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://expyuuzz4wqqyqhjn.onion
http://expyuzz4wqqyqhjn.onion
Truncated, base 32-encoded hash over RSA public key

http://expyzu4wqqyqhjn.onion
http://expyzuzz4wqqyqhqhn.onion

Not limited to HTTP(S)
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

3wcwjjnuvjyazeza.onion

The Tor network

3wcwjjnuvjyazeza
Onion Services are Self-authenticating

3wcwjnuvjyazeza.onion

Public key

The Tor network

3wcwjnuvjyazeza
Onion Services are Self-authenticating

3wcwjjnuvjyazeza.onion

SHA-1

Public key

The Tor network

3wcwjjnuvjyazeza
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

The Tor network

I talk to the client through relay R2

I have no idea who I’m talking to

I talk to the onion service through relay R2

3wcwjjnuvjyazeza
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?

Mixed-method user study

Interviews

Survey

DNS B Root Data
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

- Social Networking: 47.58%
- Search Engine: 46.42%
- Random Encounters: 46.23%
- Word of Mouth: 18.18%
- Other: 16.25%
- Not Interested: 4.26%
- No Response: 6.57%
Makeshift Solutions Ease Onion Discovery

- Social Networking: 47.58%
- Search Engine: 46.42%
- Random Encounters: 46.23%
- Word of Mouth: 18.18%
- Other: 16.25%
- Not Interested: 4.26%
- No Response: 6.57%

Percentage of Participants
Makeshift Solutions Ease Onion Discovery

- Social Networking: 47.58%
- Search Engine: 46.42%
- Random Encounters: 46.23%
- Word of Mouth: 18.18%
- Other: 16.25%
- Not Interested: 4.26%
- No Response: 6.57%

Percentage of Participants
Makeshift Solutions Ease Onion Discovery

- Social Networking: 47.58%
- Search Engine: 46.42%
- Random Encounters: 46.23%
- Word of Mouth: 18.18%
- Other: 16.25%
- Not Interested: 4.26%
- No Response: 6.57%
<table>
<thead>
<tr>
<th>Onion</th>
<th>Title</th>
<th>Added</th>
</tr>
</thead>
<tbody>
<tr>
<td>kx5p6btdjxthhvqx.onion</td>
<td></td>
<td>13 min</td>
</tr>
<tr>
<td>kuchuvztybgmbdg7.onion</td>
<td></td>
<td>an hr</td>
</tr>
<tr>
<td>n44kt6fn3khexmvmj.onion</td>
<td>Dark Net Guns - Guns on the dark web</td>
<td>an hr</td>
</tr>
<tr>
<td>ksvige6vjlnoiokd.onion</td>
<td></td>
<td>3 hr</td>
</tr>
<tr>
<td>sz6pub2csketcddgu.onion</td>
<td>xPlay - hosting service for porn videos</td>
<td>4 hr</td>
</tr>
<tr>
<td>ai5gpsxxufz4y7g.onion</td>
<td></td>
<td>4 hr</td>
</tr>
<tr>
<td>patr4lljvktjcmnn.onion</td>
<td>Radioafición electricidad y electrónica - Página principal</td>
<td>4 hr</td>
</tr>
<tr>
<td>domacuyoqnbbybul.onion</td>
<td>I2P Anonymous Webserver</td>
<td>4 hr</td>
</tr>
</tbody>
</table>
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

- Tor Bookmark: 51.84%
- Local Text File: 36.75%
- Trusted Web Pages: 34.62%
- No Solution: 25.73%
- Search Engine: 18.18%
- Memorize: 16.63%
- Other: 9.28%
- Pen and Paper: 7.93%
- Web Bookmark: 2.51%
- No Response: 6.19%

Percentage of Participants
Onion Domain Management is Chaotic

- Tor Bookmark: 51.84%
- Local Text File: 36.75%
- Trusted Web Pages: 34.62%
- No Solution: 25.73%
- Search Engine: 18.18%
- Memorize: 16.63%
- Other: 9.28%
- Pen and Paper: 7.93%
- Web Bookmark: 2.51%
- No Response: 6.19%
Onion Domains are Difficult to Remember
Onion Domains are Difficult to Remember

Meaningful prefixes appear 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
facebookcorewwwwi.onion
protonirockerxow.onion
Vanity Onion Domains

- propub3r6espa33w.onion
- nytimes3xbfgragh.onion
- facebookcorewwwwi.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

hydraruzxpnew3af.onion

529 occurrences in DNS dataset

2 occurrences in DNS dataset
Onion Lookups Suggest Typos or Phishing

 hydraruzxpnew4af.onion

 hydraruzxpnew3af.onion

Unique, correctly-formatted onion domains → Jaro-Winkler similarity score → Weight results by frequency

529 occurrences in DNS dataset
2 occurrences in DNS dataset
Onion Lookups Suggest Typos or Phishing

<table>
<thead>
<tr>
<th>Onion 1</th>
<th>#</th>
<th>Onion 2</th>
<th>#</th>
<th>J-W</th>
</tr>
</thead>
<tbody>
<tr>
<td>57g7spgrzlojinac</td>
<td>1,621</td>
<td>57g7spgrzlojinac</td>
<td>14</td>
<td>0.989</td>
</tr>
<tr>
<td>xxlvbrlooxvriy2c5</td>
<td>1,593</td>
<td>xxlvbrlooxvriy2c5</td>
<td>4</td>
<td>0.949</td>
</tr>
<tr>
<td>gx7ekbenv2riucmfe</td>
<td>1,476</td>
<td>gm7ekbenv2riucmfe</td>
<td>4</td>
<td>0.973</td>
</tr>
<tr>
<td>mischapuk6hyn72</td>
<td>1,062</td>
<td>mischayxir2mrhd</td>
<td>8</td>
<td>0.902</td>
</tr>
<tr>
<td>petya3jxfp2f7g3i</td>
<td>1,061</td>
<td>petya3jxfb2f7g3i</td>
<td>8</td>
<td>0.997</td>
</tr>
<tr>
<td>petya3jxfp2f7g3i</td>
<td>1,061</td>
<td>petya37h5tbhyvki</td>
<td>58</td>
<td>0.907</td>
</tr>
<tr>
<td>mischayxir2mrhd</td>
<td>786</td>
<td>mischayxir2mrhd</td>
<td>8</td>
<td>0.999</td>
</tr>
<tr>
<td>hydraruzxpnew4af</td>
<td>529</td>
<td>hydraruzxpnew1af</td>
<td>2</td>
<td>0.999</td>
</tr>
<tr>
<td>hydraruzxpnew4af</td>
<td>529</td>
<td>hydraruehfo5poj5</td>
<td>2</td>
<td>0.927</td>
</tr>
<tr>
<td>hydraruzxpnew4af</td>
<td>529</td>
<td>hydraruzxpnew3af</td>
<td>2</td>
<td>0.999</td>
</tr>
<tr>
<td>3g2upl4pq6kufc4m</td>
<td>472</td>
<td>tg2upl4pq6kufc4m</td>
<td>2</td>
<td>0.971</td>
</tr>
<tr>
<td>3g2upl4pq6kufc4m</td>
<td>472</td>
<td>3g2upl4t5houfo4y</td>
<td>2</td>
<td>0.924</td>
</tr>
<tr>
<td>3g2upl4pq6kufc4m</td>
<td>472</td>
<td>3g2upl4q6kufc4m</td>
<td>2</td>
<td>0.954</td>
</tr>
<tr>
<td>3g2upl4pq6kufc4m</td>
<td>472</td>
<td>3g2upl4pe3kcf24d</td>
<td>2</td>
<td>0.973</td>
</tr>
<tr>
<td>zqktlwicfeco6ri</td>
<td>410</td>
<td>zqktlwipfe3siu2</td>
<td>2</td>
<td>0.931</td>
</tr>
<tr>
<td>zqktlwicfeco6ri</td>
<td>410</td>
<td>zqktlwic4i34kbat3</td>
<td>12</td>
<td>0.946</td>
</tr>
</tbody>
</table>
Onion Lookups Suggest Typos or Phishing

<table>
<thead>
<tr>
<th>Onion 1</th>
<th>#</th>
<th>Onion 2</th>
<th>#</th>
<th>J-W</th>
</tr>
</thead>
<tbody>
<tr>
<td>57g7spgrzlojinast</td>
<td>1,621</td>
<td>57g7spgrzlojinast</td>
<td>14</td>
<td>0.989</td>
</tr>
<tr>
<td>xxlvbr1oxvriy2c5</td>
<td>1,593</td>
<td>xxlvbr1oxvriy2c5</td>
<td>4</td>
<td>0.949</td>
</tr>
<tr>
<td>gx7ekbenv2riucmf</td>
<td>1,476</td>
<td>gm7ekbenv2riucmf</td>
<td>4</td>
<td>0.973</td>
</tr>
<tr>
<td>mischapuk6hynn72</td>
<td>1,062</td>
<td>mischa5xyir2mrhd</td>
<td>8</td>
<td>0.902</td>
</tr>
<tr>
<td>petya3jxfp2f7g3i</td>
<td>1,061</td>
<td>petya3jxfb2f7g3i</td>
<td>8</td>
<td>0.997</td>
</tr>
<tr>
<td>petya3jxfp2f7g3i</td>
<td>1,061</td>
<td>petya37h5tbhyvki</td>
<td>58</td>
<td>0.907</td>
</tr>
<tr>
<td>mischa5xyix2mrhd</td>
<td>786</td>
<td>mischa5xyir2mrhd</td>
<td>8</td>
<td>0.999</td>
</tr>
<tr>
<td>hydraruzxpnew4af</td>
<td>529</td>
<td>hydraruzxpnew1af</td>
<td>2</td>
<td>0.999</td>
</tr>
<tr>
<td>hydraruzxpnew4af</td>
<td>529</td>
<td>hydraruehjq5poj5</td>
<td>2</td>
<td>0.927</td>
</tr>
<tr>
<td>hydraruzxpnew4af</td>
<td>529</td>
<td>hydraruxpnew3af</td>
<td>2</td>
<td>0.999</td>
</tr>
<tr>
<td>3g2upl4pq6kufc4m</td>
<td>472</td>
<td>tg2upl4pq6kufc4m</td>
<td>2</td>
<td>0.971</td>
</tr>
<tr>
<td>3g2upl4pq6kufc4m</td>
<td>472</td>
<td>3g2upl4t5houfo4y</td>
<td>2</td>
<td>0.924</td>
</tr>
<tr>
<td>3g2upl4pq6kufc4m</td>
<td>472</td>
<td>3g2upl4q6kuc4mm</td>
<td>2</td>
<td>0.954</td>
</tr>
<tr>
<td>3g2upl4pq6kufc4m</td>
<td>472</td>
<td>3g2upl4pe3kcf24d</td>
<td>2</td>
<td>0.973</td>
</tr>
<tr>
<td>zqktlw14fecvo6ri</td>
<td>410</td>
<td>zqktlw14pecfe3siu2</td>
<td>2</td>
<td>0.931</td>
</tr>
<tr>
<td>zqktlw14fecvo6ri</td>
<td>410</td>
<td>zqktlw14i34kbv3t</td>
<td>12</td>
<td>0.946</td>
</tr>
</tbody>
</table>

**Russian Market**

**DuckDuckGo**

**The Hidden Wiki**
Onion Sites are Hard to Verify as Authentic

- Copy/Paste: 64.41%
- Bookmarks: 52.42%
- Verify Address Bar: 45.45%
- Link on Site: 39.85%
- Check Certificate: 36.17%
- Can’t Tell: 28.63%
- Other: 13.15%
- Don’t Check: 10.44%
- No Response: 0.97%

Percentage of Participants
Onion Sites are Hard to Verify as Authentic

- Copy/Paste: 64.41%
- Bookmarks: 52.42%
- Verify Address Bar: 45.45%
- Link on Site: 39.85%
- Check Certificate: 36.17%
- Can’t Tell: 28.63%
- Other: 13.15%
- Don’t Check: 10.44%
- No Response: 0.97%

Percentage of Participants
Onion Sites are Hard to Verify as Authentic

<table>
<thead>
<tr>
<th>Method</th>
<th>Percentage of Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy/Paste</td>
<td>64.41</td>
</tr>
<tr>
<td>Bookmarks</td>
<td>52.42</td>
</tr>
<tr>
<td>Verify Address Bar</td>
<td>45.45</td>
</tr>
<tr>
<td>Link on Site</td>
<td>39.85</td>
</tr>
<tr>
<td>Check Certificate</td>
<td>36.17</td>
</tr>
<tr>
<td>Can’t Tell</td>
<td>28.63</td>
</tr>
<tr>
<td>Other</td>
<td>13.15</td>
</tr>
<tr>
<td>Don’t Check</td>
<td>10.44</td>
</tr>
<tr>
<td>No Response</td>
<td>0.97</td>
</tr>
</tbody>
</table>
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: