New Me:
Understanding Expert and Non-expert Perceptions and Usage of the Tor Anonymity Network

Kevin Gallagher  
New York University

Sameer Patil  
Indiana University

Nasir Memon  
New York University
Tor is a decentralized anonymity network.
Little is known about Tor users.
We utilized multiple recruitment strategies.

* Reddit was also used, but did not allow us to use their logo.
We recruited participants from all walks of life.
Participants took part in an interview.
There is not enough time to cover all findings.

<table>
<thead>
<tr>
<th>Category</th>
<th>Expert</th>
<th>Non-Expert</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mental Model</td>
<td>Complex network</td>
<td>On-demand service</td>
</tr>
<tr>
<td>Threat Model</td>
<td>Multiple threats</td>
<td>Specific (single) threat</td>
</tr>
<tr>
<td>Frequency of Use</td>
<td>Frequent</td>
<td>Mostly for specific uses</td>
</tr>
<tr>
<td>Discovery</td>
<td>Varied</td>
<td>Mostly through news</td>
</tr>
<tr>
<td>Morality of Tor</td>
<td>Good, positive</td>
<td>Varied, mostly positive</td>
</tr>
</tbody>
</table>
Experts treat Tor as a Complex Network.
Experts treat Tor as a Complex Network.
“When I started off I understood [Tor] pretty crudely as just kind of a way to get past state firewalls and to hide your identity from Web sites you are visiting. As I continued to use it, it’s really good for NAT [Network Address Translation] traversal for example. Like, if you want to host a Web site from your home address and you’re behind NAT, a Tor hidden service is a great way to give you that kind of access.”

(P8, Expert, Male)
Experts understood the threat model.
“Between the laptop and the entry I will write a little note that says ISP can see that I’m using Tor. And then between the entry and the middle I’m going to say ‘encrypted traffic.’ And then between the middle and the exit I’m going to say ‘encrypted traffic’ and between the exit and the Web site I’m going to say ‘ISP can see requests, but not the originator.’”

(P1, Expert, Male)
“Nodes may be owned/owned by governments.”
(P5, Expert, Unspecified gender)
Non-experts view Tor as a service.
“As far as I’m aware the way it works is it bounces your signal around a lot . . . To various countries and such.”

(P3, Non-expert, Male)
“And then like IP address . . . I don’t know . . . does Tor jumble up your IP? Maybe, perhaps it does, perhaps it doesn’t. Perhaps it gives you a new IP.”

(P2, Non-expert, Female)
Non-experts misunderstand the threat model.
“I know that I’m not doing anything dangerous but they don’t know that, so I can see why the government would want to have access to that kind of thing. Or maybe they can receive alerts from Tor saying ‘hey this person is suspicious by your standards’ . . . but that’s bad business, so...”

(P4, Non-expert, Female)
Our findings have a few actionable implications.
Our findings have a few actionable implications.
<table>
<thead>
<tr>
<th>Category</th>
<th>Expert</th>
<th>Non-Expert</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mental Model</td>
<td>Complex network</td>
<td>On-demand service</td>
</tr>
<tr>
<td>Threat Model</td>
<td>Multiple threats</td>
<td>Specific (single) threat</td>
</tr>
<tr>
<td>Frequency of Use</td>
<td>Frequent</td>
<td>Mostly for specific uses</td>
</tr>
<tr>
<td>Discovery</td>
<td>Varied</td>
<td>Mostly through news</td>
</tr>
<tr>
<td>Morality of Tor</td>
<td>Good, positive</td>
<td>Varied, mostly positive</td>
</tr>
</tbody>
</table>