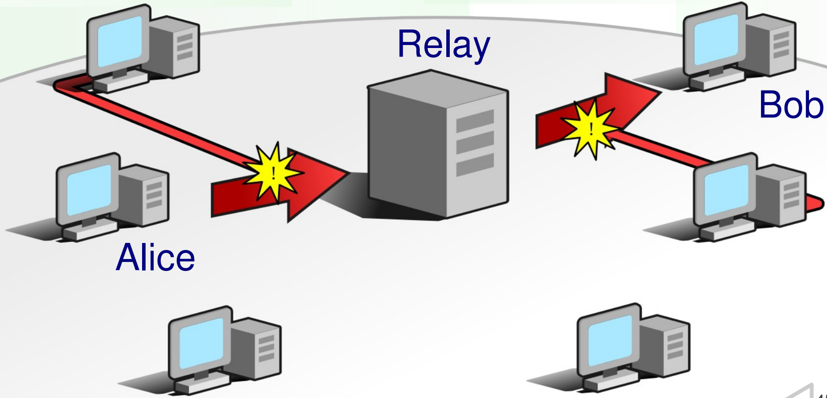
A Basic Relay System



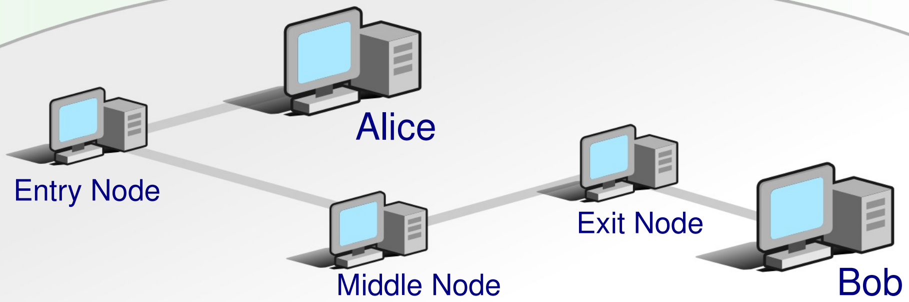
An Evil Relay



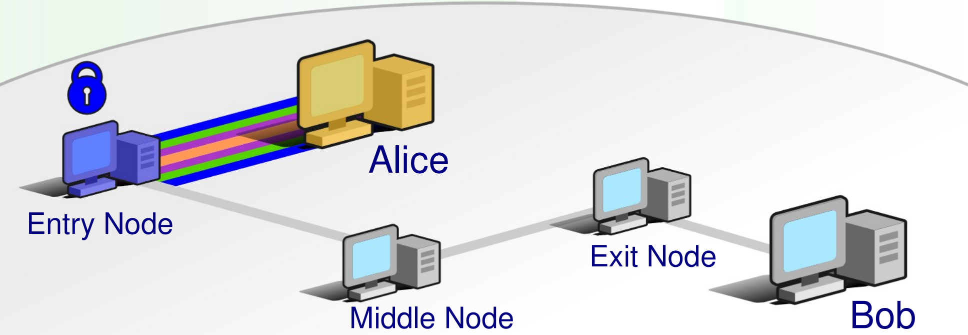
An Evil Network



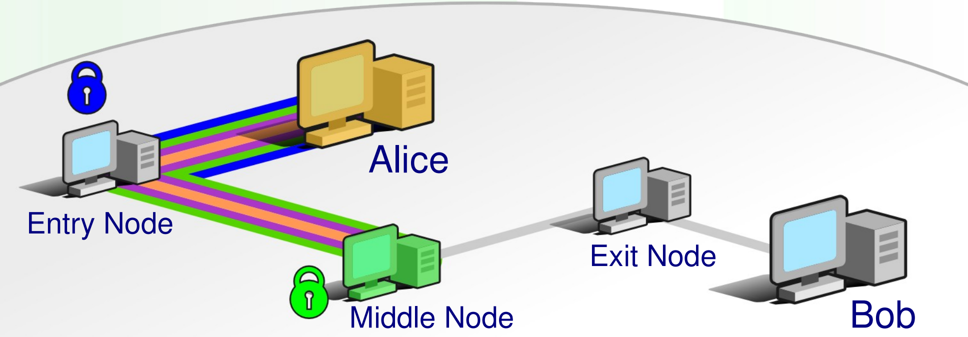
How Tor Works



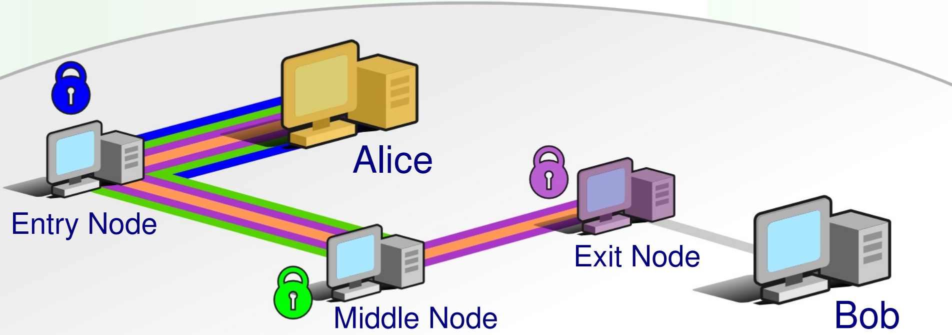
Alice connects to an Entry Node.



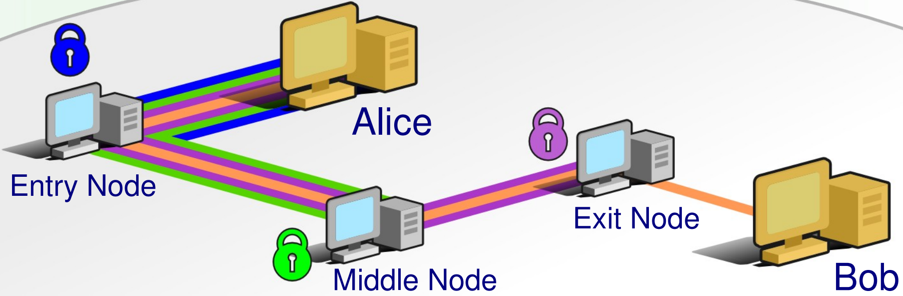
The data is routed through a Middle Node.



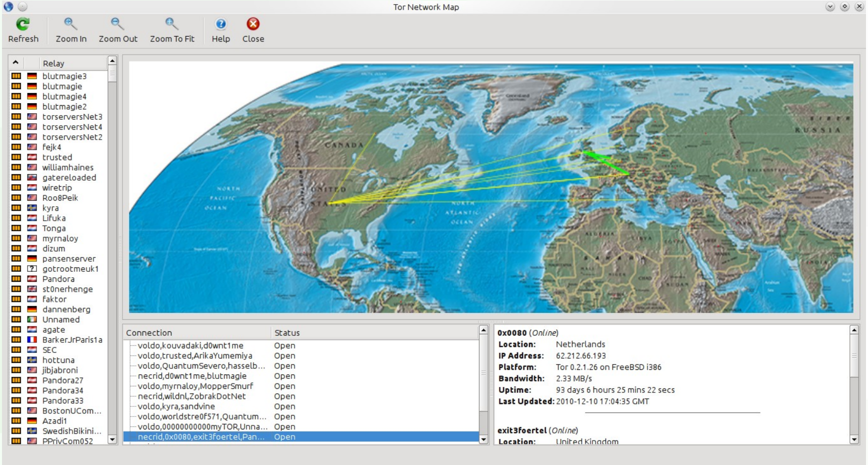
The data is routed through an Exit Node.



Alice's circuit to Bob is established.



Vidalia Network Map



Relay

- blutmagie3
- blutmagie
- blutmagie4
- blutmagie2
- torserversNet3
- torserversNet4
- torserversNet2
- fejk4
- trusted
- williamhaines
- gatereloaded
- wiretrip
- Roo8Peik
- kyra
- Lifuka
- Tonga
- myrnaloy
- dizum
- pansenserver
- gotrootmeuk1
- Pandora
- st0nerhenge
- faktor
- dannenberg
- Unnamed
- agate
- BarkerJrParis1a
- SEC
- hottuna
- jibjabroni
- Pandora27
- Pandora34
- Pandora33
- BostonUCom...
- Azadi1
- SwedishBikini...
- PPrivCom052

Connection	Status
voldo,kouvadaki,d0wnt1me	Open
voldo,trusted,ArikaYumemiya	Open
voldo,QuantumSevero,hasselb...	Open
necrid,d0wnt1me,blutmagie	Open
voldo,myrnaloy,MopperSmurf	Open
necrid,wildnl,ZobrakDotNet	Open
voldo,kyra,sandvine	Open
voldo,worldstre0f571,Quantum...	Open
voldo,0000000000myTOR,Unna...	Open
necrid,0x0080,exit3foertel,Pan...	Open

0x0080 (*Online*)

Location:	Netherlands
IP Address:	62.212.66.193
Platform:	Tor 0.2.1.26 on FreeBSD i386
Bandwidth:	2.33 MB/s
Uptime:	93 days 6 hours 25 mins 22 secs
Last Updated:	2010-12-10 17:04:35 GMT

exit3foertel (*Online*)

Location: United Kingdom

Metrics

- Measuring the Tor Network anonymously
- NSF grant for research
- Archive of hourly consensus, ExoneraTor, VisiTor
- Metrics portal:

  `https://metrics.torproject.org`

Operating Systems leak info like a sieve...

Applications, network stacks, plugins, oh my...

Operating Systems leak info like a sieve...

Applications,
network stacks,
plugins, oh my...
...some
call this sharing.

Operating Systems leak info like a sieve...

Did you know Microsoft Word and OpenOffice Writer are browsers?

Operating Systems leak info like a sieve...

`www.decloak.net`

Discover how much you like to share!

Mobile Operating Systems

- Entirely new set of challenges for something designed to know where you are at all times.
- Orbot: Tor on Android. **`https://guardianproject.info/apps/`**
- Tor on iphone, maemo/meego, symbian, etc
- Tor on Windows CE. For example: **`http://www.gsmk.de`**
- Guardian Project, **`https://guardianproject.info/`**

Next steps:

Visit us at **`https://www.torproject.org/`** for more information, links, and ideas.

Credits and Thanks

- ***Presentation:*** Andrew Lewman, Executive Director for The Tor Project – **andrew@torproject.org**
- ***Danger!***, **http://flickr.com/photos/hmvh/58185411/sizes/o/** hmvh, CC-BY-SA.
- ***500k,*** **http://www.flickr.com/photos/lukaskracic/334850378/sizes/l/** Luka Skracic, used with permission.
- ***Illustration and Design:*** J.M.Todaro – **http://jmtodaro.com**