

[redacted]

Summer school on real-world crypto and privacy 2015
Šibenik, Croatia

Jacob Appelbaum

[redacted]

05 June 2015

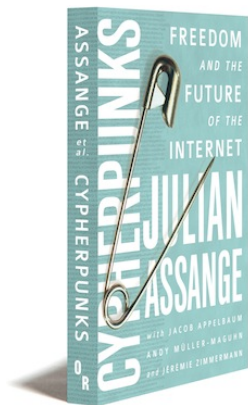
Happy Anniversary

Thank you Edward Snowden!

Context

"World War III is a guerrilla information war with no division between military and civilian participation." - Marshall McLuhan in Culture Is Our Business

Anonymity and Censorship: a cypherpunk history



Anonymity and Censorship: an academic history

anonbib: <http://www.freehaven.net/anonbib/>

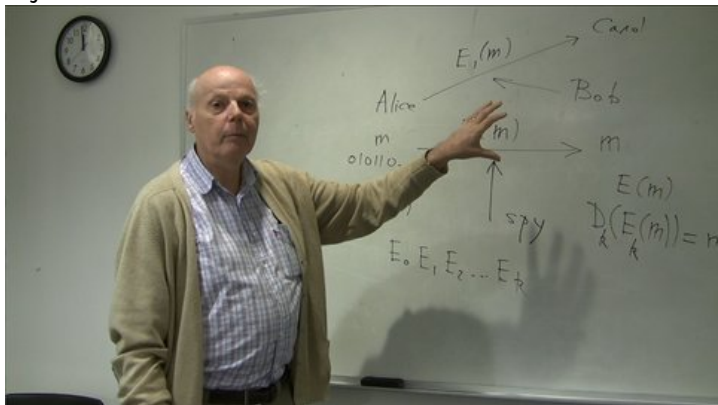
ensorbib: <http://www.cs.kau.se/philwint/censorbib/>

Surveillance in context

"But it is just terrorists..."

Surveillance in context

"But it is just terrorists..."



Surveillance in context


"We Kill People Based on Metadata" - Michael Hayden, Former Director of the CIA

Mass surveillance as an API

Actual XKeyscore rule sample:

```
// START_DEFINITION
requires grammar version 5
/**
 * Identify clients accessing Tor bridge information.
 */
fingerprint('anonymizer/tor/bridge/tls') =
ssl_x509_subject('bridges.torproject.org') or
ssl_dns_name('bridges.torproject.org');
```

OTR thwarts passive surveillance



[OC: No decrypt available for this OTR encrypted message.]

Tor, Tails, Redphone and more

TOP SECRET//COMINT//REL FVEY//20340601

Examples: Jan-February 2012

(TS//SI//REL)

Impact > to production Use Risk <	TRIVIAL Loss/lack of insight to small aspect of target communications, presence	MINOR Loss/lack of insight to significant aspect of target communications, presence	MODERATE Loss/lack of insight to large component of target communications, presence	MAJOR Loss/lack of insight to majority of target communications, presence	CATASTROPHIC Near-total loss/lack of insight to target communications, presence
Current Highest Priority Target Use	TeamViewer Join.Me LaplinskGold			Tor TrueCrypt TAILS	
Current Operational Target Use	Muslima				
Current Low Priority/Previous Higher Priority Target Use	Purematrimony.com			Web.de Cspace	
Technical Thought Leader Recommendations, Experimentation	Zemana Anti-Keylogger			Redphone	

TOP SECRET//COMINT//REL FVEY//20340601

"You never change things by fighting the existing reality. To change something, build a new model that makes the existing model obsolete." -
R. Buckminster Fuller

Building a new model

We know that cryptography works when applied properly.
We need a cryptographic system to protect metadata and content.

An anonymity system for everyone: <https://www.torproject.org/>

Tor

An anonymity system for everyone: <https://www.torproject.org/>
Full details available in our torspec
<https://gitweb.torproject.org/torspec.git> repository and in
various peer reviewed papers.

Tor

An anonymity system for everyone: <https://www.torproject.org/>

Full details available in our torspec

<https://gitweb.torproject.org/torspec.git> repository and in various peer reviewed papers.

Tom Ritter produced an incredible overview document:

https://ritter.vg/blog-all_about_tor.html

Tor

An anonymity system for everyone: <https://www.torproject.org/>

Full details available in our torspec

<https://gitweb.torproject.org/torspec.git> repository and in various peer reviewed papers.

Tom Ritter produced an incredible overview document:

https://ritter.vg/blog-all_about_tor.html

Free Software for Freedom, community run, freely available, etc.

How does Tor work?

The basic idea is conceptually simple: compartmentalize information

How does Tor work?

The basic idea is conceptually simple: compartmentalize information
Currently the network has ~6500 nodes for Tor ~2m active daily users

User interface

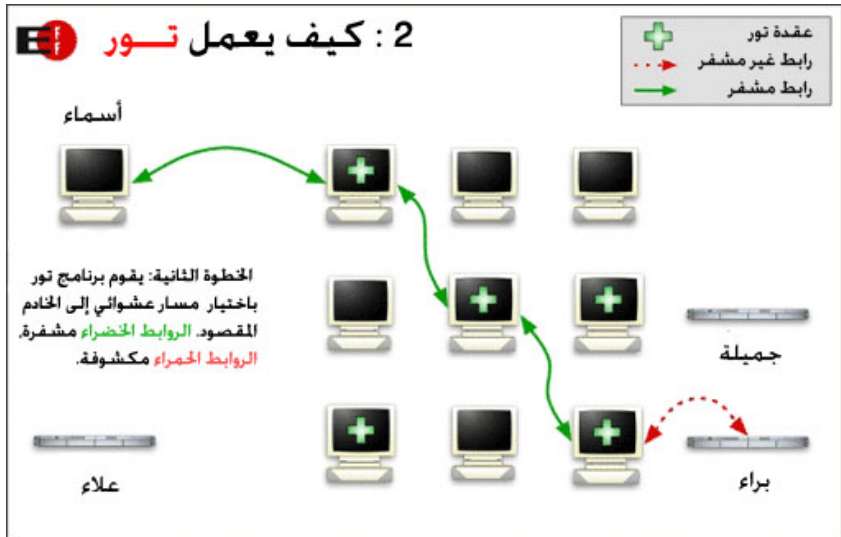
Two primary interfaces:

- Tor as a SOCKS proxy
- Tor (as a) Browser

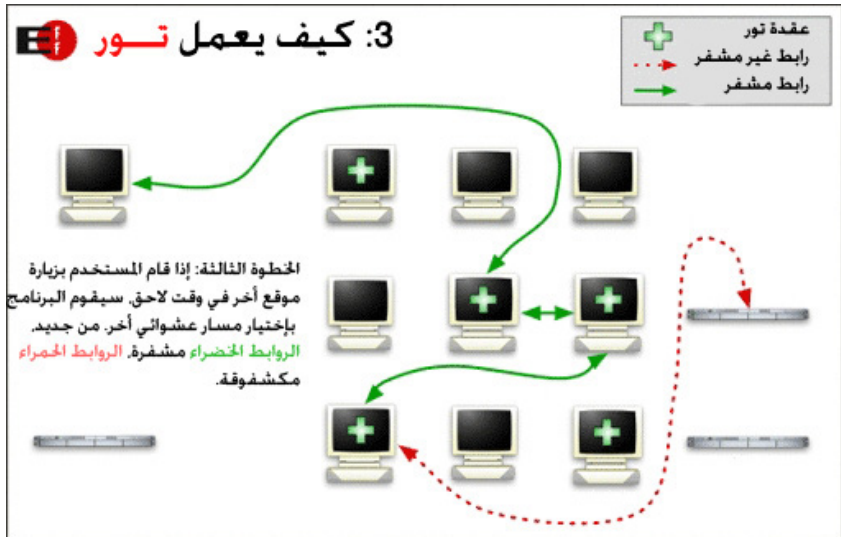
Tor circuit



Tor circuit



Tor circuit



Tor circuits

- Constrained by various parameters tuned by members of the network itself.
- Source routed
- Compartmentalized with cryptography

The Tor Network

The Tor network assigns various flags and details to nodes:

- Dir
- Directory Authority
- Fast
- Guard
- HSDir
- Stable

The Tor Network

Directory Authorities produce a consensus document

The consensus

A document cryptographically binding together various details about nodes

The consensus

A document cryptographically binding together various details about nodes

- Observed bandwidth
- IP and port information
- cryptographic details
- ...

The consensus

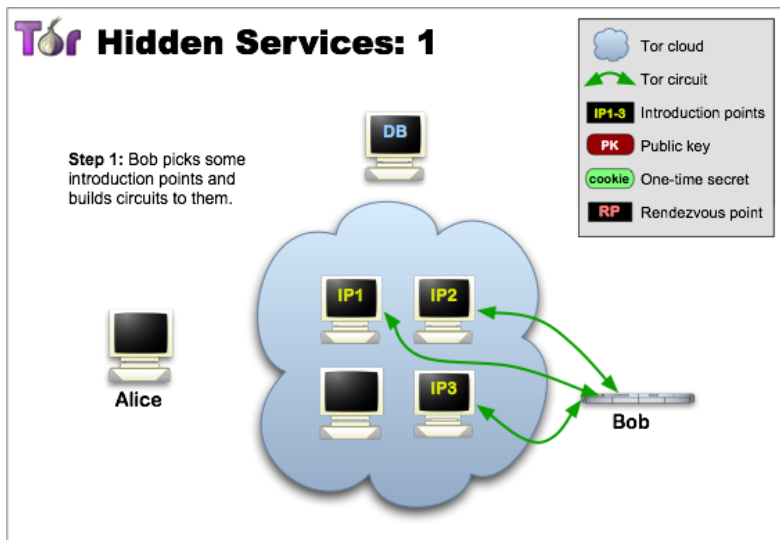
A document cryptographically binding together various details about nodes

- Observed bandwidth
- IP and port information
- cryptographic details
- ...

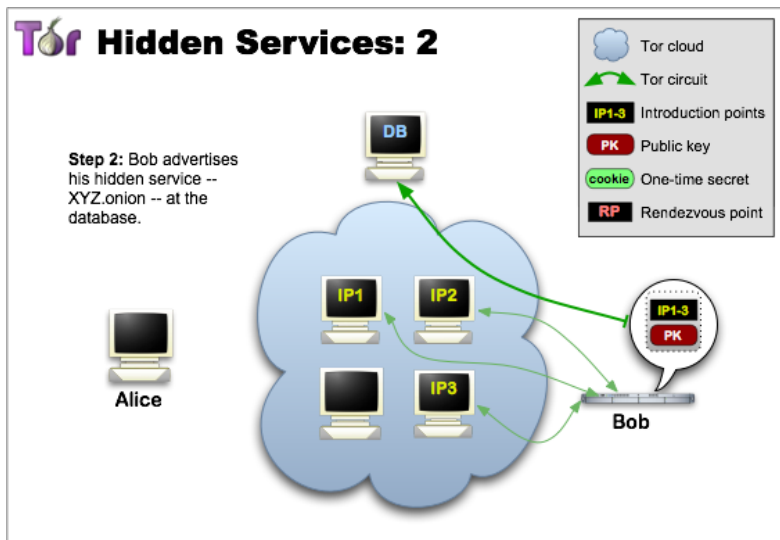
Hidden Services

- See rend-spec.txt in torspec
- Also see <https://www.torproject.org/docs/hidden-services.html>
- End to End Encrypted, anonymized connections
- Used to host TCP services

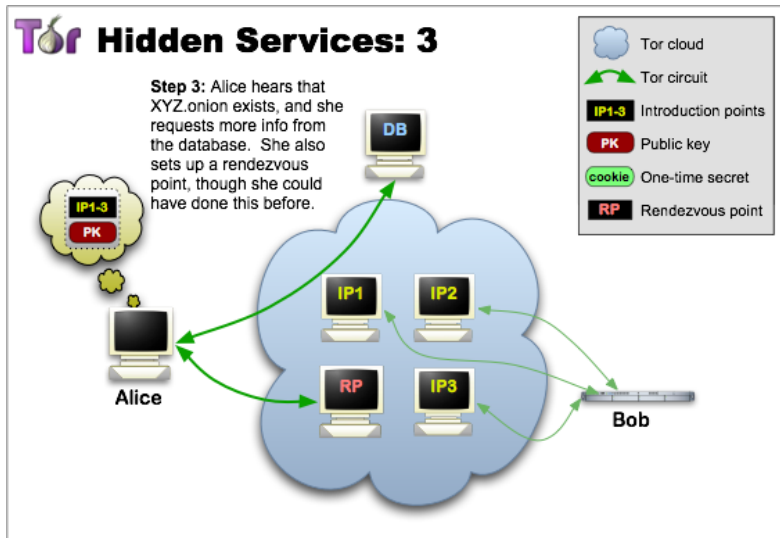
Tor Hidden Services



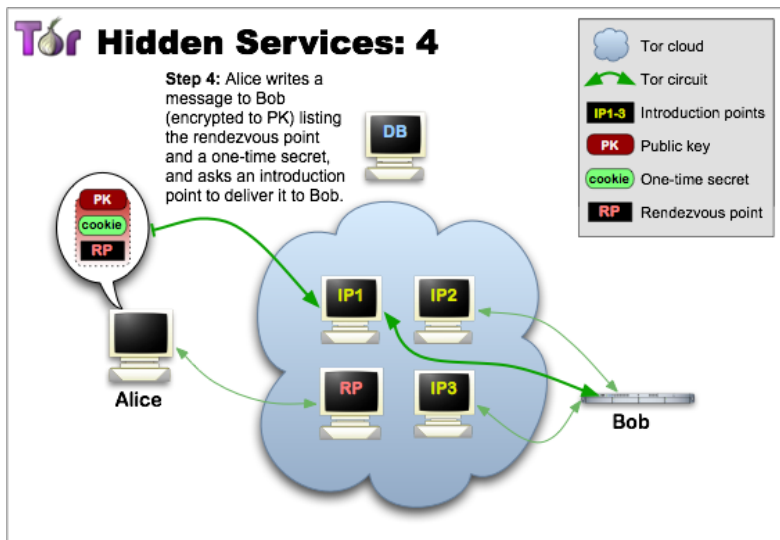
Tor Hidden Services



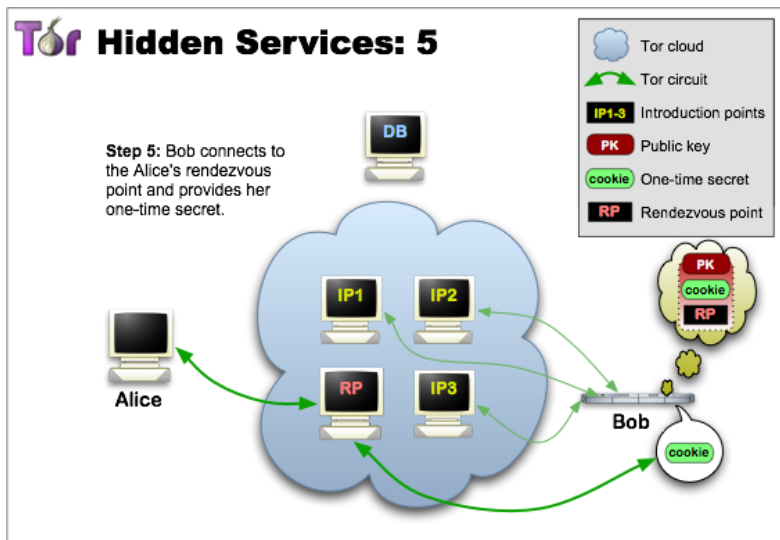
Tor Hidden Services



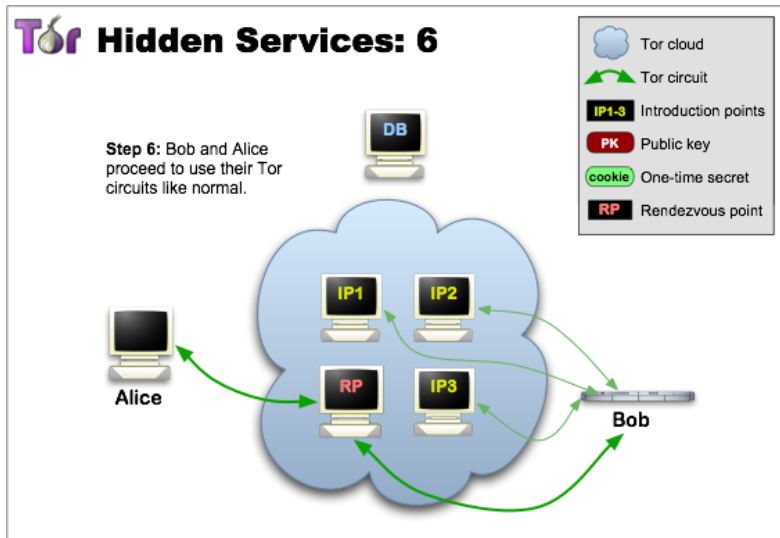
Tor Hidden Services



Tor Hidden Services

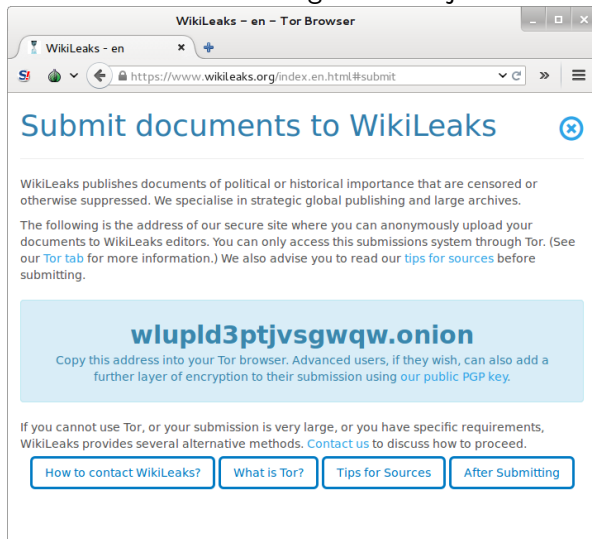


Tor Hidden Services



An example built on anonymity technology

The Tor Browser on Tails visiting a normal journalistic website:



The internet is more than the world wide web

- Jabber offered over Tor Hidden Services composed with OTR
- Pond: <https://pond.imperialviolet.org/>
- Tails: <https://tails.boum.org/>

making the existing model obsolete

Privacy Enhancing Technologies change the playing field.

History provides a model for change

Russell-Einstein Manifesto - issued July 9, 1955 in London

History provides a model for change

"Remember your humanity, and forget the rest."

Questions?

I encourage you to become the next Chelsea Manning, Thomas Drake, Jesselyn Radack, William Binney, Mark Klein, J. Kirk Wiebe, Edward Snowden, Daniel Ellsberg - a long line of heroic people whose sacrifices have brought us here today.