

RSA[®]Conference2016

San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: SBX3-W05

Cryptoparty: tuTORial—Learn How to Use TOR to Be Anonymous Online



Connect **to**
Protect

Runa A. Sandvik

Independent security researcher
@runasand

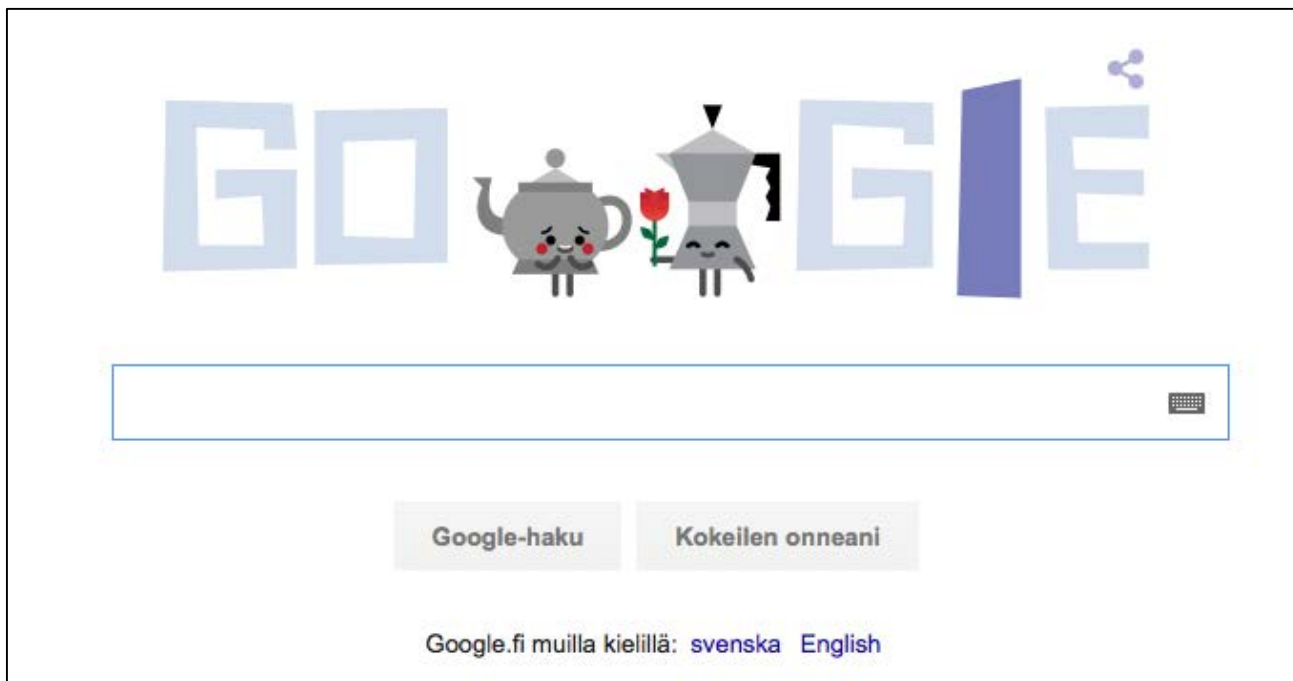


#RSAC

More than just anonymity, part I



#RSAC



More than just anonymity, part II



#RSAC



Brad Heath ✓
@bradheath

[Follow](#)

[@georgemaschke](#) I use it all the time. Last year, it was the only way I could look up cases in PA because the state court website blocked me.

RETWEETS	LIKES
13	26



1:04 PM - 21 Jan 2016

← ↻ ❤️ ⋮

About Tor and The Tor Project



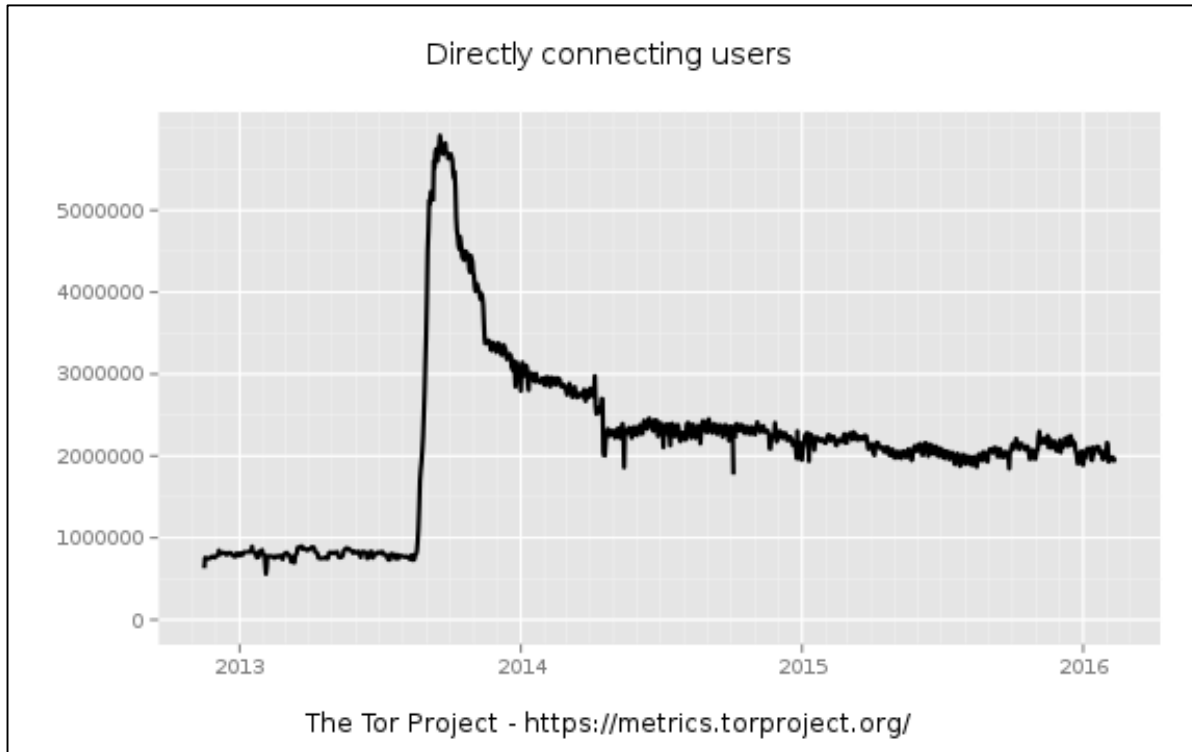
#RSAC

- Onion routing was developed by the U.S. NRL in the mid-1990s
- An alpha version of Tor launched in 2002
- Tor—the second generation onion router—was released in 2004
- The Tor Project 501(c)(3) was founded in 2006
- Around 2 million users worldwide in 2016

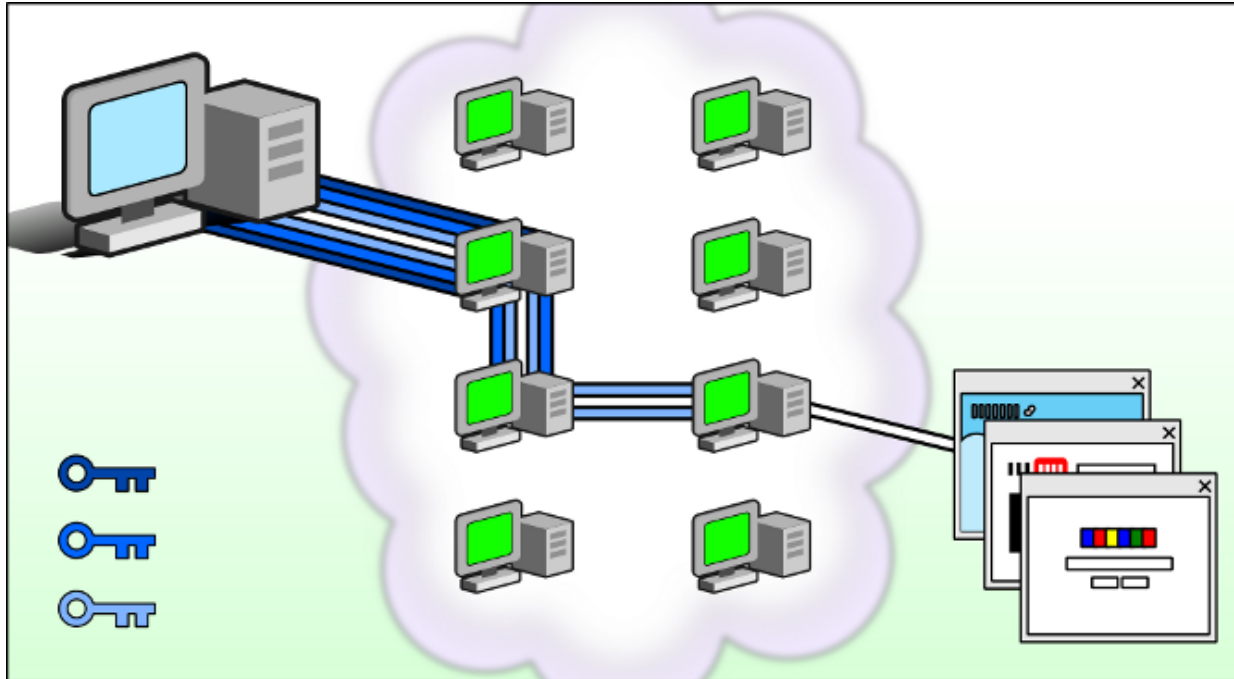
Directly connecting Tor users



#RSAC



How Tor works



Tor and censorship resistance



- Around 7,000 relays in the network
- Around 3,000 bridges in the network
- *Bridges* get around a censor that blocks by IP
- *Pluggable transports* get around a censor that blocks by DPI
- <https://www.torproject.org/docs/pluggable-transport.html.en>

About the Tor Browser, part I




#RSAC

About Tor

about:tor

Startpage

Tor Browser 4.0



Congratulations!

This browser is configured to use Tor.
You are now free to browse the Internet anonymously.

[Test Tor Network Settings](#)

Search securely with Startpage.

What Next?

Tor is NOT all you need to browse anonymously!
You may need to change some of your browsing habits to ensure your identity stays safe.

[Tips On Staying Anonymous »](#)

You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- [Run a Tor Relay Node »](#)
- [Volunteer Your Services »](#)
- [Make a Donation »](#)

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. [Learn more about The Tor Project »](#)

About the Tor Browser, part II



#RSAC

- Firefox Extended Support Release, with additional patches
- Pre-configured to use Tor, self-updating
- More user-friendly than five years ago, but still slow
- Will block browser plugins such as Flash
- Ensures the use of HTTPS with *HTTPS Everywhere*

About Hidden Services, part I



- *.onion* is a special-use domain name (RFC7686)
- Example: *facebookcorewwi.onion*
- Users can choose the security properties they want
- Traffic never leaves the Tor network
- *Tor onion services: more useful than you think [32c3]*

About Hidden Services, part II

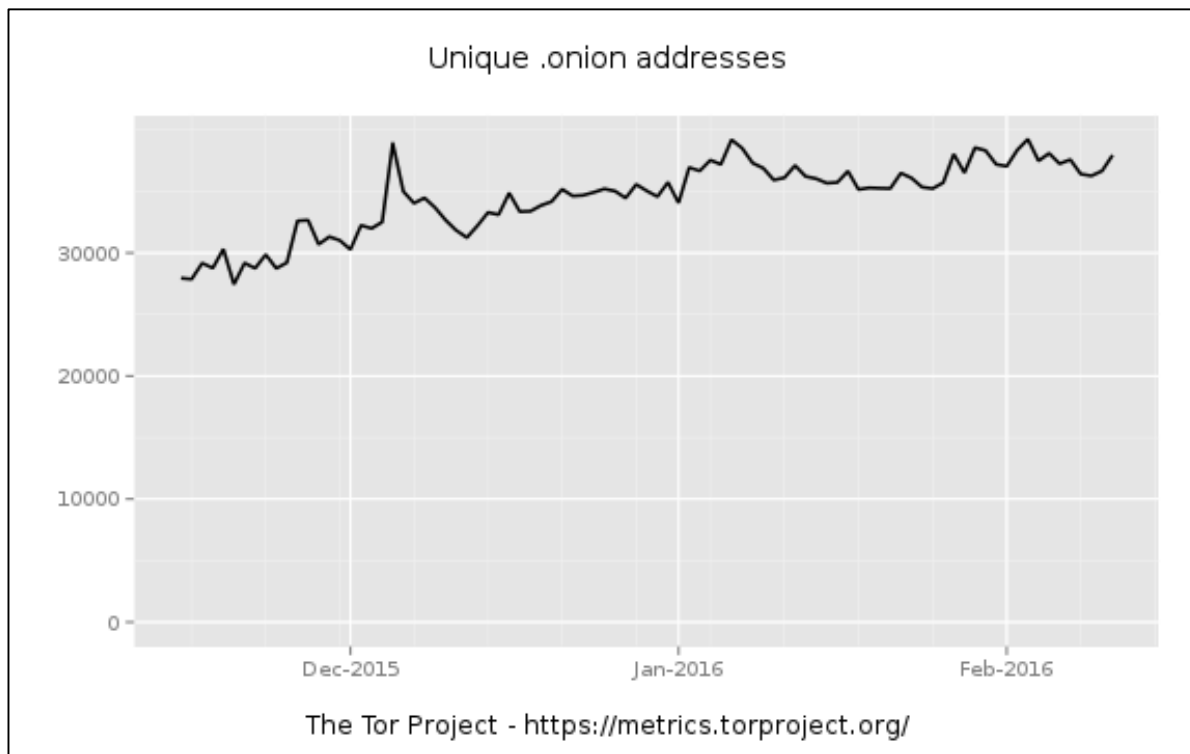


- Self-authenticated
- End-to-end encrypted
- NAT punching
- Limit surface area

Unique .onion addresses



#RSAC



On the deep, dark, mysterious web



- SecureDrop
- Blockchain.info*
- Facebook*
- OnionShare
- Instant messaging (Pond, Ricochet, XMPP)

Facebook's .onion with EV SSL cert



Researching the network and its users



#RSAC

- Tor network status protocol: <https://onionoo.torproject.org/>
- Tor Metrics: <https://metrics.torproject.org/>
- Simulate Tor network topologies: <https://shadow.github.io/>
- Selected papers in anonymity: <http://freehaven.net/anonbib/>
- Tor relay and bridge explorer: <https://globe.torproject.org/>