RSA®Conference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SBX3-W05

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

Runa A. Sandvik

Independent security researcher
@runasand

#RSAC

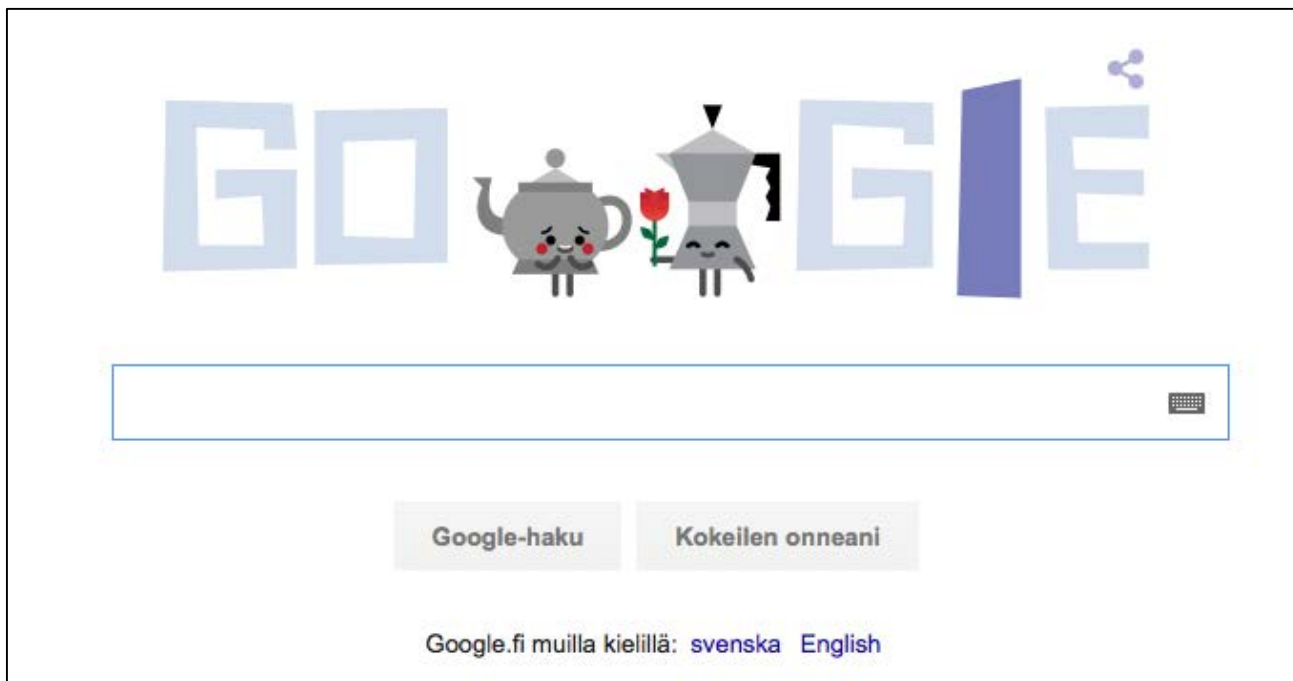# More than just anonymity, part I

RSAConference2016

More than just anonymity, part II
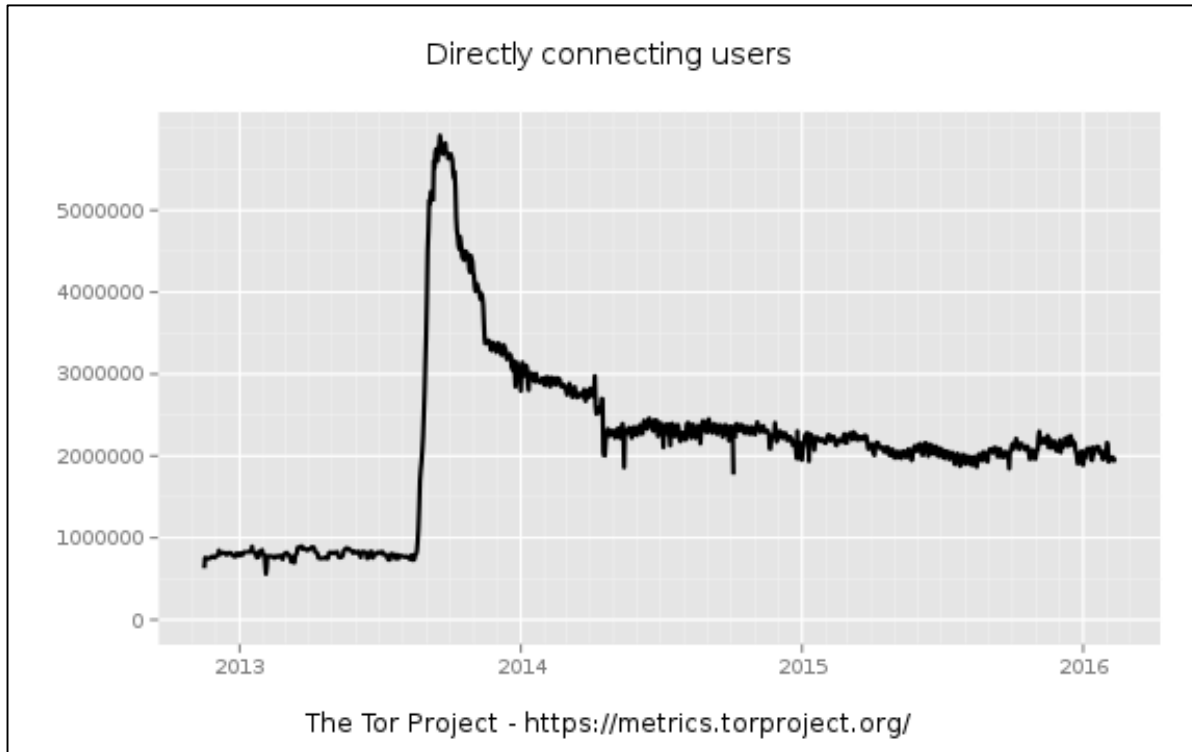
RSAConference2016

About Tor and The Tor Project

- 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
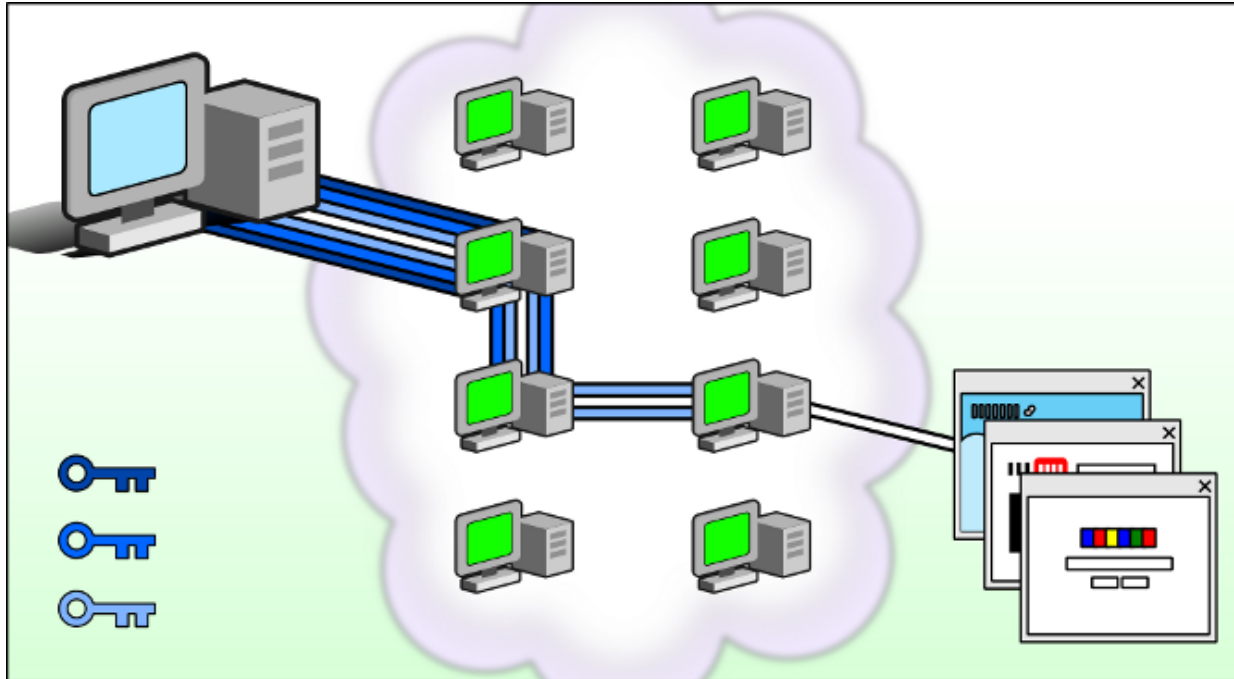
- Around 2 million users worldwide in 2016

RSA Conference2016

Directly connecting Tor users

Directly connecting users

The Tor Project - https://metrics.torproject.org/

RSAConference2016

How Tor works

RSAConference2016

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-transports.html.en

RSA Conference 2016

About the Tor Browser, part I

RSAConference2016

About the Tor Browser, part II

- 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*

RSA Conference2016

About Hidden Services, part I

- *.onion* is a special-use domain name (RFC7686)

- Example: *facebookcorewwwi.onion*

- Users can choose the security properties they want

- Traffic never leaves the Tor network

- *Tor onion services: more useful than you think [32c3]*

RSA Conference2016

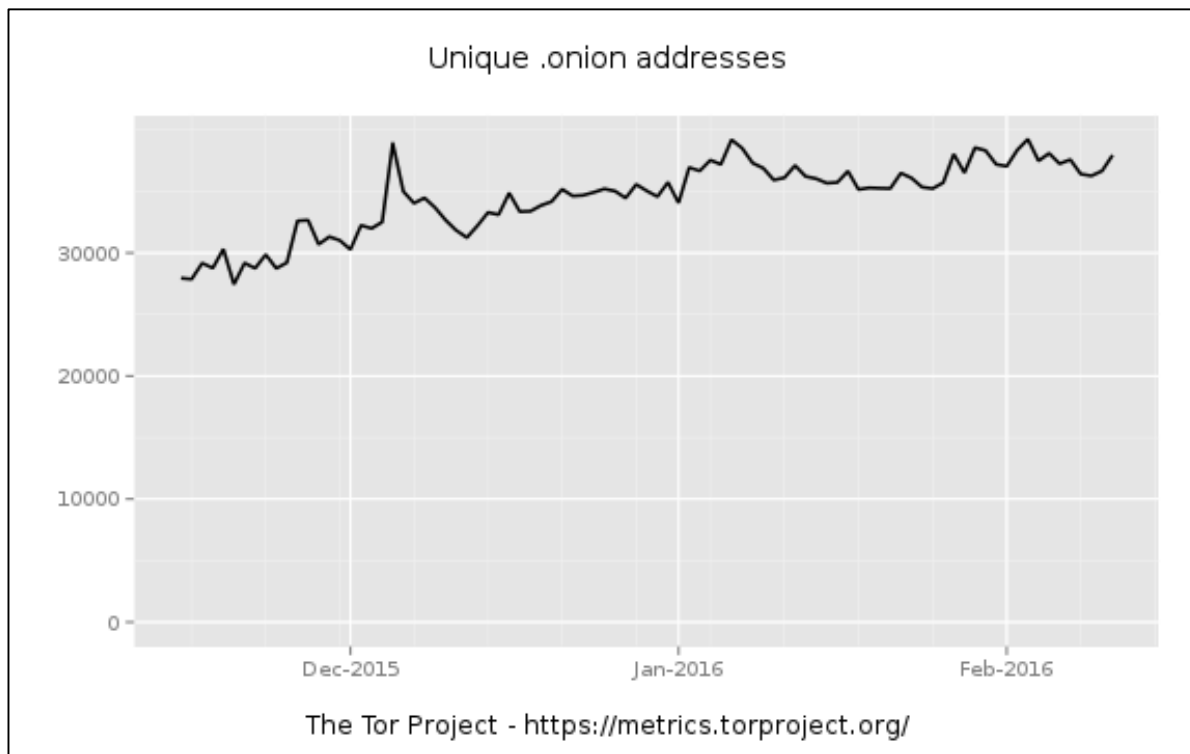# About Hidden Services, part II

- Self-authenticated

- End-to-end encrypted

- NAT punching

- Limit surface area

RSA Conference2016

Unique .onion addresses

Unique .onion addresses

The Tor Project - https://metrics.torproject.org/

RSAConference2016

On the deep, dark, mysterious web

- SecureDrop

- Blockchain.info*

- Facebook*

- OnionShare

- Instant messaging (Pond, Ricochet, XMPP)

RSAConference2016

Facebook's .onion with EV SSL cert

RSAConference2016

Researching the network and its users

- 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/

RSA Conference2016