

Privacy and usability implications of onion domains

February 18, 2018

Philipp Winter

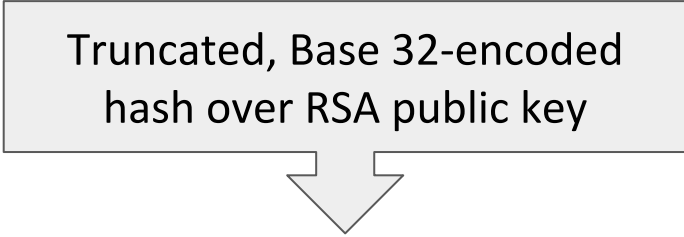
<http://expyuzz4wqqyqhjn.onion>

Special-use domain



`http://expyuzz4wqqyqhjn.onion`

Truncated, Base 32-encoded
hash over RSA public key



<http://expyuzz4wqqyqhjn.onion>

You are not limited to HTTP(S)

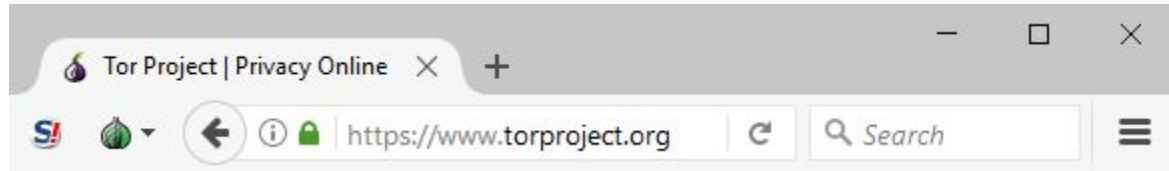
A grey rectangular box with a thin black border. Inside the box, the text "You are not limited to HTTP(S)" is written in a black, sans-serif font. From the bottom center of the box, a large, hollow, downward-pointing arrow extends downwards.

<http://expyuzz4wqqyqhjn.onion>

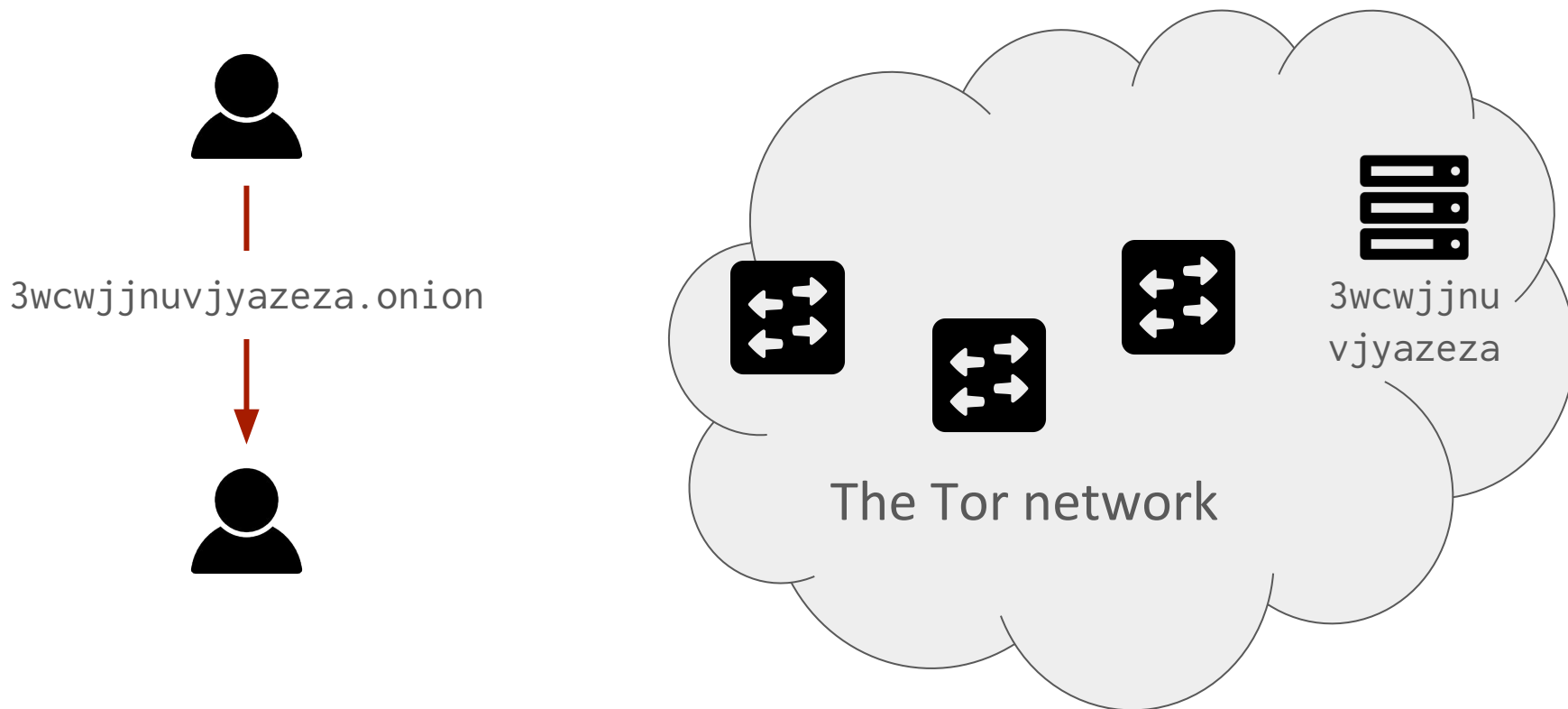
Onion service UI is designed to be seamless



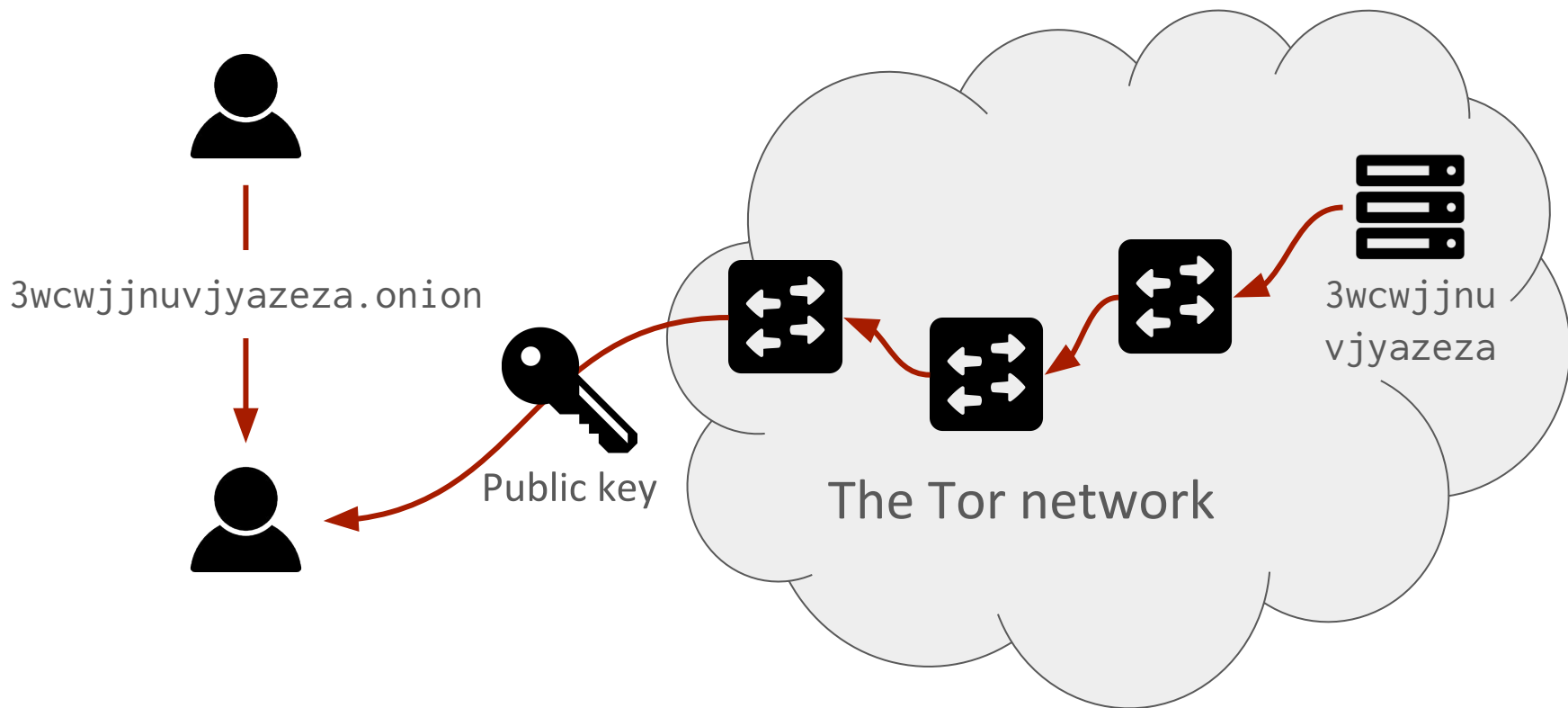
Onion service UI is designed to be seamless



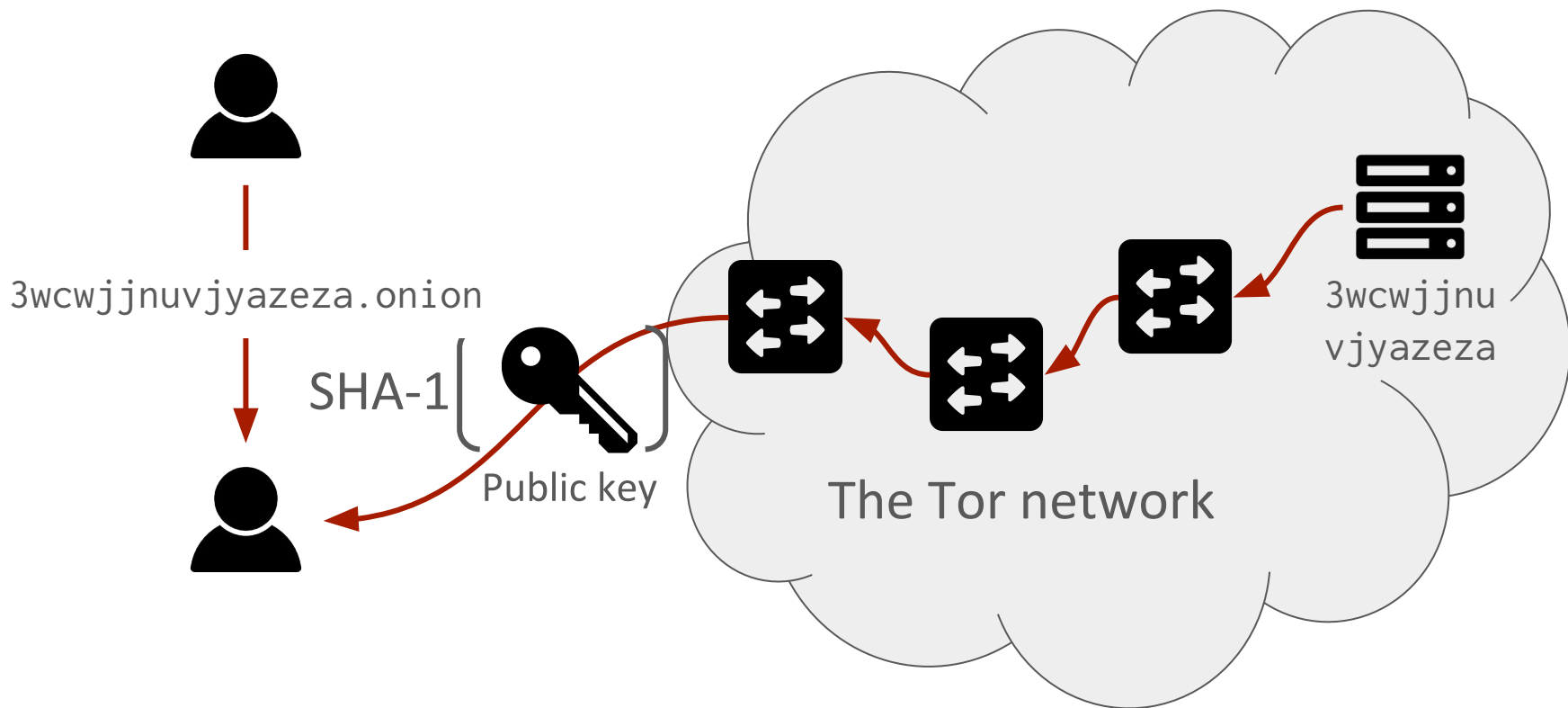
Onion services are self-authenticating



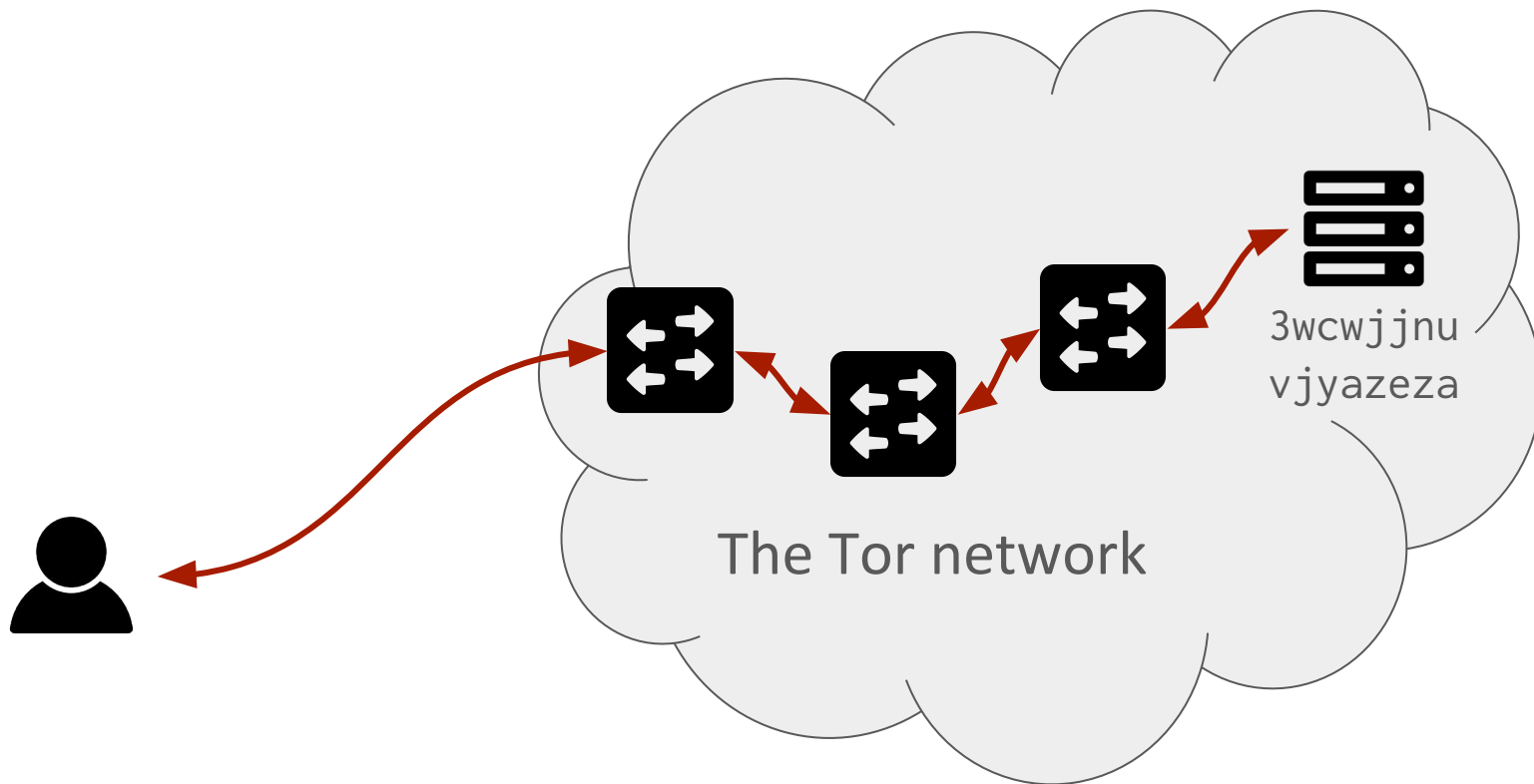
Onion services are self-authenticating



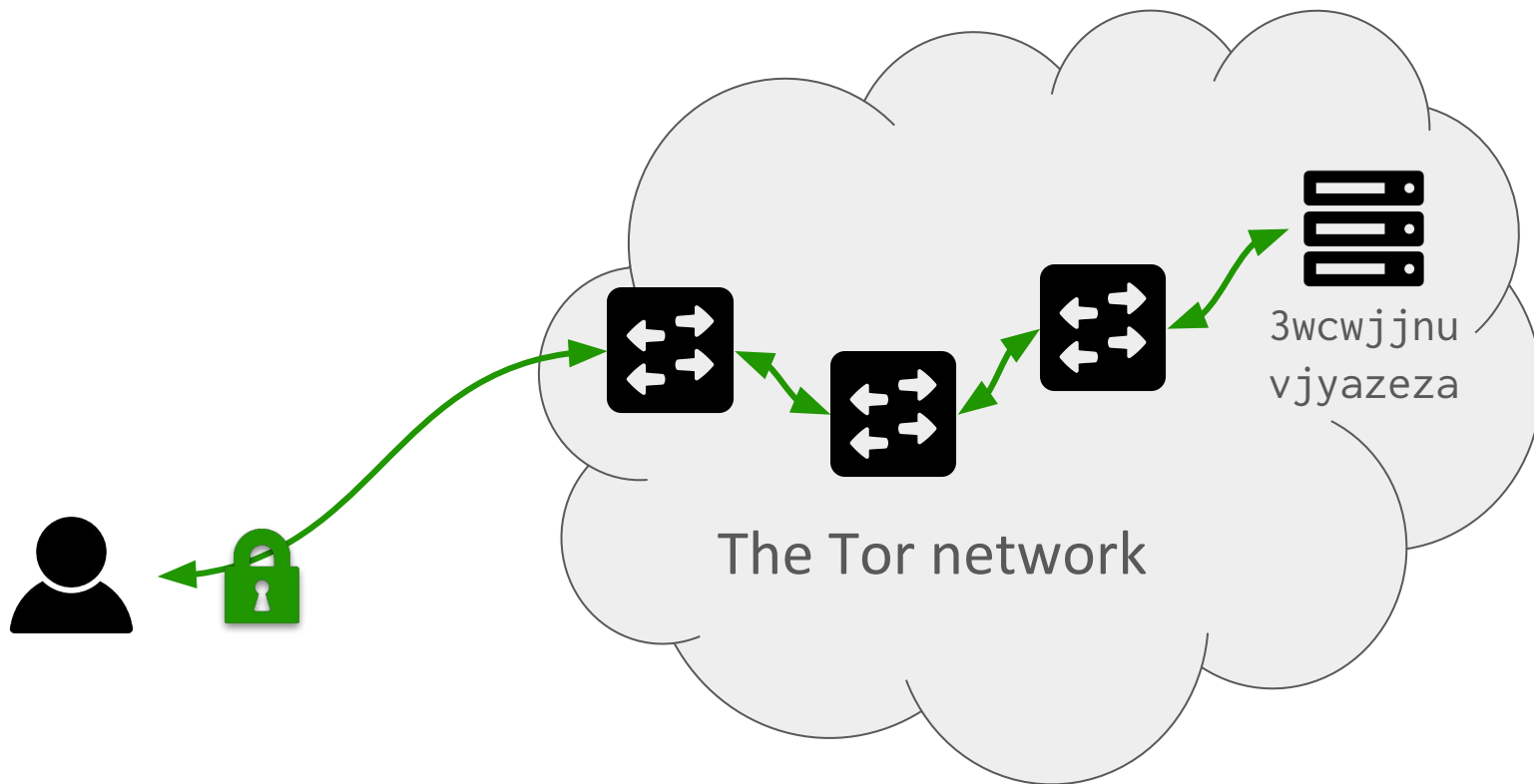
Onion services are self-authenticating



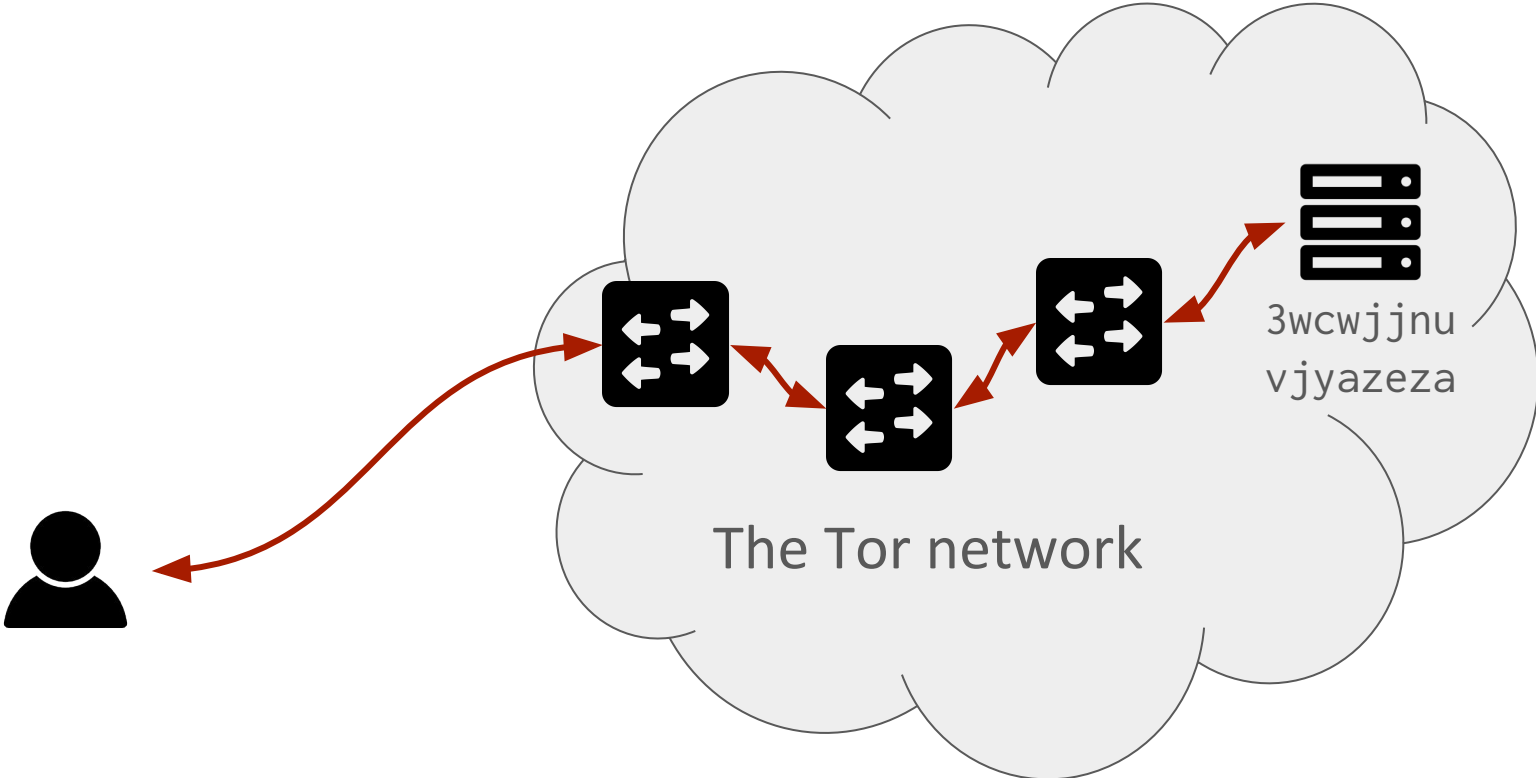
Onion services are end-to-end encrypted



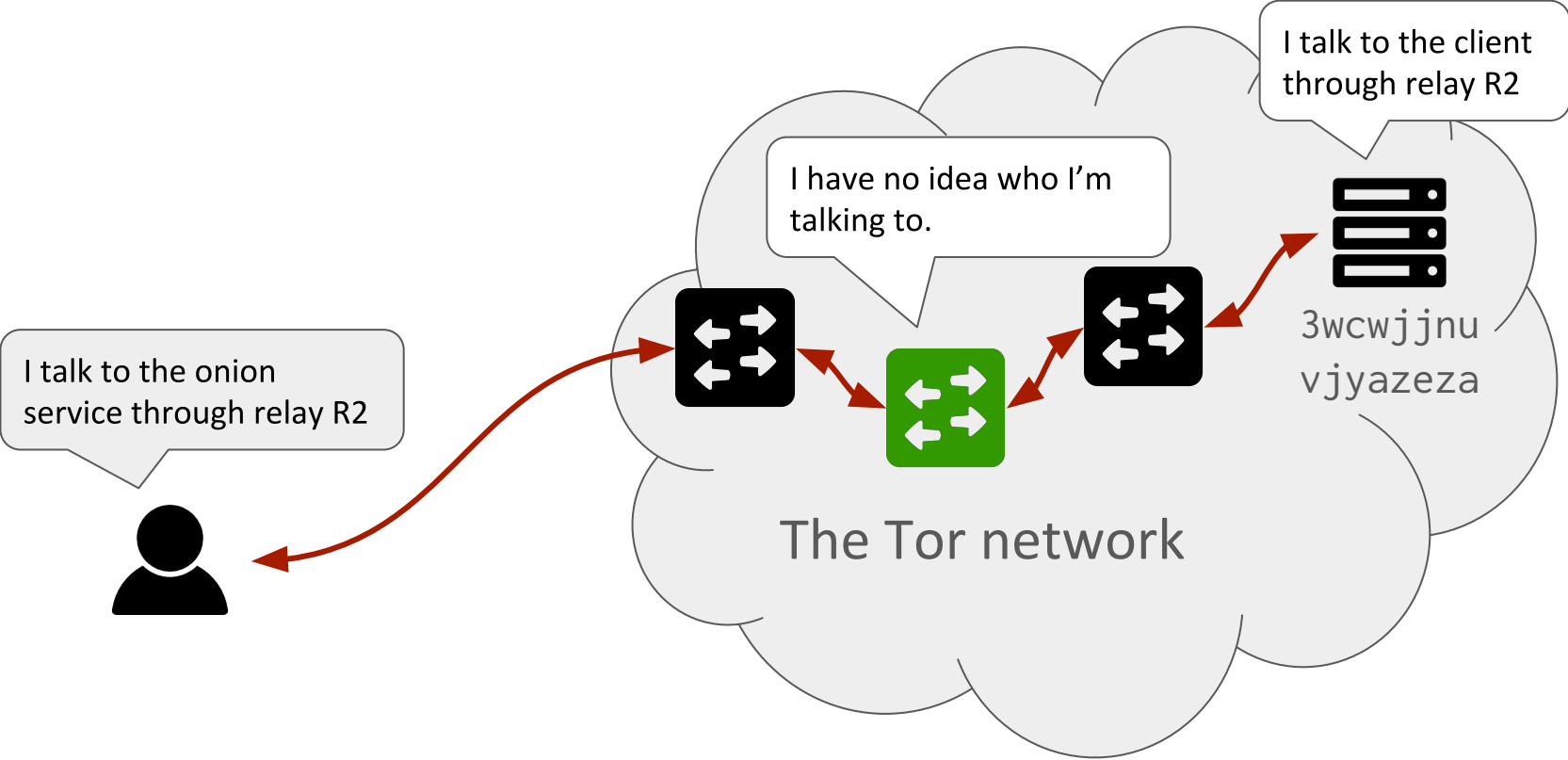
Onion services are end-to-end encrypted



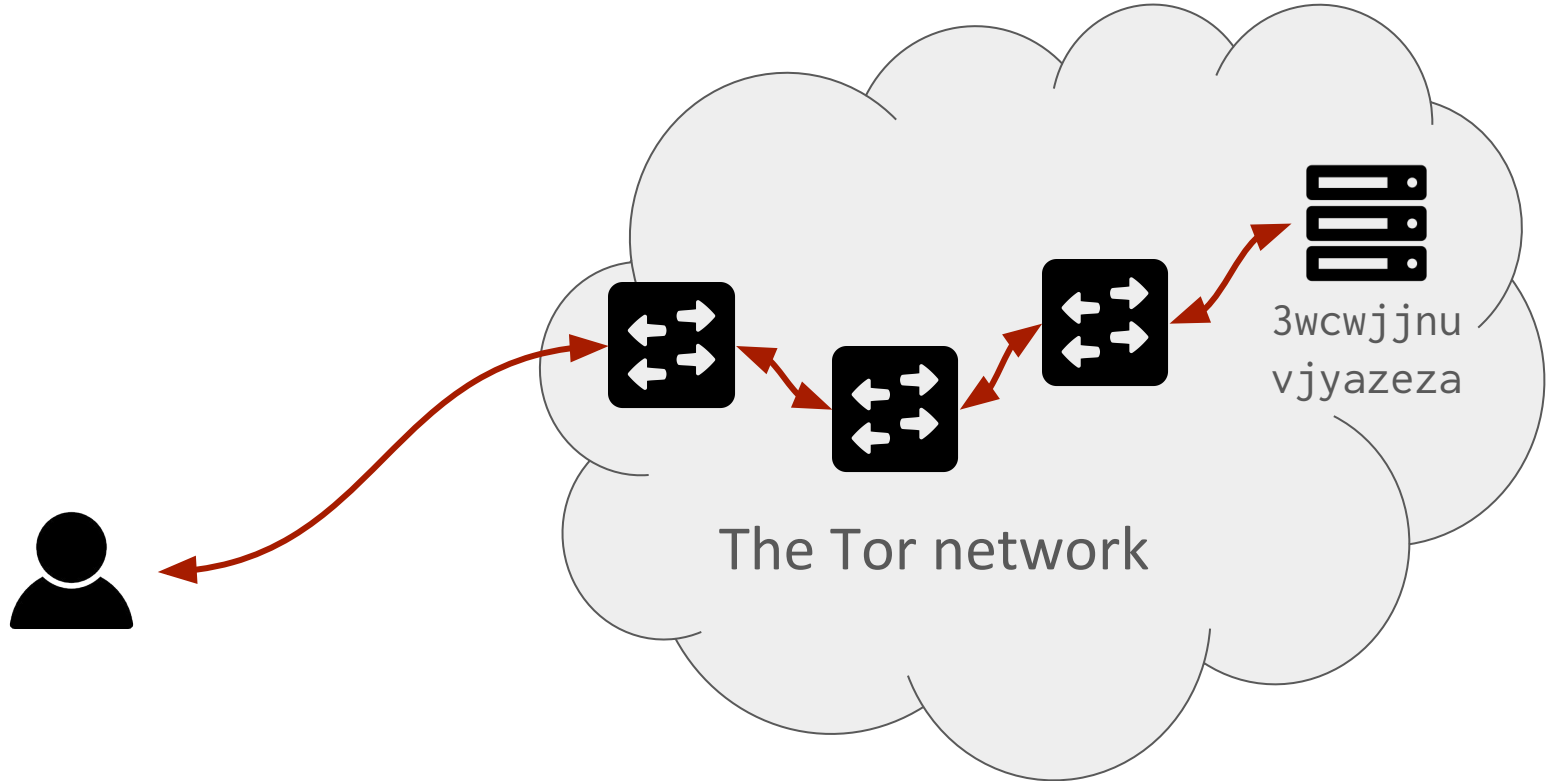
Both client and server are anonymous



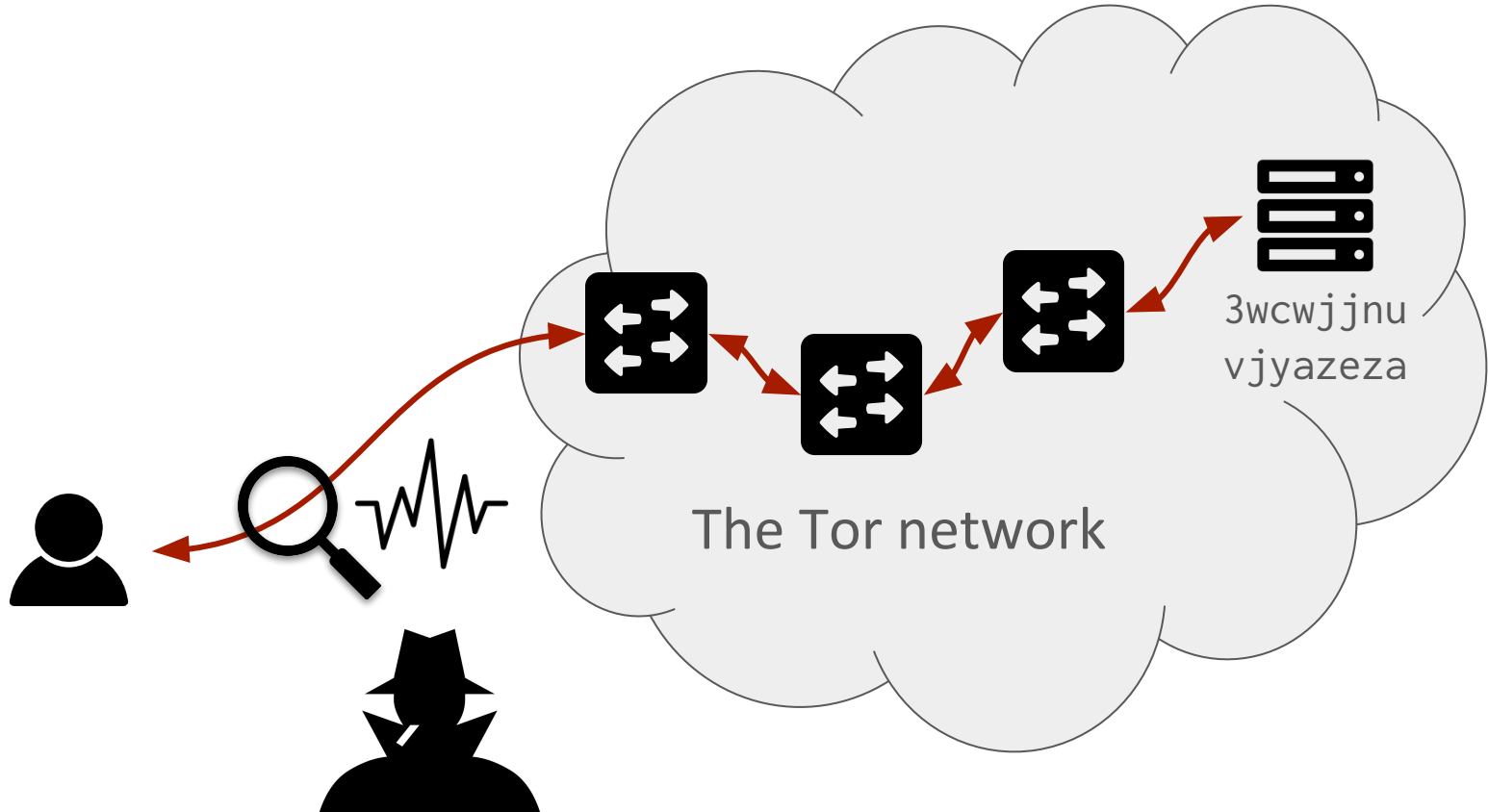
Both client and server are anonymous



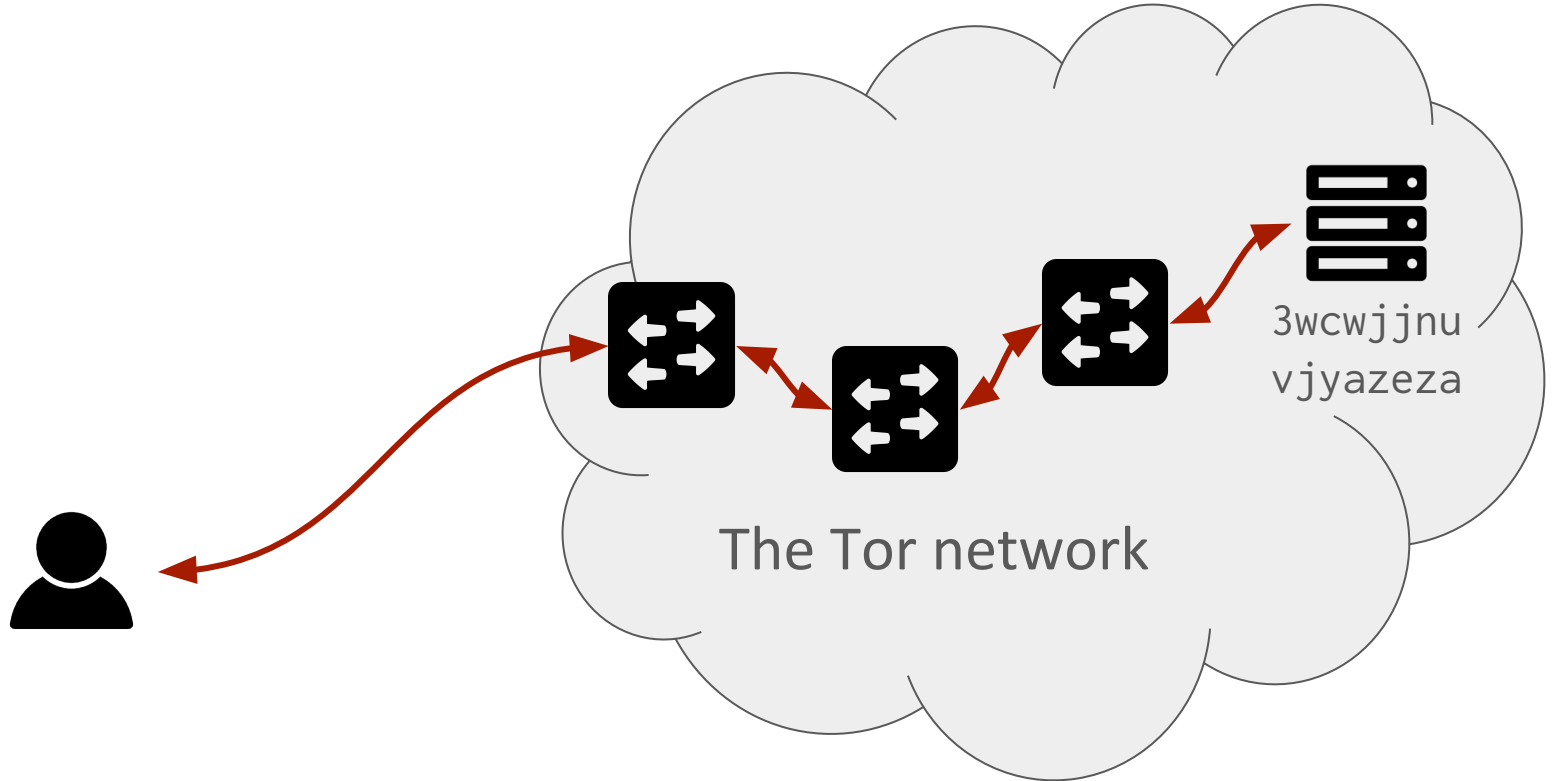
Traffic analysis is still possible



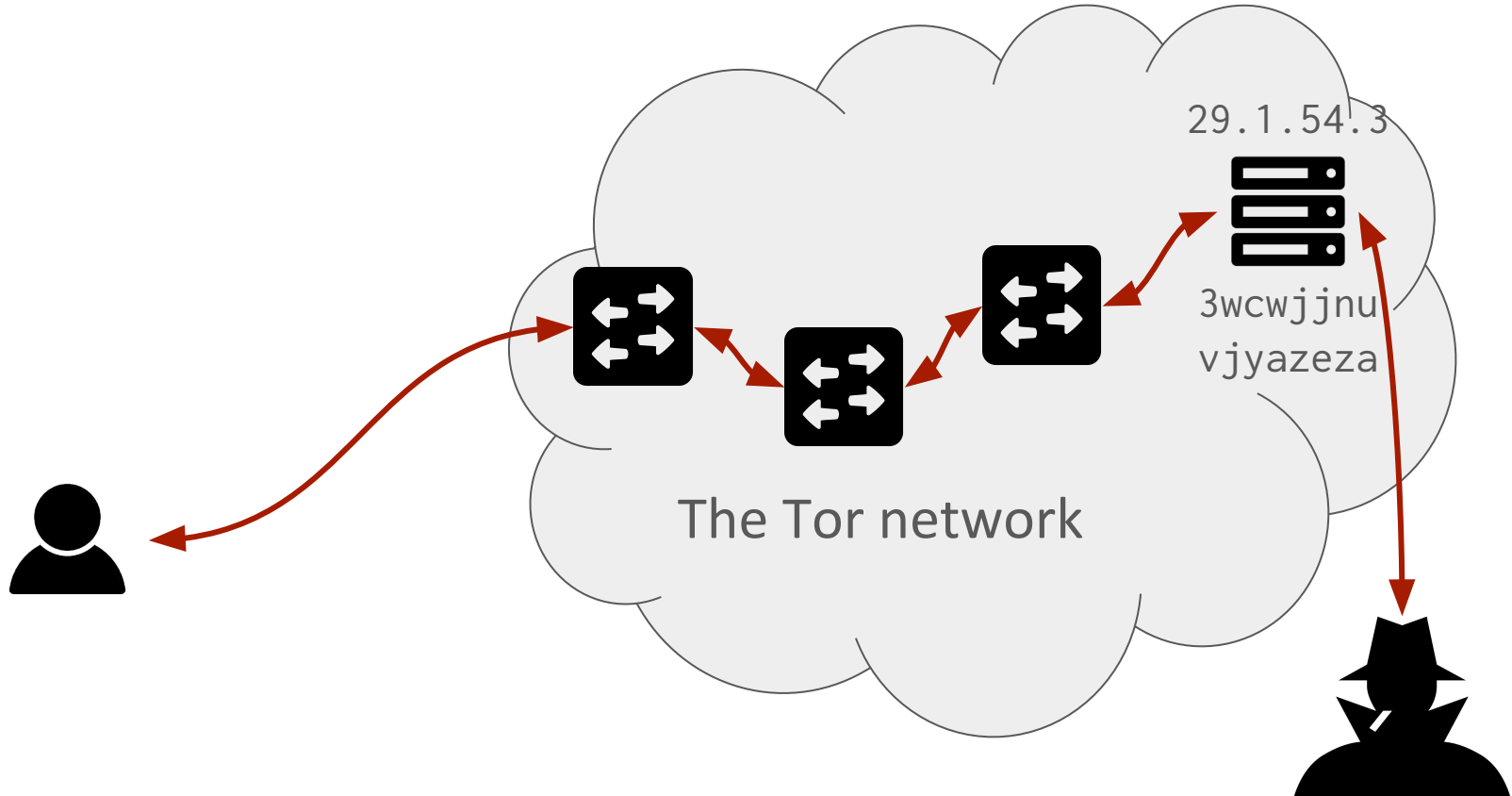
Traffic analysis is still possible



Configuration errors still an issue



Configuration errors still an issue



Onion services have usability issues

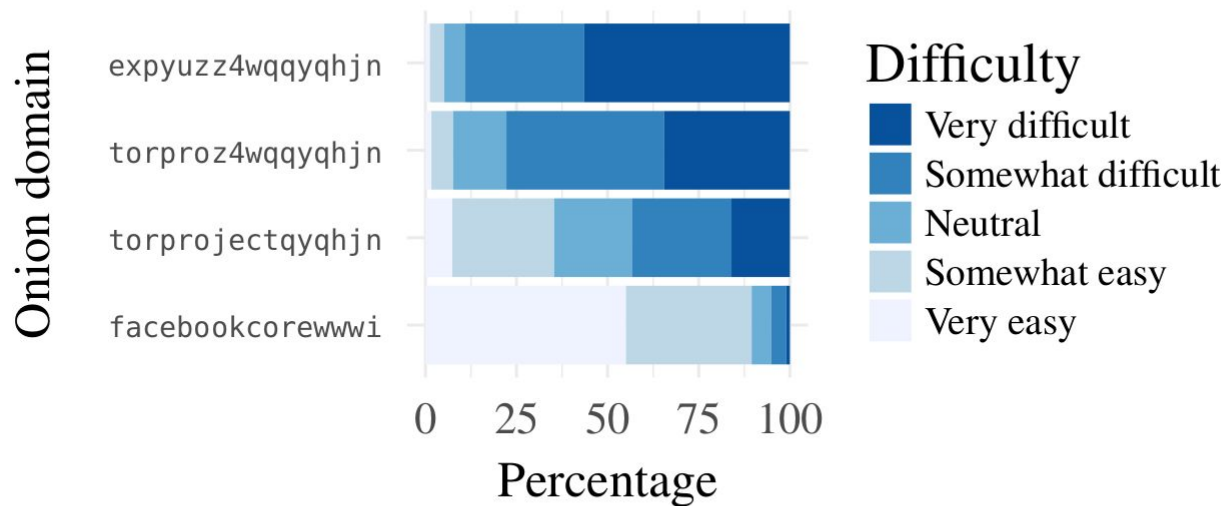
<http://expyuzz4wqqyqhjn.onion>

How do Tor users interact with onion services?

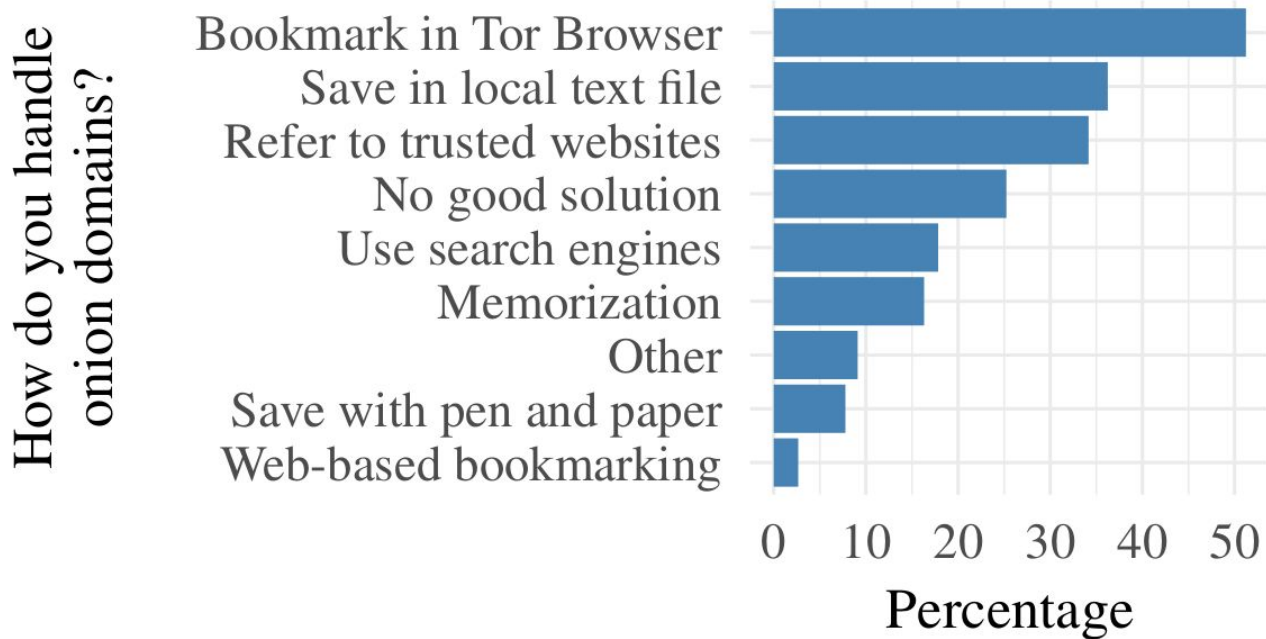
- Started a usability study in April 2017
- Interviewed **17 people** of diverse backgrounds
- Conducted online survey, attracting **828 responses**
- Preliminary data available online
 - <https://nymity.ch/onion-services/>



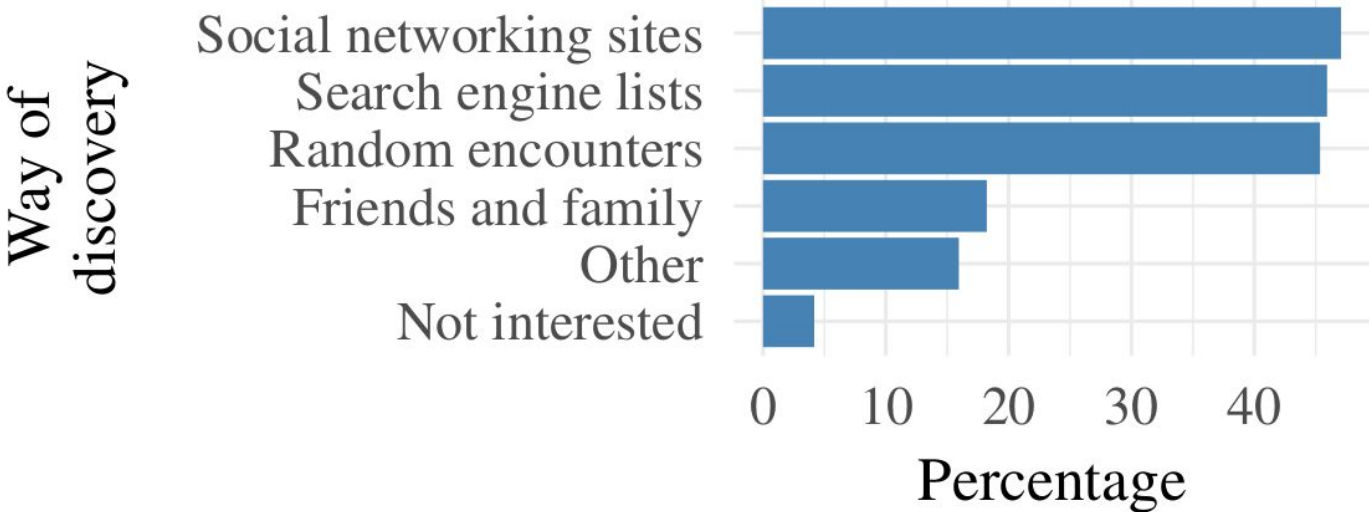
Onion domains are difficult to remember



Onion domain management is chaotic



Makeshift solutions ease onion domain discovery





The Red Cross Helped an Executive Get a Job at Save the Children After Forcing Him Out For Sexual Harassment

by Justin Elliott and Ariana Tobin, Jan. 25, 5 a.m. EST

A senior Red Cross official harassed a subordinate and was accused of raping another. The charity's now-general counsel David Meltzer praised him on his way out for "leadership" and "dedication."

Browse the archive:

Choose a month

SITES

ProPublica
ProPublica Illinois
The Data Store

SECTIONS

News Apps
Get Involved
The Nerd Blog
@ProPublica
Topics
Series

INFO

About Us
Board and Advisors
Officers and Staff
Jobs and Fellowships
Media Center
Reports
Impact
Awards
Corrections

POLICIES

Code of Ethics

FOLLOW

Newsletters
Podcast
iOS and Android
RSS Feed

MORE

Leak to Us
Steal Our Stories
Browse via Tor
Contact Us
Donate



The Red Cross Helped an Executive Get a Job at Save the Children After Forcing Him Out For Sexual Harassment

by Justin Elliott and Ariana Tobin, Jan. 25, 5 a.m. EST

A senior Red Cross official harassed a subordinate and was accused of raping another. The charity's now-general counsel David Meltzer praised him on his way out for "leadership" and "dedication."

Browse the archive:

Choose a month

SITES

- ProPublica
- ProPublica Illinois
- The Data Store

SECTIONS

- News Apps
- Get Involved
- The Nerd Blog
- @ProPublica
- Topics
- Series

INFO

- About Us
- Board and Advisors
- Officers and Staff
- Jobs and Fellowships
- Media Center
- Reports
- Impact
- Awards
- Corrections

POLICIES

- Code of Ethics

FOLLOW

- Newsletters
- Podcast
- iOS and Android
- RSS Feed

MORE

- Leak to Us
- Support Us
- Browse via Tor**
- Contact Us
- Donate

I wasn't aware that onion site search engines exist. It's been near impossible for me to find them so far.

Survey respondent

FRESH ONIONS



[INDEX](#) [FAQ](#) [JSON](#) [SRC](#) [STATS](#) -- 4316 certified fresh onions, 30 in the last 24 hours.

inc. never seen alive only (n/a genuine fake) show subdomains show fh default search title only match phrase

search: [Go >>>](#)

search for title, email, bitcoin addr or enter ".onion" domain for onion info. [\[G\]](#) means genuine, [\[F\]](#) means a fake clone site. domain status is [alive](#), [problems](#) or [down](#). showing 500 of 16009 results. [\[JSON\]](#)

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 ><(((°>

Onion	Title	Added	Visited At	Last Up
(i) smwujoefmv7q7mq4.onion	Index of /	5 hr	an hr	an hr
(i) pwr1zq6wijpxlvq6.onion	Home - Zion	5 hr	58 min	58 min
(i) oao75oxtg4p7nbon.onion		6 hr	an hr	an hr
(i) 7b6122nj5pvdpscs.onion		6 hr	an hr	6 hr
(i) 5hpxq3t2xe57c13t.onion	Welcome To Deep Web Coming Soon	6 hr	an hr	6 hr
(i) statv2gccyh7roto.onion	UnderMarket #StatusPage	6 hr	6 hr	6 hr
(i) d5b7er7mozxf5erw.onion		12 hr	12 hr	12 hr
(i) lnkfzecnslxo6jqc.onion	Rapture - Login	12 hr	12 hr	12 hr
(i) gfpysuzi2kwtctcy.onion	0xD3adC0d3	12 hr	3 hr	3 hr
(i) yuc6s7qghvnx4uk4.onion	This is My Dark Website	12 hr	9 hr	9 hr
(i) wfs3mpch63m7y3gh.onion	Zetsystemech	12 hr	an hr	an hr
(i) btctxivxusngb7ub.onion		12 hr	an hr	an hr
(i) archive7bgastbl4.onion	Archive7	13 hr	60 min	60 min
(i) uddofq2xrss7ybcx.onion		17 hr	5 hr	16 hr
(i) mn4xc37ubvydz7f2.onion	آراء حرة - قائمة المنشديات	17 hr	5 hr	5 hr
(i) fx3z257ruh2dmq2h.onion	Optimus Prime Team	17 hr	5 hr	5 hr
(i) bqpy5dr6xzmz66xa.onion	CriticalHackerSquad	17 hr	5 hr	5 hr
(i) 25o1s7lg36mtj4hf.onion	Site hosted by HostDanyyy hosting service Free anonymous webhosting	17 hr	10 hr	10 hr
(i) pjaopjqvjk6be4wz.onion	Dream Market PGP authentication	20 hr	3 hr	3 hr

Vanity onion domains

- Generate onion domains until hash resembles desired string
- The good:
 - Hints at onion service content
- The bad:
 - Breeds false sense of security
 - Economically unfair

propub3r6espa33w.onion

nytimes3xbfgragh.onion

facebookcorewwi.onion

protonirockerxow.onion

I only memorize the first part of the domain.

Survey respondent

I understand vanity onion domains are a sign of the weakness of the hash algorithm used by Tor.

Survey respondent

These people who created their onion name using scallion or other tools should notice that other people can make [the] same private key.

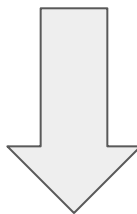
Survey respondent

Making onion domains more usable

- Have Tor Browser help with **encrypted bookmarks**
- Make it easier for site foo.com to announce its onion service
- Allow onion service operators to **opt-in to publishing mechanism**
- Some UI elements are **misunderstood**
- Better documentation and education

Next-generation onion domains are longer

expyuzz4wqqyqhjn.onion



gff4ixq3takworeuhkubzz4xh2ulytoct4xrpazkiykhupa1qlo53ryd.onion

Thanks for listening!

- Project information: <https://nymity.ch/onion-services/>
- Contact: phw@nymity.ch
- Thanks to The Tor Project, Tor community, and collaborators!



Annie



Laura



Marshini



Nick