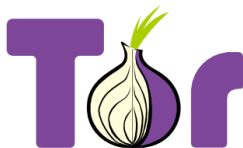


# DEA Tor Overview

Andrew Lewman  
andrew@torproject.org

January 11, 2013



**TorProject.org**

# What are we talking about?

- Crash course on anonymous communications
- Quick overview of Tor
- Quick overview of Tor Hidden Services
- Future directions

# The Tor Project, Inc.

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

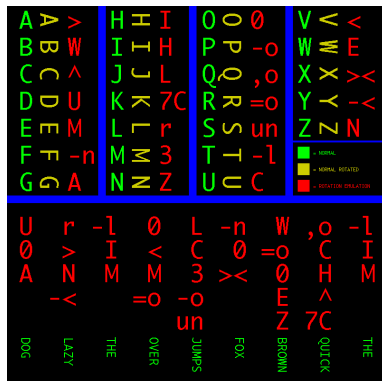


# What is anonymity?



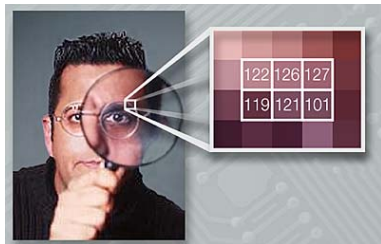
# Anonymity isn't cryptography

- Cryptography protects the contents in transit
- You still know who is talking to whom, how often, and how much data is sent.



# Anonymity isn't steganography

Attacker can tell Alice is talking to someone, how often, and how much data is sent.



# Anonymity isn't just wishful thinking...

- "You can't prove it was me!"

# Anonymity isn't just wishful thinking...

- "You can't prove it was me!"
- "Promise you won't look"



# Anonymity isn't just wishful thinking...

- "You can't prove it was me!"
- "Promise you won't look"
- "Promise you won't remember"

# Anonymity isn't just wishful thinking...

- "You can't prove it was me!"
- "Promise you won't look"
- "Promise you won't remember"
- "Promise you won't tell"

# Anonymity isn't just wishful thinking...

- "You can't prove it was me!"
- "Promise you won't look"
- "Promise you won't remember"
- "Promise you won't tell"
- "I didn't write my name on it!"

# Anonymity isn't just wishful thinking...

- "You can't prove it was me!"
- "Promise you won't look"
- "Promise you won't remember"
- "Promise you won't tell"
- "I didn't write my name on it!"
- "Isn't the Internet already anonymous?"

..since "weak" isn't anonymity.

- *"You can't prove it was me!"* Proof is a very **strong** word. Statistical analysis allows suspicion to become certainty.

..since "weak" isn't anonymity.

- *"You can't prove it was me!"* Proof is a very **strong** word. Statistical analysis allows suspicion to become certainty.
- *"Promise you won't look/remember/tell"* Will other parties have the abilities and incentives to keep these promises?

..since "weak" isn't anonymity.

- *"You can't prove it was me!"* Proof is a very **strong** word. Statistical analysis allows suspicion to become certainty.
- *"Promise you won't look/remember/tell"* Will other parties have the abilities and incentives to keep these promises?
- *"I didn't write my name on it!"* Not what we're talking about.

..since "weak" isn't anonymity.

- *"You can't prove it was me!"* Proof is a very **strong** word. Statistical analysis allows suspicion to become certainty.
- *"Promise you won't look/remember/tell"* Will other parties have the abilities and incentives to keep these promises?
- *"I didn't write my name on it!"* Not what we're talking about.
- *"Isn't the Internet already anonymous?"* Nope!



# Anonymous communication

- People have to hide in a crowd of other people (“anonymity loves company”)
- The goal of the system is to make all users look as similar as possible, to give a bigger crowd
- Hide who is communicating with whom
- Layered encryption and random delays hide correlation between input traffic and output traffic

# Low versus High-latency anonymous communication systems

- Tor is not the first system; ZKS, mixmaster, single-hop proxies, Crowds, Java Anon Proxy.
- Low-latency systems are vulnerable to end-to-end correlation attacks.
- High-latency systems are more resistant to end-to-end correlation attacks, but by definition, less interactive.

# 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)
- Multi-hour delays: email, nntp, blog posting? (tens of thousands of users?)

## 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)
- Multi-hour delays: email, nntp, blog posting? (tens of thousands of users?)
  - And if anonymity loves company...

# What is Tor?

- online anonymity software and network

# What is Tor?

- online anonymity software and network
- open source, freely available (3-clause BSD license)

# What is Tor?

- online anonymity software and network
- open source, freely available (3-clause BSD license)
- active research environment:  
Drexel, Univ of Waterloo, Georgia Tech, Princeton, Boston University, University College London, Univ of Minnesota, National Science Foundation, Naval Research Labs, Cambridge UK, Bamberg Germany, MIT...

# What is Tor?

- online anonymity software and network
- open source, freely available (3-clause BSD license)
- active research environment:  
Drexel, Univ of Waterloo, Georgia Tech, Princeton, Boston University, University College London, Univ of Minnesota, National Science Foundation, Naval Research Labs, Cambridge UK, Bamberg Germany, MIT...
- increasingly diverse toolset:  
Tor, Tor Browser Bundle, Tails LiveCD, Tor Weather, Tor auto-responder, Secure Updater, Orbot, Torora, Tor Check, Arm, Nymble, Tor Control, and so on.



# Other Systems

- VPN - Virtual Private Network, 1 to 1 connection, can redirect all traffic, generally encrypted

# Other Systems

- VPN - Virtual Private Network, 1 to 1 connection, can redirect all traffic, generally encrypted
- Proxy - 1 to 1 connection, per application traffic redirection, sometimes encrypted

# Other Systems

- VPN - Virtual Private Network, 1 to 1 connection, can redirect all traffic, generally encrypted
- Proxy - 1 to 1 connection, per application traffic redirection, sometimes encrypted
- I2P - Garlic routing, closed network, anonymity and reputation

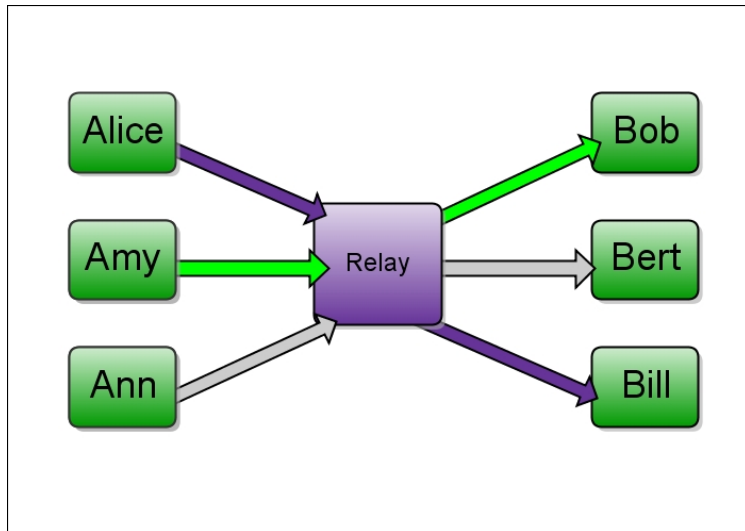
# Other Systems

- VPN - Virtual Private Network, 1 to 1 connection, can redirect all traffic, generally encrypted
- Proxy - 1 to 1 connection, per application traffic redirection, sometimes encrypted
- I2P - Garlic routing, closed network, anonymity and reputation
- Freenet - closed network, anonymity, distributed file storage and sharing

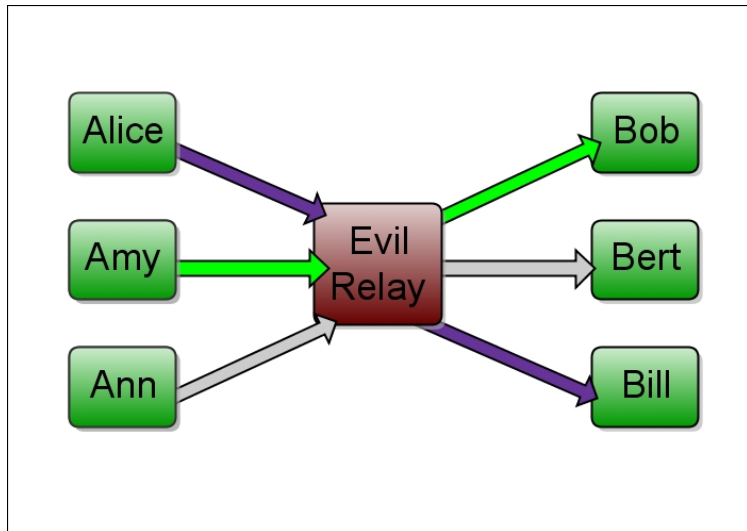
## Other Systems

- VPN - Virtual Private Network, 1 to 1 connection, can redirect all traffic, generally encrypted
- Proxy - 1 to 1 connection, per application traffic redirection, sometimes encrypted
- I2P - Garlic routing, closed network, anonymity and reputation
- Freenet - closed network, anonymity, distributed file storage and sharing
- GNUnet - closed network, anonymity, distributed file storage and sharing

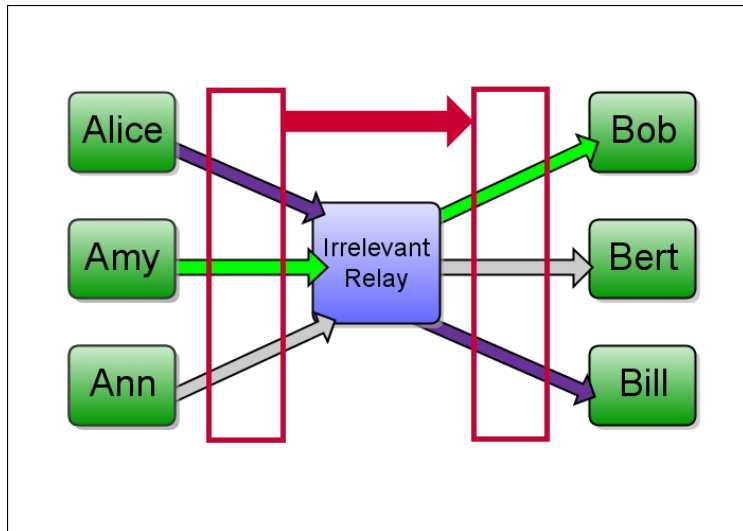
## How is Tor different from other systems?



## How is Tor different from other systems?

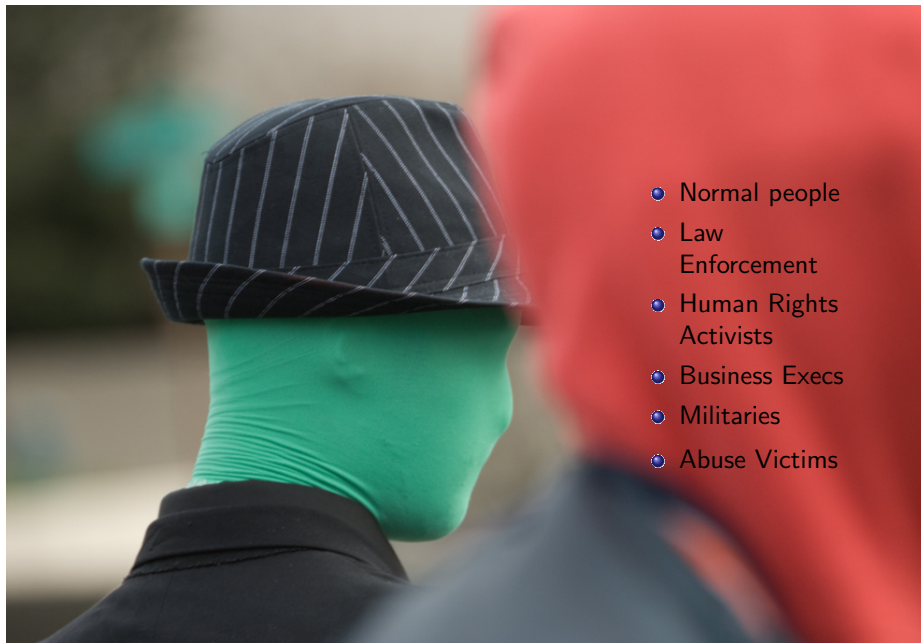


## How is Tor different from other systems?





# Who uses Tor?



- Normal people
- Law Enforcement
- Human Rights Activists
- Business Execs
- Militaries
- Abuse Victims

# Who uses Tor?

- *Normal users*

linking sensitive information to their current identities, online advertising networks, search engines, censorship circumvention

# Who uses Tor?

- *Law enforcement*  
accidental disclosure to targets, family and friend concerns, separating work from home life

# Who uses Tor?

- *Rights Activists*

Personal safety, family safety, narrowly-defined publicity, censorship circumvention

# Who uses Tor?

- *Business Execs*  
separating work from home life, competitor research, censorship circumvention

# Who uses Tor?

- *Abuse Victims and Survivors*

complete separation of past abuse and current life, finding help and safety, need to help others anonymously

# Who uses Tor?

- *Militaries*

intelligence gathering, separating work from home life, other activities

# Doesn't Tor enable criminals to do bad things?

“ *Criminals can already do bad things. Since they're willing to break laws, they already have lots of options available that provide better privacy than Tor provides.* ”

source:

<https://www.torproject.org/docs/faq-abuse.html.en#WhatAboutCriminals>



estimated 500k to 900k daily users



# Tor hides communication patterns by relaying data through volunteer servers

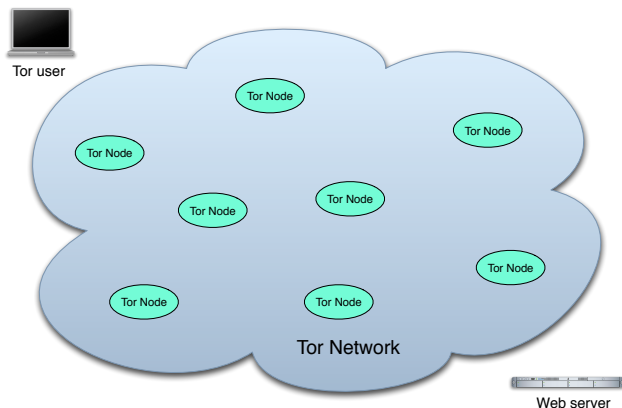


Diagram: Robert Watson

# Tor hides communication patterns by relaying data through volunteer servers

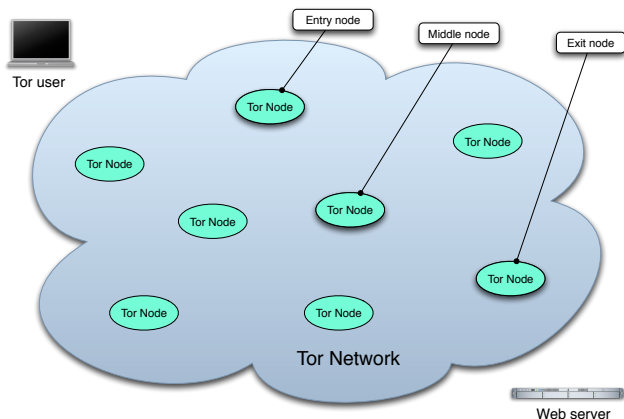


Diagram: Robert Watson

# Tor hides communication patterns by relaying data through volunteer servers

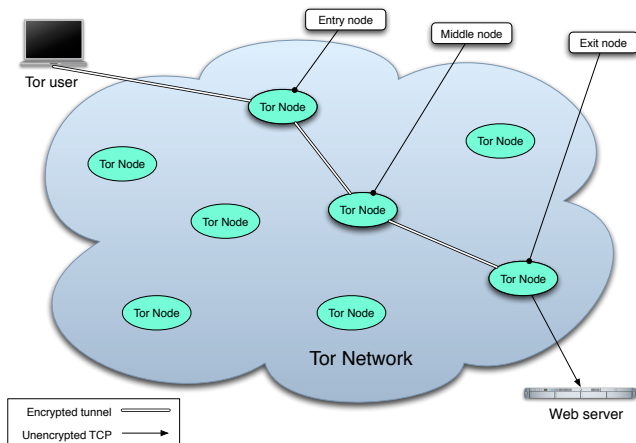


Diagram: Robert Watson

# Tor hides communication patterns by relaying data through volunteer servers

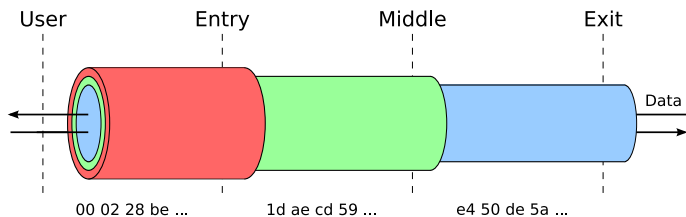


Diagram: Robert Watson

# Vidalia Network Map

**Relay**

- chomsky
- rainbowwarrior
- politkovskaja
- rockhall
- THEOPHYLAKT...
- TestTorRelay...
- trusted
- blutmagie
- blutmagie4
- blutmagie3
- blutmagie2
- TORy2
- TORy0
- parapapa
- oilsrv1
- Evey
- TORy1
- TORy3
- PPrivCom035
- PPrivCom034
- OldPlanetExpr...
- roszapeter
- CCN3
- CorvidLabs1
- Merav
- nonononon
- raidz
- ippages
- zeller
- raskin
- PPrivCom012
- PPrivCom053
- kyra
- kato
- morales
- Lifuka
- maumau
- PPrivCom013
- Shaman0

**Connection**

Connection	Status
FordModelA.sprockets.maumau2	Open
FordModelA.maumau.chaoscomputerclub3	Open

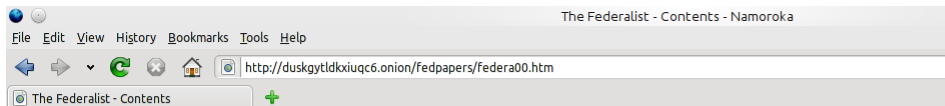
**maumau2 (Online)**

**Location:** Romania  
**IP Address:** 195.60.76.239  
**Platform:** Tor 0.2.2.25-alpha (git-fa48973a63191469) on  
**Bandwidth:** 5.54 MB/s  
**Uptime:** 12 days 17 hours 16 mins 56 secs  
**Last Updated:** 2011-05-14 21:25:17 GMT

# Metrics

- Measuring metrics anonymously
- NSF grant to find out
- Archive of hourly consensus, ExoneraTor, VisiTor
- Metrics portal:  
<https://metrics.torproject.org/>

# Tor hidden services allow privacy enhanced hosting of services



## The Federalist

The text of this version is primarily taken from the first collected 1788 "McLean edition", but spelling and punctuation errors -- mainly printer's lapses -- have been corrected. The main heads have also been taken from that edition and something like "The Same Subject Continued" we have repeated the previous heading and appended "(continued)", s have been guided by the excellent edition by Jacob E. Cooke, Wesleyan University Press, 1961. The footnotes are the edition used a variety of special typographical symbols for superscripts, we use numerals. Editors's footnotes are in original typography used for emphasis, such as all caps or italics, has been used here. We have tried to identify the



dot onion you say?

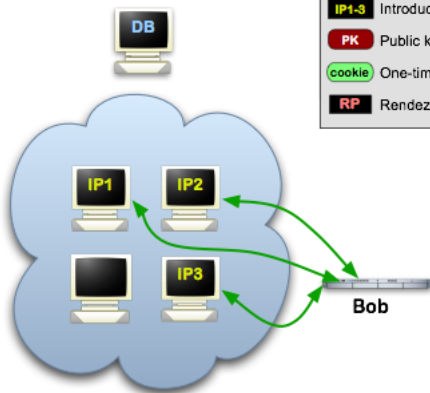


A screenshot of a web browser's address bar. The address bar contains the text `http://duskgytldkxiuqc6.onion/fedpapers/federa00.htm`. To the left of the text is a small icon representing a document or page. The address bar is set against a light gray background.

# Hidden Services, in graphics

## Tor Hidden Services: 1

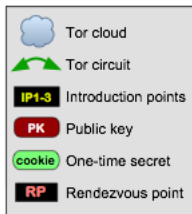
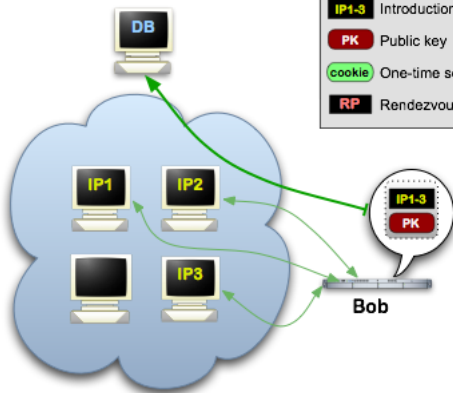
**Step 1:** Bob picks some introduction points and builds circuits to them.



# Hidden Services, in graphics

## Tor Hidden Services: 2

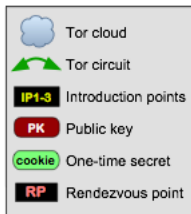
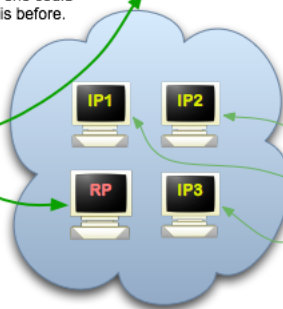
**Step 2:** Bob advertises his hidden service -- XYZ.onion -- at the database.



# Hidden Services, in graphics

## Tor Hidden Services: 3

**Step 3:** Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.



# Hidden Services, in graphics

## Tor Hidden Services: 4

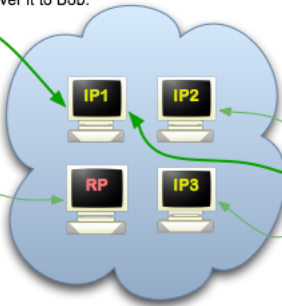
**Step 4:** Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.



Alice



DB



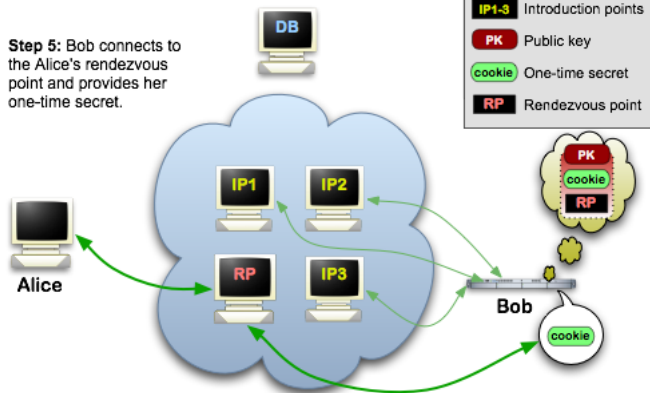
- Tor cloud
- Tor circuit
- Introduction points
- Public key
- One-time secret
- Rendezvous point

Bob

# Hidden Services, in graphics

## Tor Hidden Services: 5

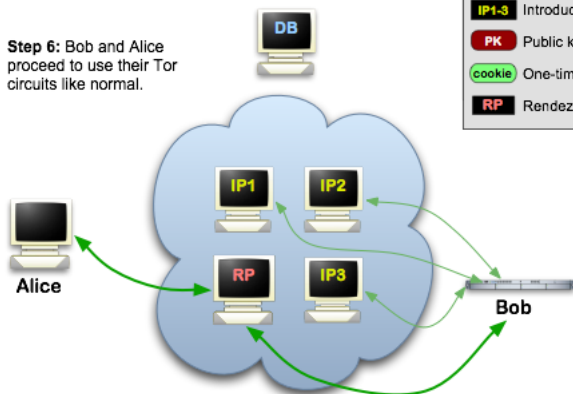
**Step 5:** Bob connects to the Alice's rendezvous point and provides her one-time secret.



# Hidden Services, in graphics

## Tor Hidden Services: 6

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



- Tor cloud
- Tor circuit
- Introduction points
- Public key
- One-time secret
- Rendezvous point

# 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



- Applications, network stacks, plugins, oh my.... some call this "sharing"
- Did you know Microsoft Word and OpenOffice Writer are browsers?

# Operating Systems leak info like a sieve



- Applications, network stacks, plugins, oh my.... some call this "sharing"
- Did you know Microsoft Word and OpenOffice Writer are browsers?
- [www.decloak.net](http://www.decloak.net) is a fine test

# 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 Mobile, <http://www.gsmk.de> as an example.
- Guardian Project, <https://guardianproject.info/>

Thanks!



Visit <https://www.torproject.org/> for more information, links, and ideas.

## Credits & Thanks

- who uses tor?  
<http://www.flickr.com/photos/mattw/2336507468/siz>, Matt Westervelt, CC-BY-SA.
- danger!, <http://flickr.com/photos/hmvh/58185411/sizes/o/>, hmvh, CC-BY-SA.
- 500k, <http://www.flickr.com/photos/lukaskracic/334850378/sizes/1/>, Luka Skracic, used with permission.
- zscaler research, <http://research.zscaler.com/2011/12/web-threats-trends-and-statistics.html>