16. Anonymity and Formalizing Privacy

Blase Ur
May 23rd, 2019
CMSC 23210 / 33210
Anonymity
Techniques for (some) anonymity

- Encrypt everything
- Use Tor to communicate
- Off-the-record (OTR) messaging
- Don’t use services that track you
Virtual Private Networks (VPNs)
Overview of Tor

• The Onion Router (Tor)
  – Onion routing introduced by U.S. Naval Research Labs ~ 20 years ago
  – Dingledine, Matthewson, Syverson introduced Tor in a USENIX Security paper in ‘04
How Tor works (graphics from EFF)

Step 1: Alice’s Tor client obtains a list of Tor nodes from a directory server.
How Tor works (graphics from EFF)

Step 2: Alice's Tor client picks a random path to destination server. **Green links are encrypted, red links are in the clear.**

Alice → Jane → Dave → Bob
Step 3: If at a later time, the user visits another site, Alice’s tor client selects a second random path. Again, green links are encrypted, red links are in the clear.
How Tor works
What does Tor protect against?
What does Tor NOT protect against?
Threats Against Tor

• Vulnerabilities in the protocol
• Vulnerabilities in the implementation
• Adversaries controlling large parts of the network and analyzing traffic/timing
• Vulnerabilities on the user’s end
  – E.g., old version of Firefox
• Human error on the part of the user
• Not enough users! (no hiding in the crowd)
Tor warnings

https://www.torproject.org/download/download#warning

Want Tor to really work?

You need to change some of your habits, as some things won’t work exactly as you are used to.

a. Use Tor Browser
   Tor does not protect all of your computer’s Internet traffic when you run it. Tor only protects your applications that are properly configured to send their Internet traffic through Tor. To avoid problems with Tor configuration, we strongly recommend you use the Tor Browser. It is pre-configured to protect your privacy and anonymity on the web as long as you’re browsing with Tor Browser itself. Almost any other web browser configuration is likely to be unsafe to use with Tor.

b. Don’t torrent over Tor
   Torrent file-sharing applications have been observed to ignore proxy settings and make direct connections even when they are told to use Tor. Even if your torrent application connects only through Tor, you will often send out your real IP address in the tracker GET request, because that’s how torrents work. Not only do you de-anonymize your torrent traffic and your other simultaneous Tor web traffic this way, you also slow down the entire Tor network for everyone else.

c. Don’t enable or install browser plugins
   Tor Browser will block browser plugins such as Flash, RealPlayer, Quicktime, and others: they can be manipulated into revealing your IP address. Similarly, we do not recommend installing additional addons or plugins into Tor Browser, as these may bypass Tor or otherwise harm your anonymity and privacy.

d. Use HTTPS versions of websites
   Tor will encrypt your traffic to and within the Tor network, but the encryption of your traffic to the final destination website depends upon on that website. To help ensure private encryption to websites, Tor Browser includes HTTPS Everywhere to force the use of HTTPS encryption with major websites that support it. However, you should still watch the browser URL bar to ensure that websites you provide sensitive information to display a blue or green URL bar button, include https:// in the URL, and display the proper expected name for the website. Also see EFF’s interactive page explaining how Tor and HTTPS relate.

e. Don’t open documents downloaded through Tor while online
   Tor Browser will warn you before automatically opening documents that are handled by external applications. DO NOT IGNORE THIS WARNING. You should be very careful when downloading
Making anonymity usable (example)

• Tor browser bundle
• TAILS (The Amnesic Incognito Live System)
• OTR (off-the-record) messaging tools
Why Johnny Can’t Blow the Whistle

• Identify stop-points in Tor Browser Bundle
• Highlight the security reason behind delays
• Combine Vidalia control window & browser
• Change icon
• Direct users to the right OS version
Deanonymization