How Do Tor Users Interact With Onion Services?

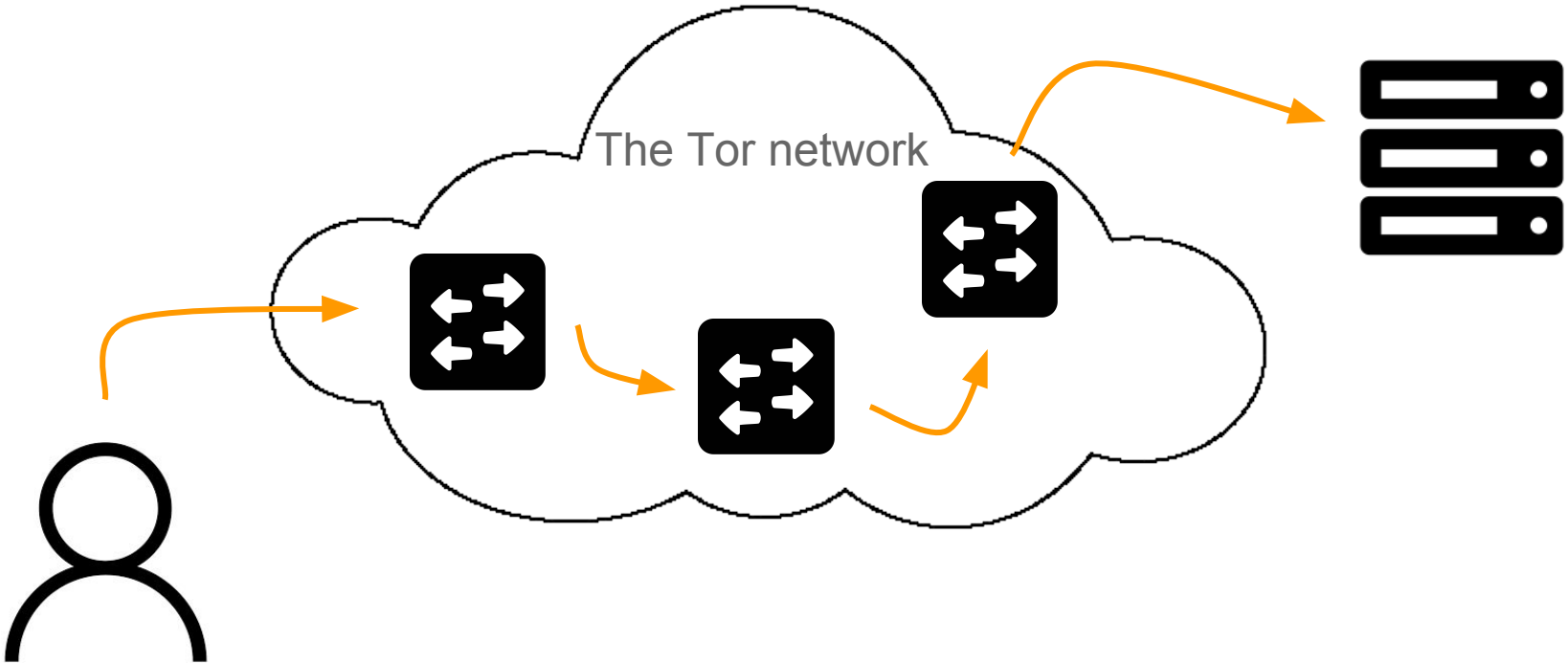




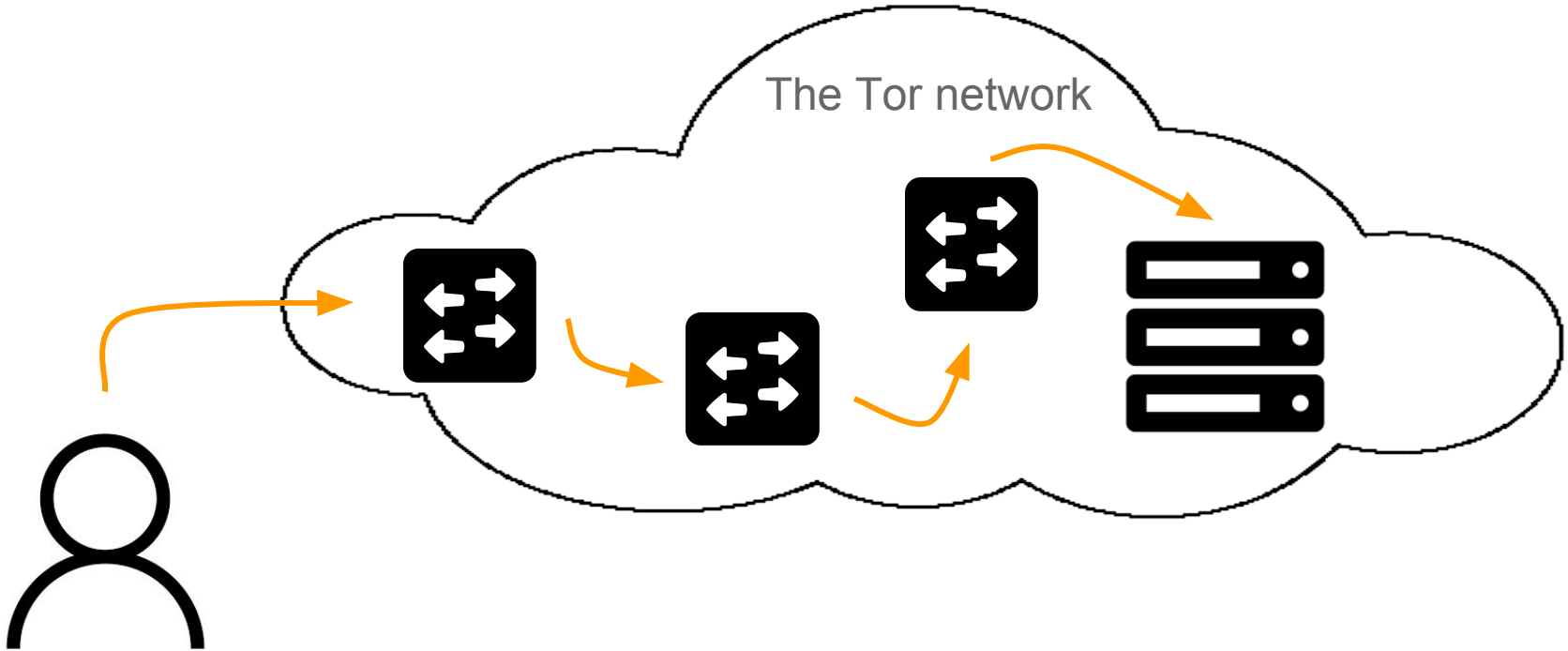

Philipp Winter, **Annie Edmundson**, Laura Roberts, Agnieszka Dutkowska-Zuk, Marshini Chetty, Nick Feamster

USENIX Security Symposium
15 August 2018

Tor is a Decentralized Anonymity Network



Onion Services Provide Server Anonymity



How Do Users Interact with Onion Services?

- What are users' mental models of onion services?
- How do users use and manage onion services?
- What are the challenges of using onion services?

Main Findings

Despite extra security and privacy properties of onion services, many users are confronted with usability issues

- Discovering the existence of onion services
- Managing and remembering onion domains
- Susceptibility to phishing attacks

We can learn from the issues users have encountered to implement design improvements

Overview

1. **Onion Services Background + Features**
2. Methods
3. Results
    a. Onion Sites Discovery
    b. Vanity Domains
    c. Verifying Onion Sites
4. Future Directions & Conclusions

http://expyuzz4wqqyqhjn.onion

Special-use domain

http://expyuzz4wqqyqhjn.onion

Truncated, base 32-encoded hash over RSA public key

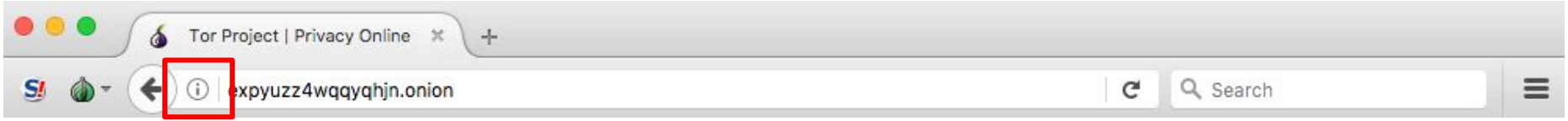
http://expyuzz4wqqyqhjn.onion

Not limited to HTTP(S)

http://expyuzz4wqqyqhjn.onion

Onion Service UI is Designed to be Seamless

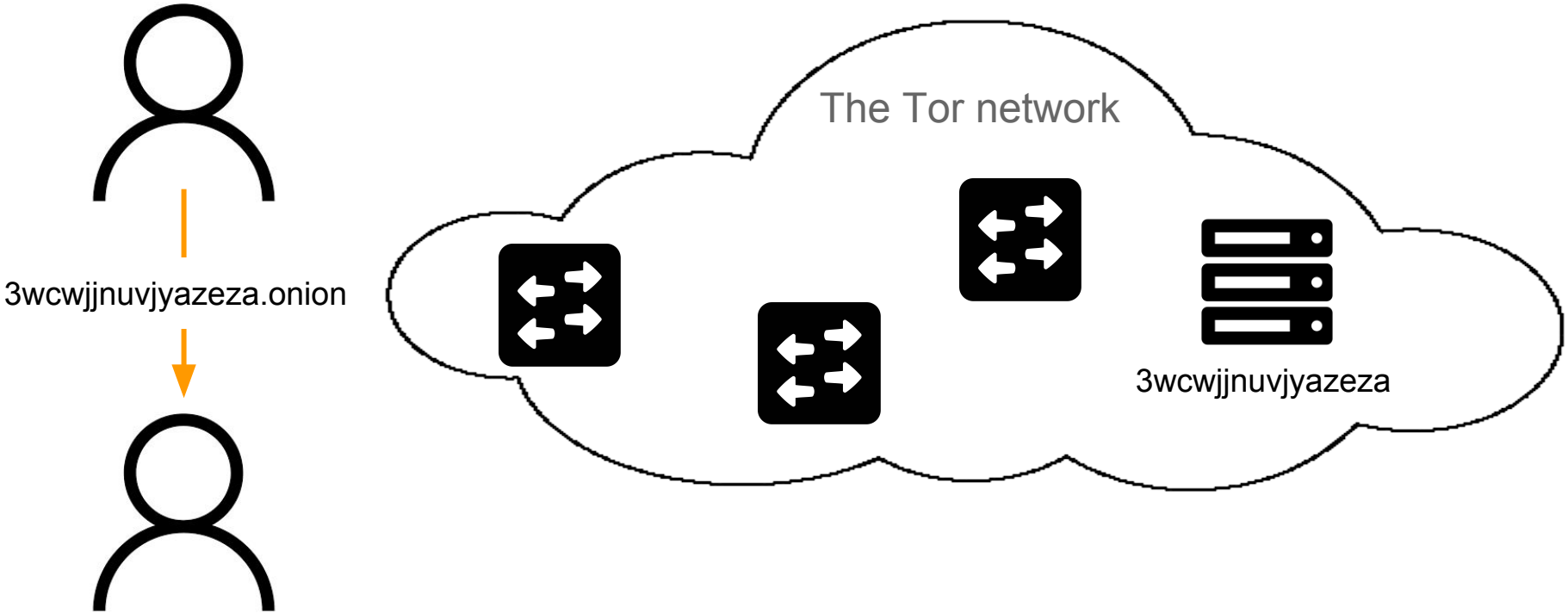
Onion Service UI is Designed to be Seamless



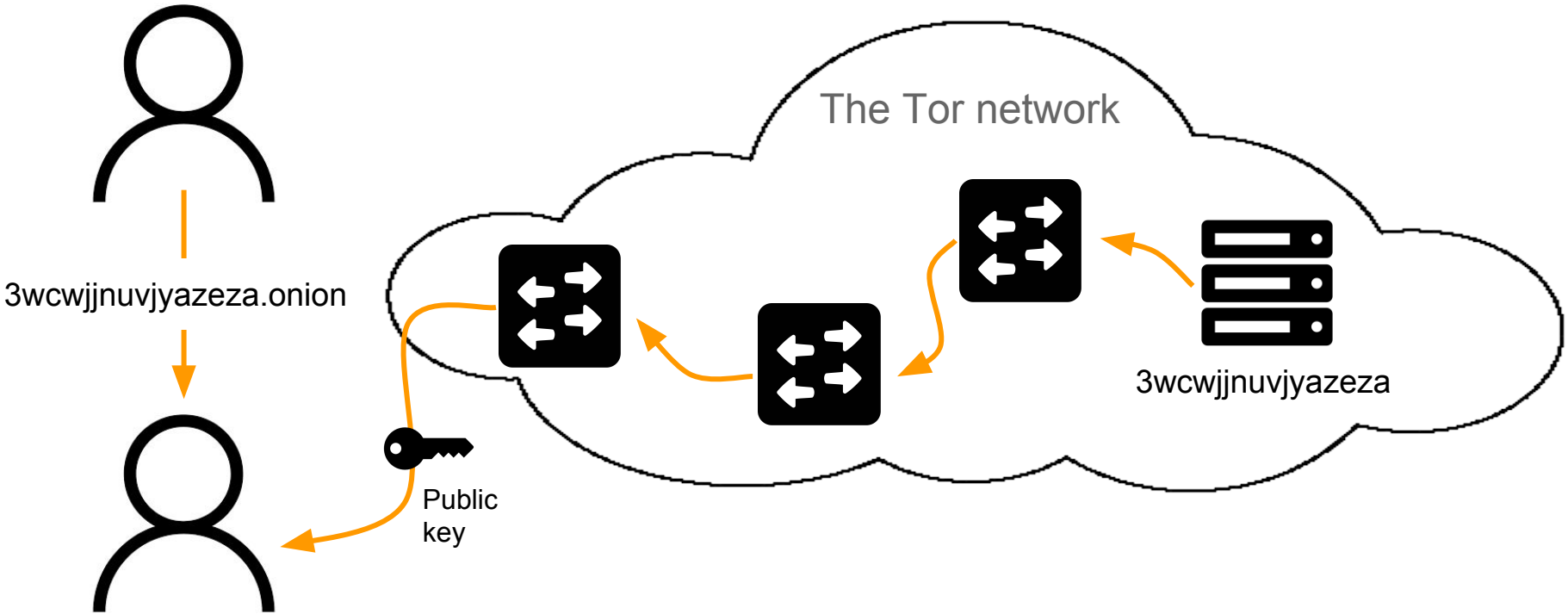
Onion Service UI is Designed to be Seamless

Onion Service UI is Designed to be Seamless

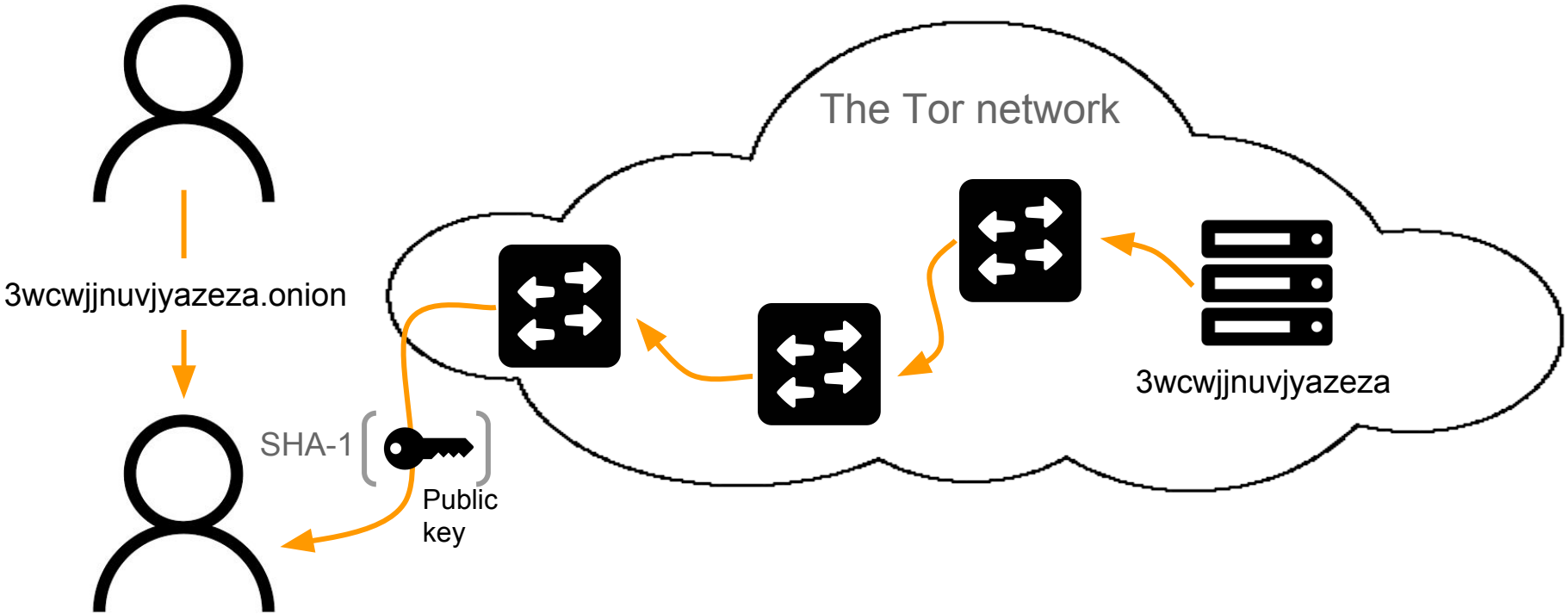
Onion Services are Self-authenticating



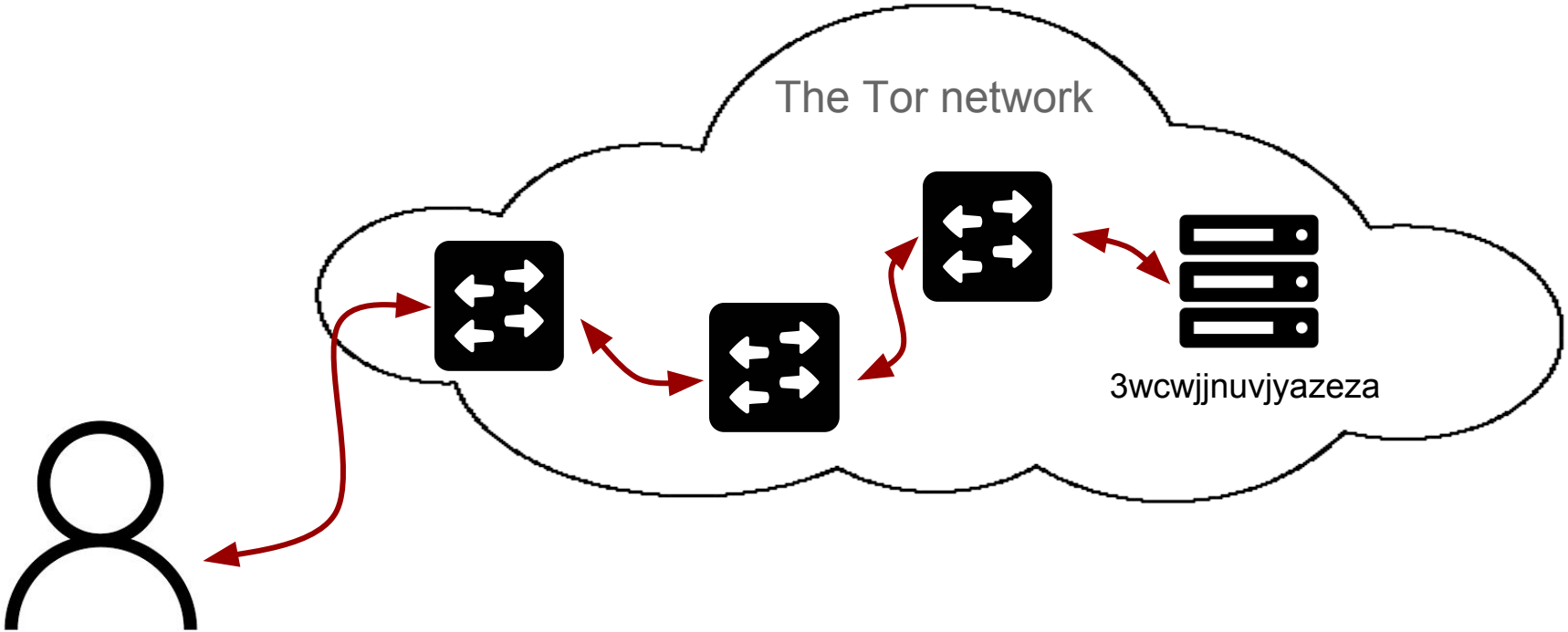
Onion Services are Self-authenticating



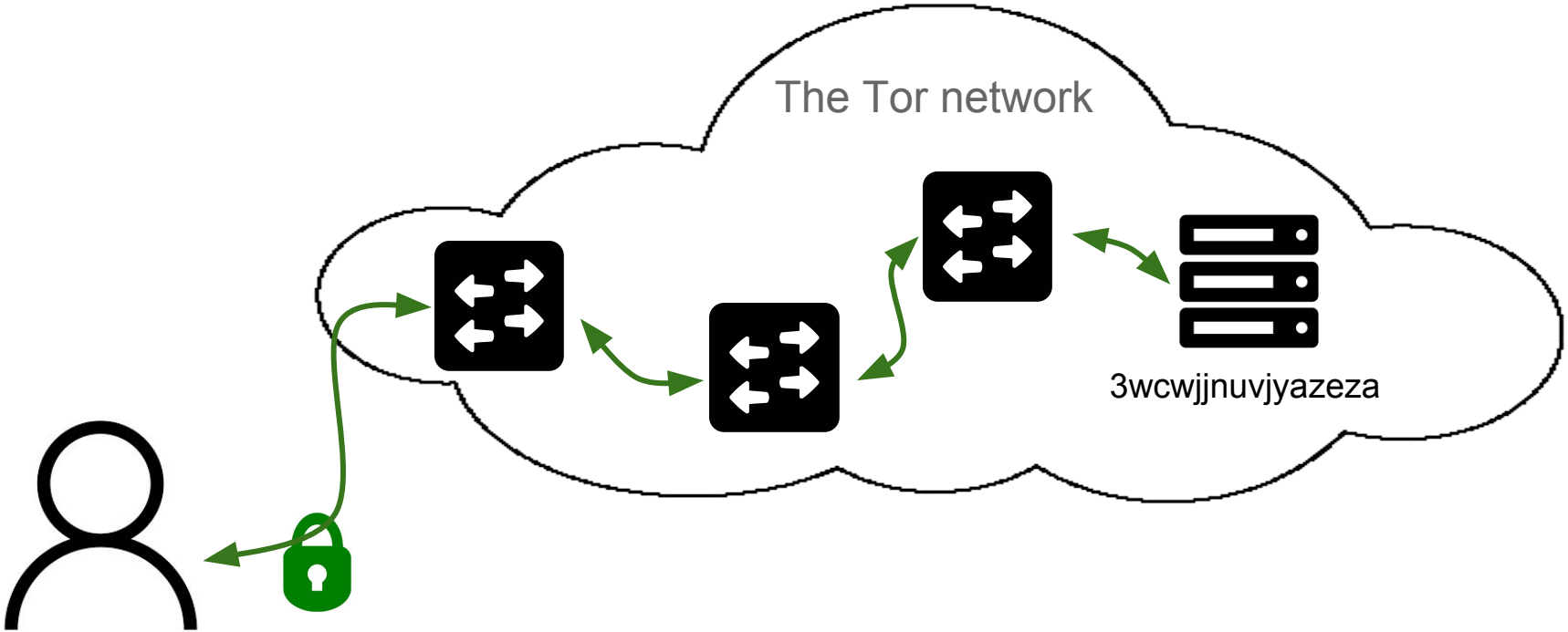
Onion Services are Self-authenticating



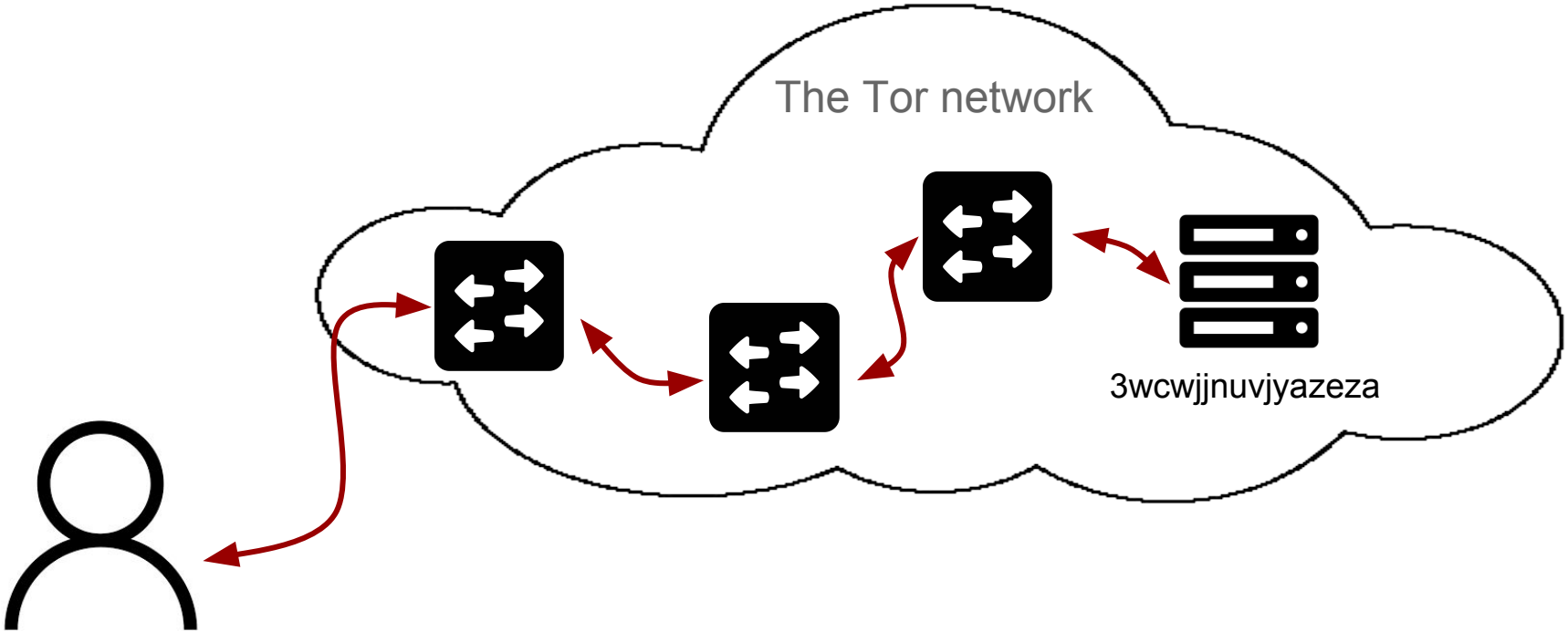
Onion Services are End-to-end Encrypted



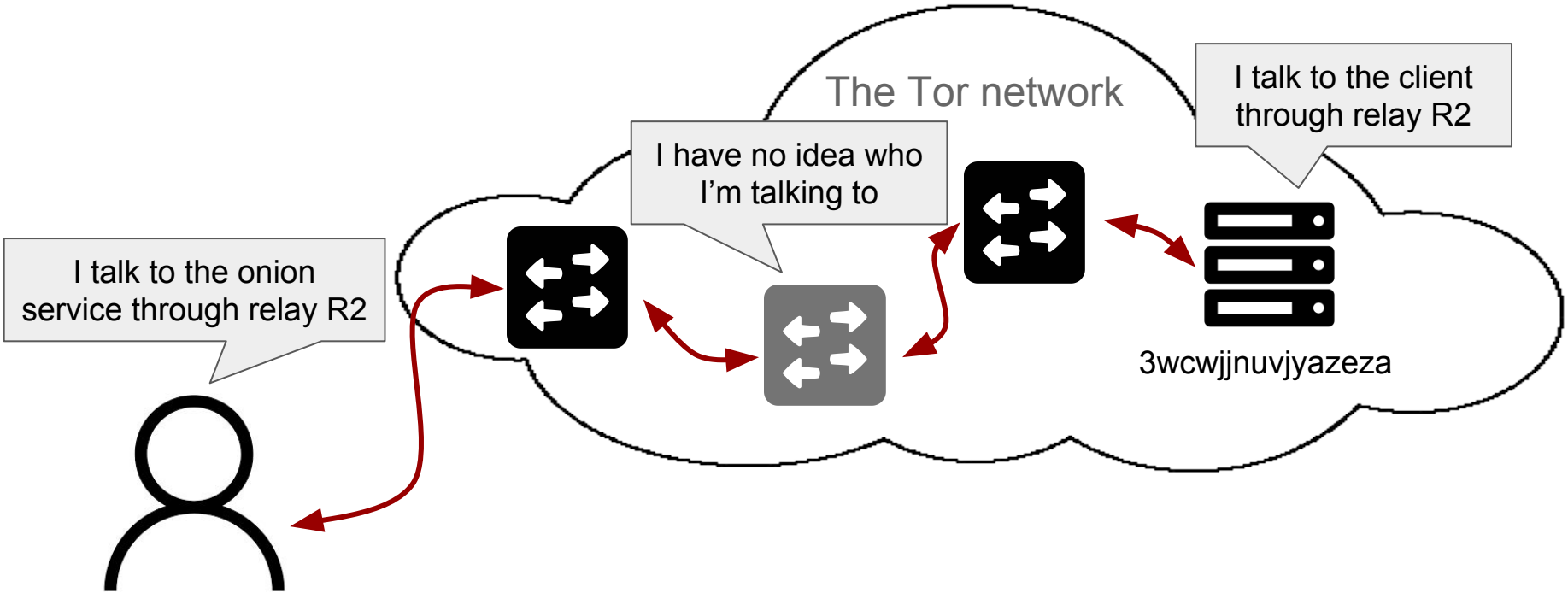
Onion Services are End-to-end Encrypted



Both Client and Server are Anonymous



Both Client and Server are Anonymous



While onion services provide anonymity benefits, they are not perfect.

- Susceptible to traffic analysis attacks
- Configuration errors
- Usability issues

Overview

1. Onion Services Background + Features
2. **Methods**
3. Results
    a. Onion Sites Discovery
    b. Vanity Domains
    c. Verifying Onion Sites
4. Future Directions & Conclusions

How Do Users Interact with Onion Services?

- What are users' mental models of onion services?
- How do users use and manage onion services?
- What are the challenges of using onion services?

How Do Users Interact with Onion Services?

How Do Users Interact with Onion Services?

Mixed-method user study

Interviews

- N=17
- Diverse backgrounds
- Exploratory

Survey

DNS B Root Data

How Do Users Interact with Onion Services?

Mixed-method user study

Interviews

- N=17
- Diverse backgrounds
- Exploratory

Survey

- N=517
- 49 questions (mix of open-ended and closed-ended)
- 4 attention checks

DNS B Root Data

How Do Users Interact with Onion Services?

Mixed-method user study

Interviews

- N=17
- Diverse backgrounds
- Exploratory

Survey

- N=517
- 49 questions (mix of open-ended and closed-ended
- 4 attention checks

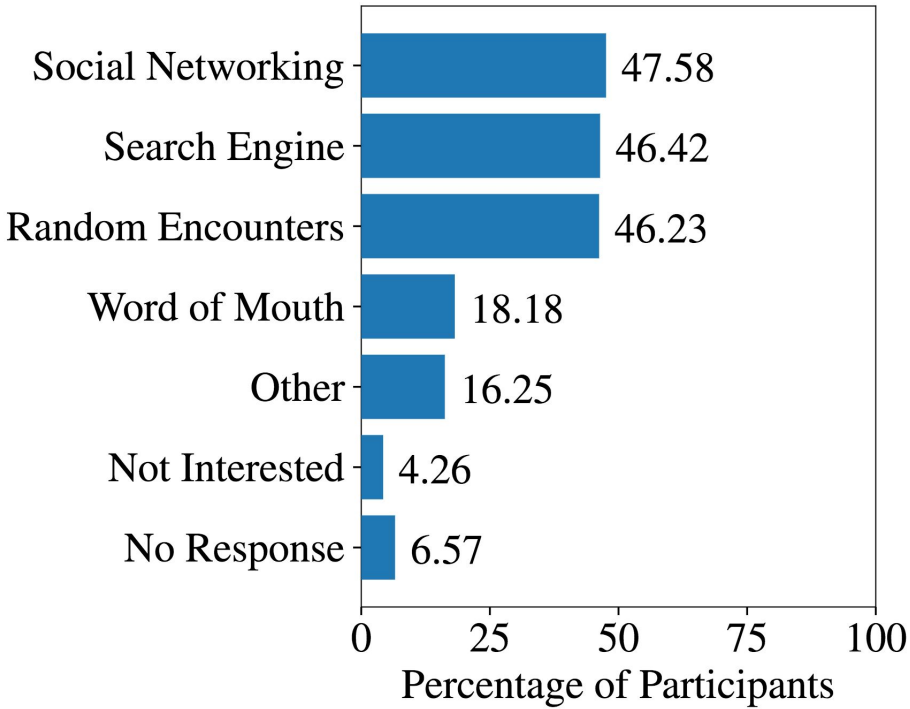
DNS B Root Data

- ~2 days of data
- Filtered correctly formatted .onion domains
- 15,471 leaked onion domains

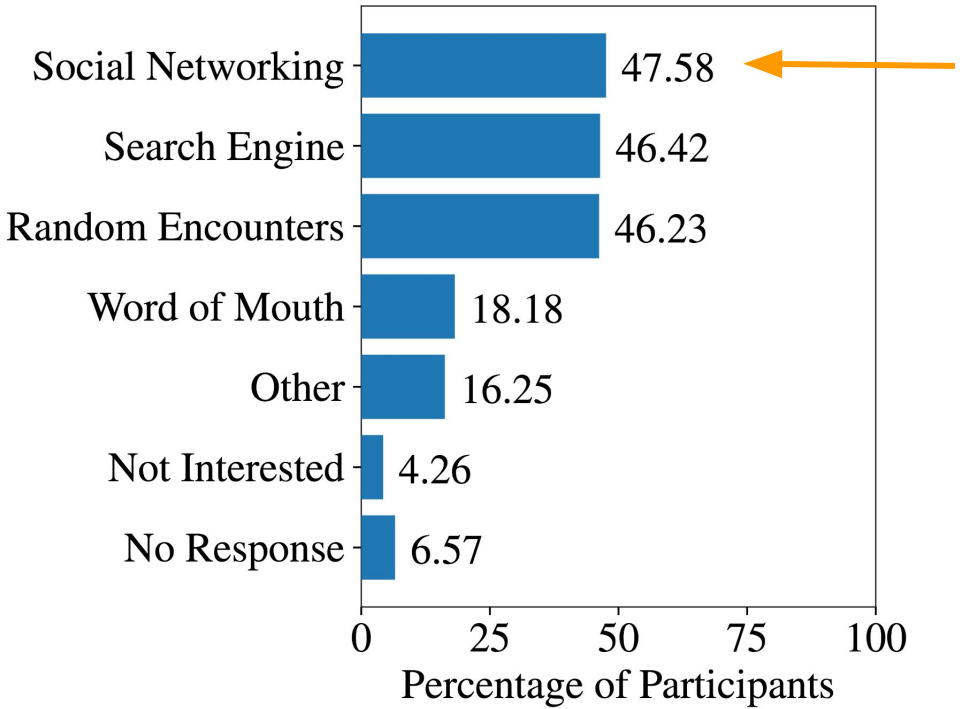
Overview

1. Onion Services Background + Features
2. Methods
3. **Results**
   a. **Onion Sites Discovery**
   b. **Vanity Domains**
   c. **Verifying Onion Sites**
4. Future Directions & Conclusions

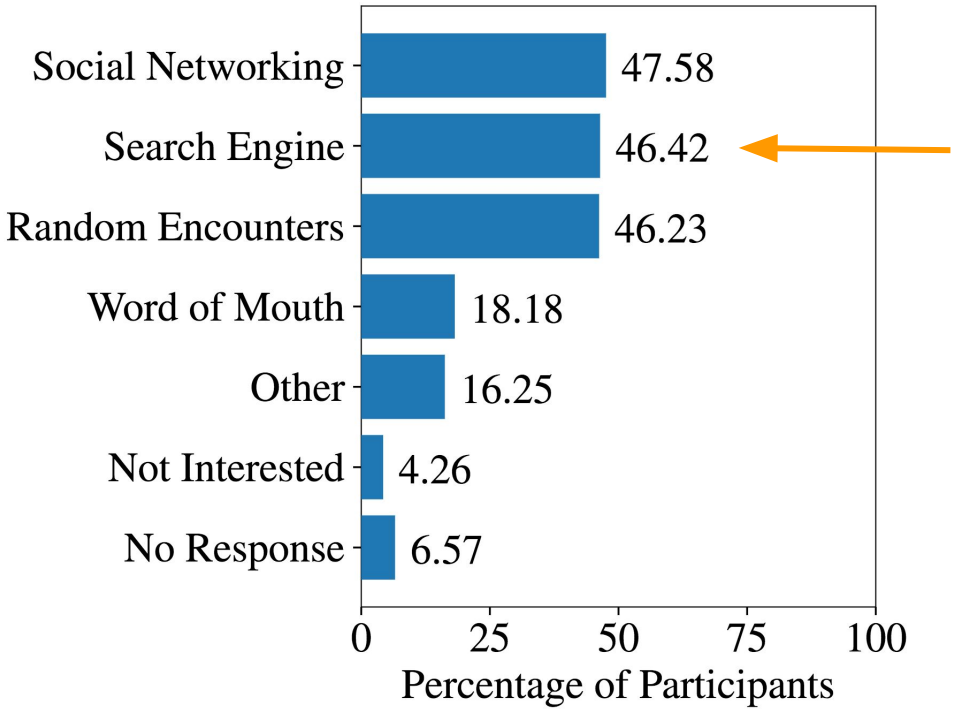
Makeshift Solutions Ease Onion Discovery



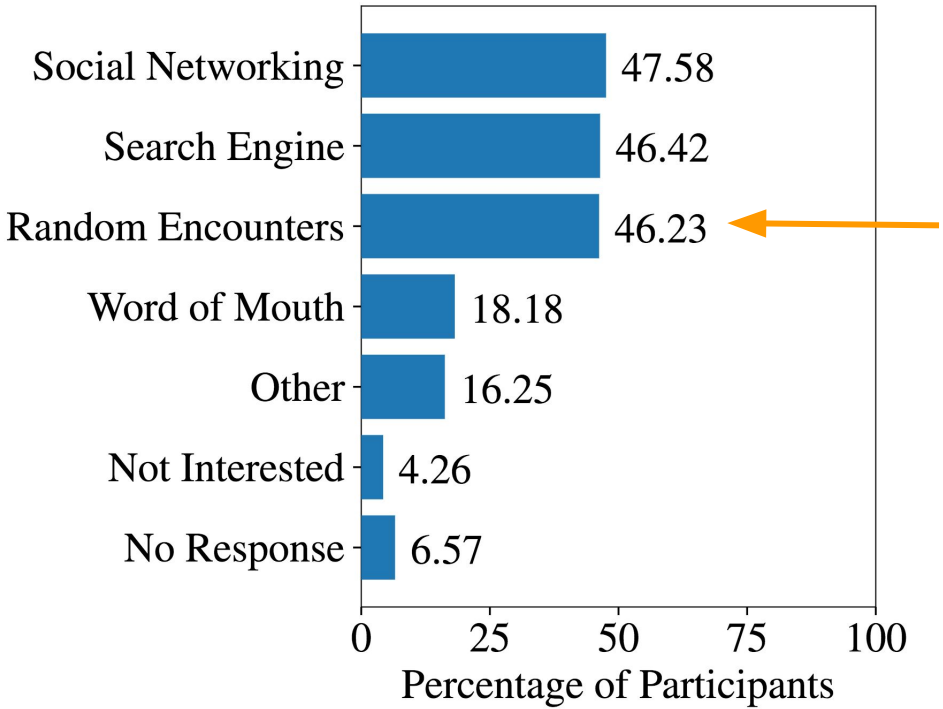
Makeshift Solutions Ease Onion Discovery



Makeshift Solutions Ease Onion Discovery



Makeshift Solutions Ease Onion Discovery

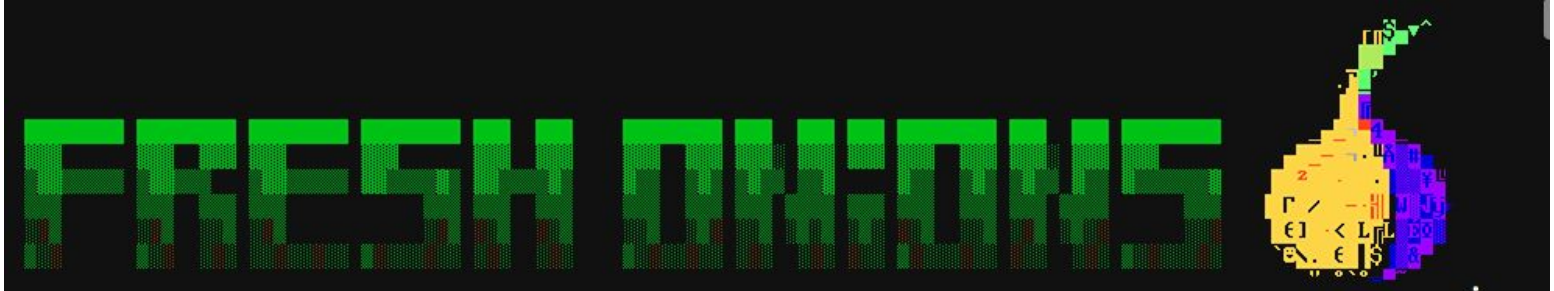


Browse the archive:

Choose a month

Browse the archive:

Choose a month



INDEX FAQ JSON SRC STATS -- 50 certified fresh onions, 0 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 19361 results. [JSON]

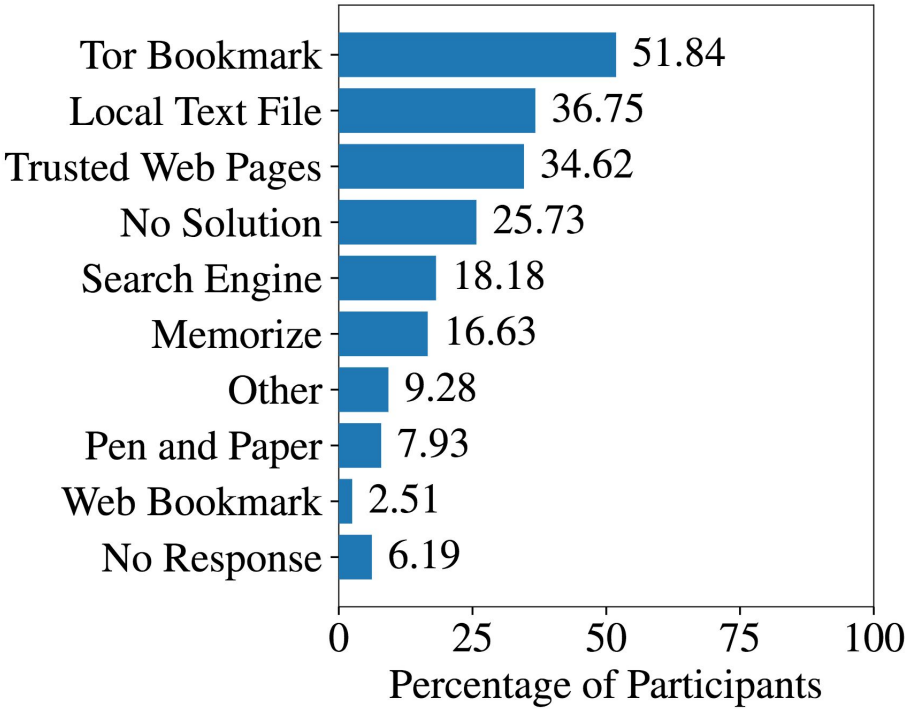
``.,,,.´``. 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 ><(((°>

	Onion	Title	Added
(i)	kx5p6btdjxthhvqx.onion		13 min
(i)	kuchuzvtvbgmbdg7.onion		an hr
(i)	n44kt6fn3khcmvmj.onion	Dark Net Guns - Guns on the dark web	an hr
(i)	ksvige6vjlnwoikd.onion		3 hr
(i)	sz6pub2csketddgu.onion	xPlay - hosting service for porn videos	4 hr
(i)	ai5gpgsxxufz4y7g.onion	黑暗之首	4 hr
(i)	patr4lljvktjcmnn.onion	Radioafición electricidad y electrónica - Página principal	4 hr
(i)	domamuwmjouwbbul.onion	I2P Anonymous Webserver	4 hr

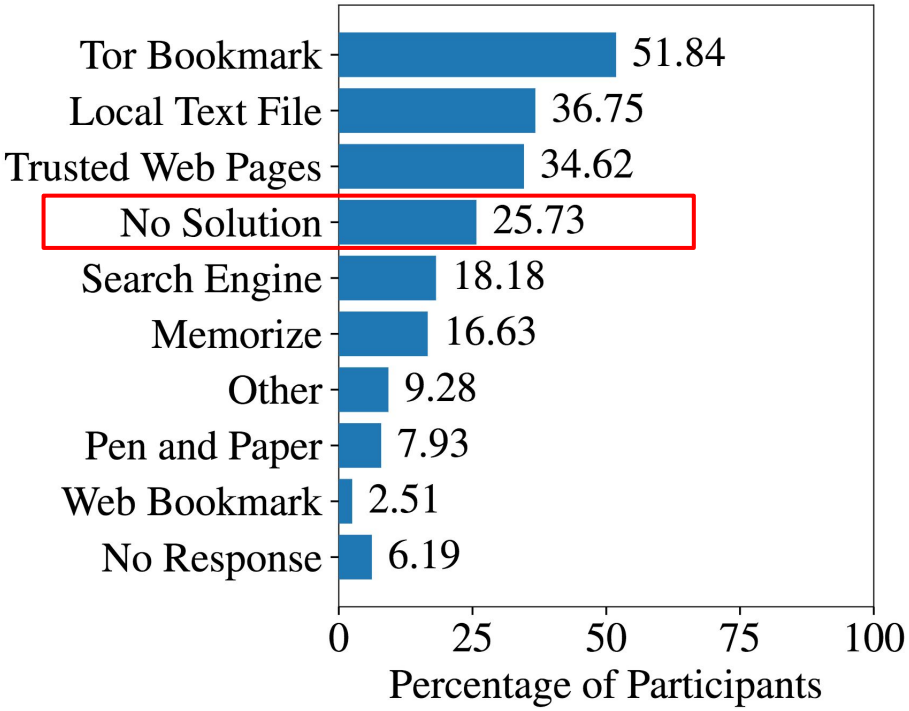
I wasn't aware that onion site search engines exist. It's been near impossible for me to find them so far.

Survey Respondent (S195)

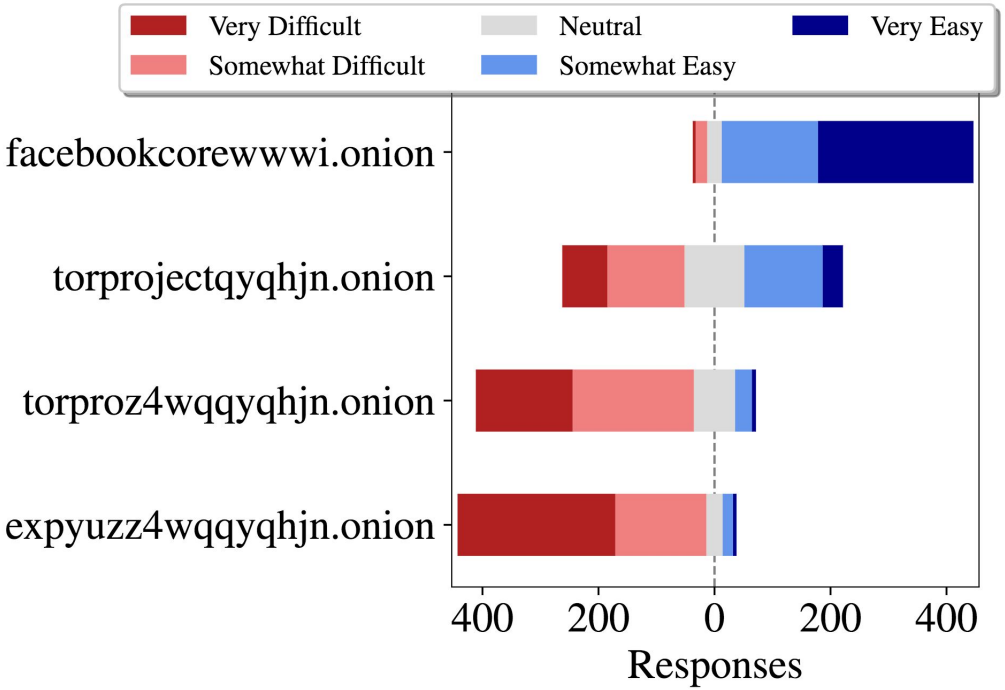
Onion Domain Management is Chaotic



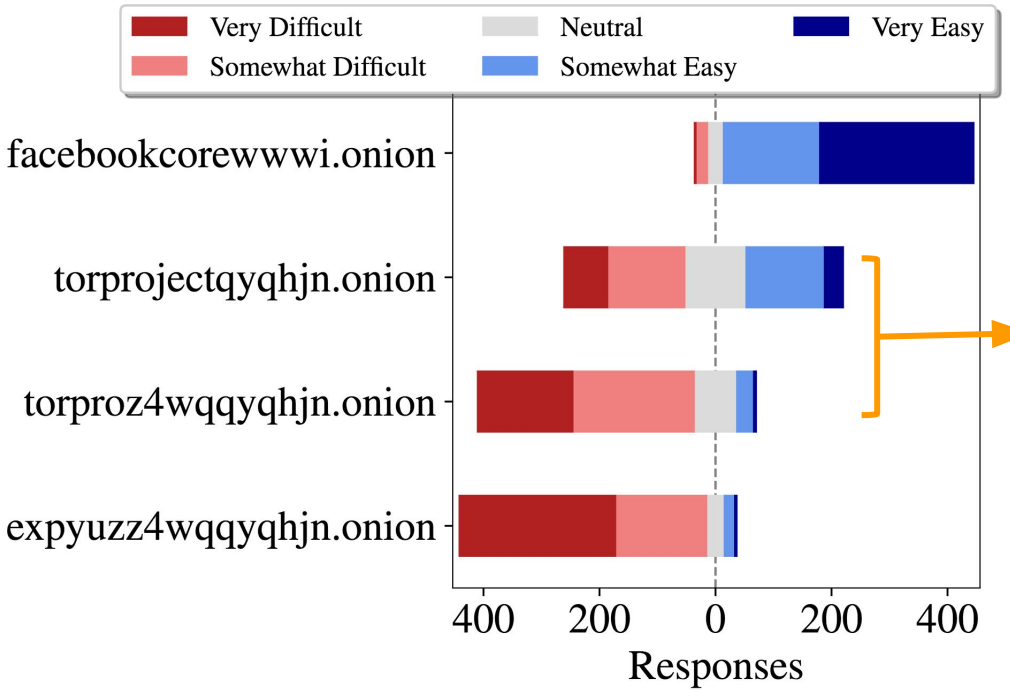
Onion Domain Management is Chaotic



Onion Domains are Difficult to Remember



Onion Domains are Difficult to Remember



Meaningful prefixes appea
to make remembering
easier

Phonetic pronunciation plays a large part in how I remember onions.

Survey Respondent (S46)

Vanity Onion Domains

propub3r6espa33w.onion

nytimes3xbfgragh.onion

facebookcorewwwi.onion

protonirockerxow.onion

Vanity Onion Domains

propub3r6espa33w.onion

nytimes3xbfgragh.onion

facebookcorewwwi.onion

protonirockerxow.onion

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

I only memorize the first part of the domain.

Survey Respondent (S96)

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

Survey Respondent (S454)

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 (S552)

Onion Lookups Suggest Typos or Phishing

`hydraruzxpnew4af.onion`

`hydraruzxpnew3af.onion`

Onion Lookups Suggest Typos or Phishing

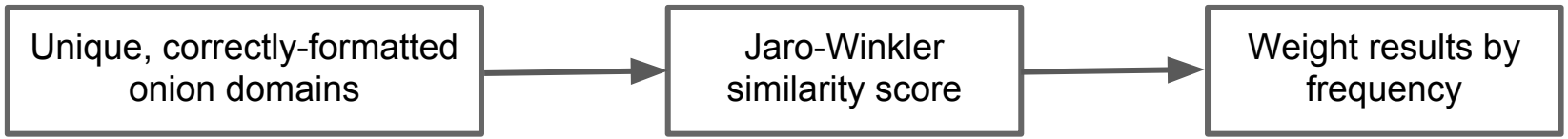
`hydraruzxpnew4af.onion` → 529 occurrences in DNS dataset

`hydraruzxpnew3af.onion` → 2 occurrences in DNS dataset

Onion Lookups Suggest Typos or Phishing

`hydraruzxpnew4af.onion` → 529 occurrences in DNS dataset

`hydraruzxpnew3af.onion` → 2 occurrences in DNS dataset



Onion Lookups Suggest Typos or Phishing

Onion 1	#	Onion 2	#	J-W
57g7spgrzlojinas	1,621	57g7spgrziojinas	14	0.989
xxlvbrloxvriy2c5	1,593	xxlvbrioxvriy2c5	4	0.949
gx7ekbenv2riucmf	1,476	gm7ekbenv2riucmf	4	0.973
mischapuk6hyrn72	1,062	mischa5xyir2mrhd	8	0.902
petya3jxfp2f7g3i	1,061	petya3jxfb2f7g3i	8	0.997
petya3jxfp2f7g3i	1,061	petya37h5tbhyvki	58	0.907
mischa5xyix2mrhd	786	mischa5xyir2mrhd	8	0.999
hydraruzxpnew4af	529	hydraruzxpnew1af	2	0.999
hydraruzxpnew4af	529	hydraruehfq5poj5	2	0.927
hydraruzxpnew4af	529	hydraruzxpnew3af	2	0.999
3g2upl4pq6kufc4m	472	tg2upl4pq6kufc4m	2	0.971
3g2upl4pq6kufc4m	472	3g2upl4t5houfo4y	2	0.924
3g2upl4pq6kufc4m	472	3g2upl4oq6kuc4mm	2	0.954
3g2upl4pq6kufc4m	472	3g2upl4pe3kcf24d	2	0.973
zqktlwi4fecvo6ri	410	zqktlwipcfe3siu2	2	0.931
zqktlwi4fecvo6ri	410	zqktlwi4i34kbat3	12	0.946

Onion Lookups Suggest Typos or Phishing

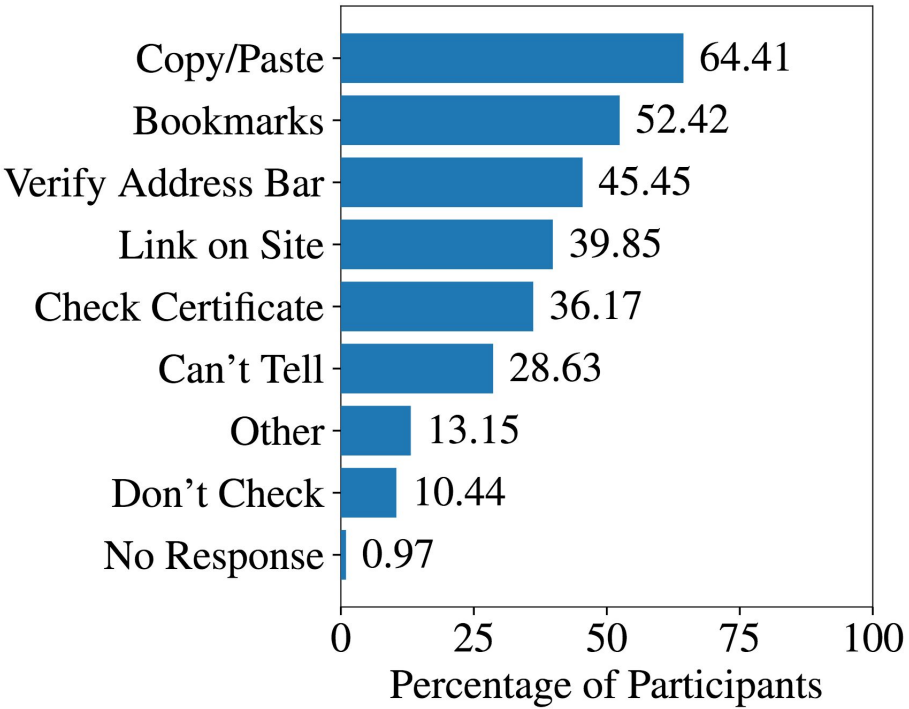
Onion 1	#	Onion 2	#	J-W
57g7spgrzlojinas	1,621	57g7spgrziojinas	14	0.989
xxlvbrloxvriy2c5	1,593	xxlvbrioxvriy2c5	4	0.949
gx7ekbenv2riucmf	1,476	gm7ekbenv2riucmf	4	0.973
mischapuk6hyrn72	1,062	mischa5xyir2mrhd	8	0.902
petya3jxfp2f7g3i	1,061	petya3jxfb2f7g3i	8	0.997
petya3jxfp2f7g3i	1,061	petya37h5tbhyvki	58	0.907
mischa5xyix2mrhd	786	mischa5xyir2mrhd	8	0.999
hydraruzxpnew4af	529	hydraruzxpnew1af	2	0.999
hydraruzxpnew4af	529	hydraruehfq5poj5	2	0.927
hydraruzxpnew4af	529	hydraruzxpnew3af	2	0.999
3g2upl4pq6kufc4m	472	tg2upl4pq6kufc4m	2	0.971
3g2upl4pq6kufc4m	472	3g2upl4t5houfo4y	2	0.924
3g2upl4pq6kufc4m	472	3g2upl4oq6kuc4mm	2	0.954
3g2upl4pq6kufc4m	472	3g2upl4pe3kcf24d	2	0.973
zqktlwi4fecvo6ri	410	zqktlwipcfe3siu2	2	0.931
zqktlwi4fecvo6ri	410	zqktlwi4i34kbat3	12	0.946

Russian Market

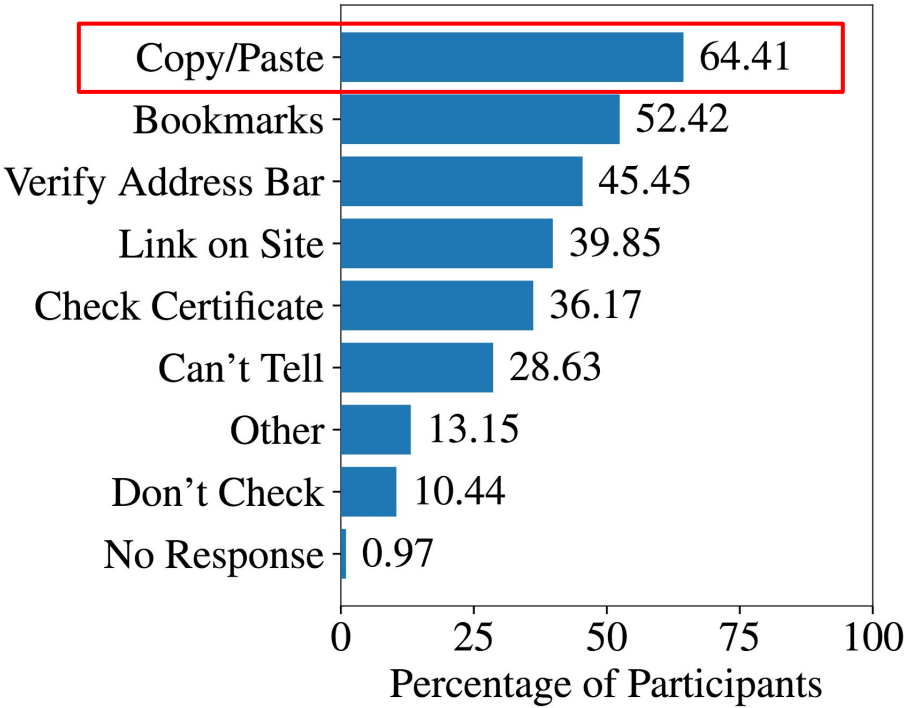
DuckDuckGo

The Hidden Wiki

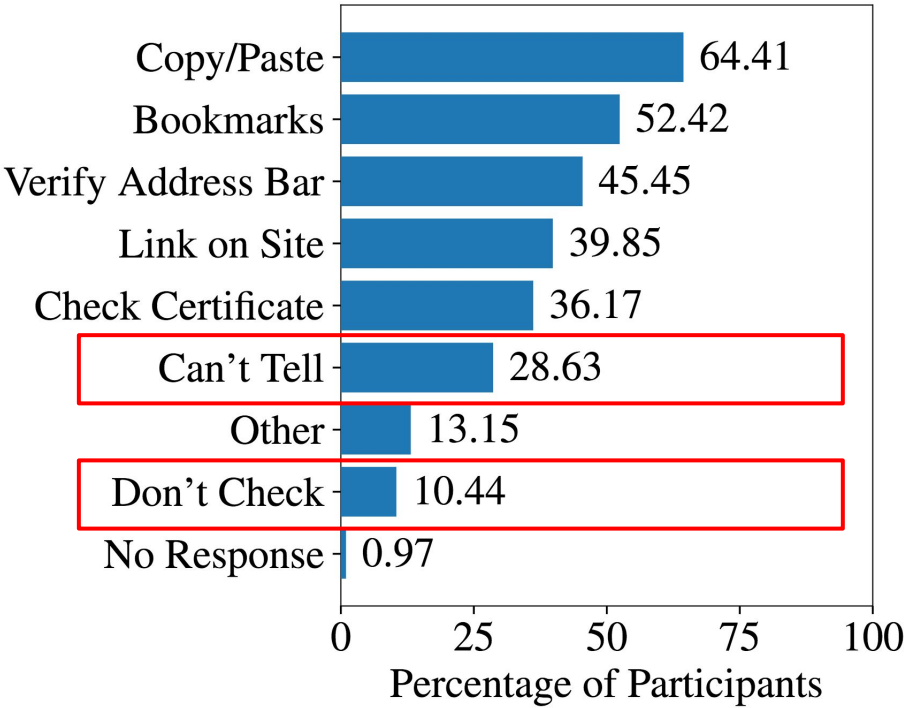
Onion Sites are Hard to Verify as Authentic



Onion Sites are Hard to Verify as Authentic



Onion Sites are Hard to Verify as Authentic



Summary of Findings

- Discovering onion services is challenging because they are private by default
- Vanity domains are more memorable but provide a false sense of security
- Users are lacking a way to verify the authenticity of onion domains

Overview

1. Onion Services Background + Features
2. Methods
3. Results
    a. Onion Sites Discovery
    b. Vanity Domains
    c. Verifying Onion Sites
4. **Future Directions & Conclusions**

Making Onion Domains More Usable

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

Conclusion

Despite extra security and privacy properties of onion services, many users are confronted with usability issues

- Susceptibility of onion services to phishing attacks
- Discovering the existence of onion services
- Managing and remembering onion domains

Conclusion

Despite extra security and privacy properties of onion services, many users are confronted with usability issues

- Susceptibility of onion services to phishing attacks
- Discovering the existence of onion services
- Managing and remembering onion domains

We can learn from the issues users have encountered to implement design improvements

- Better discovery mechanisms
- Better verification mechanisms

Questions?

More info at: https://nymity.ch/onion-services/

https://hci.princeton.edu

https://citp.princeton.edu/

Sponsored by: