13. Anonymity Tools; Designing for Activists and Journalists

Blase Ur and Mainack Mondal

May 7th, 2018

CMSC 23210 / 33210

THE UNIVERSITY OF CHICAGO

Security, Usability, & Privacy Education & Research

Today's class

- Anonymity and censorship
- More secure / anonymous browsing
  - Private browsing modes
  - VPNs
  - Tor
- Leaking data to journalists

Why is anonymity valuable?

Why do people criticize censorship?

Press censorship in practice

Techniques for censoring the Internet

- Methods (see, e.g., Aryan et al. FOCI '13):
  - DNS hijacking / prefix hijacking
  - HTTP header (host and keyword) filtering
  - Connection throttling on SSH
  - Physical threats
  - Dropping HTTPS / TLS traffic
  - IP, Keyword, DNS poisoning
  - Deep packet inspection
  - Active probes against Tor bridges
  - Self-censorship (chilling effect)

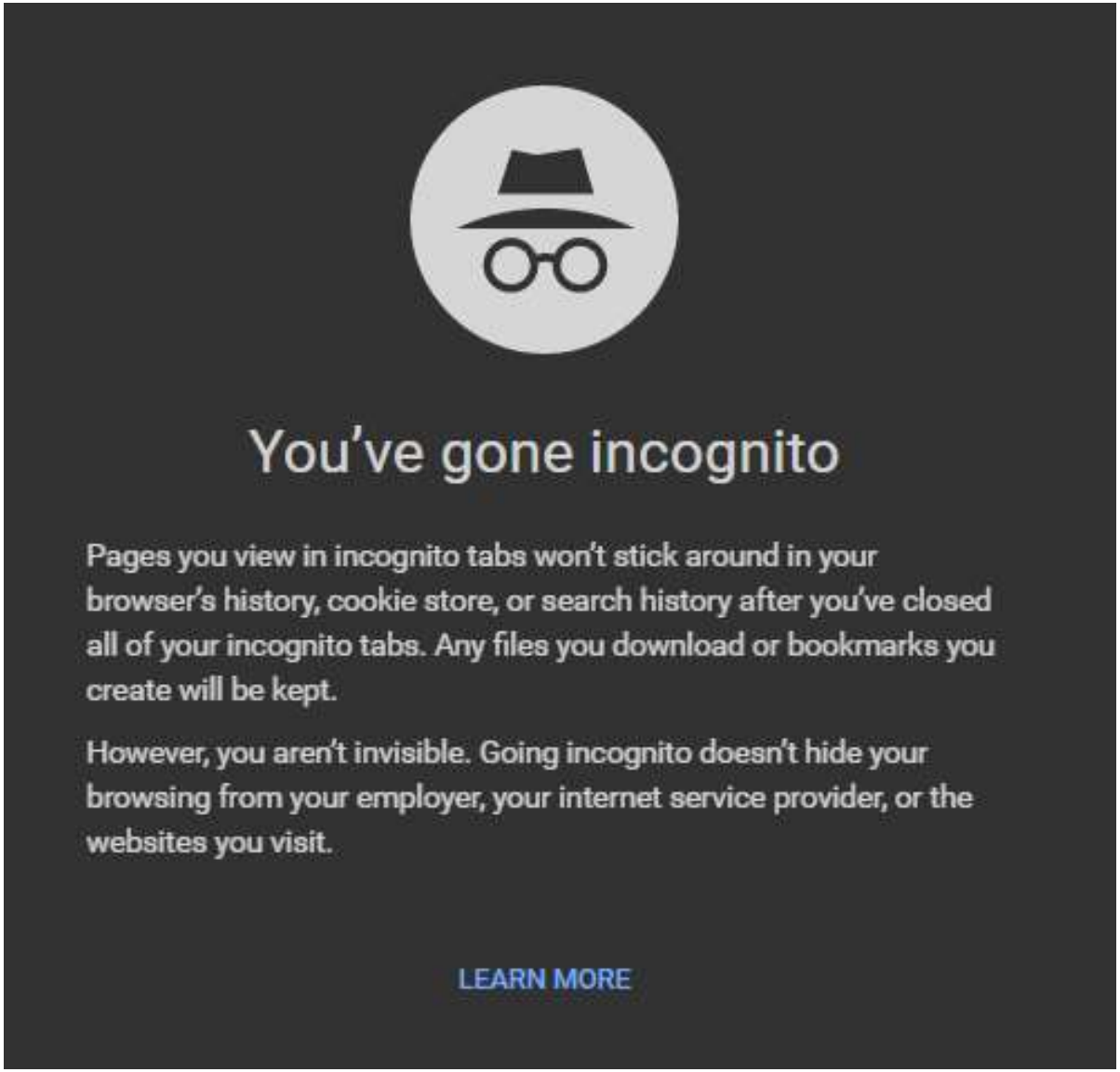
Techniques for (some) anonymity

- Encrypt everything
- Use Tor to communicate
- Off-the-record (OTR) messaging
- Don’t use services that track you

Private browsing

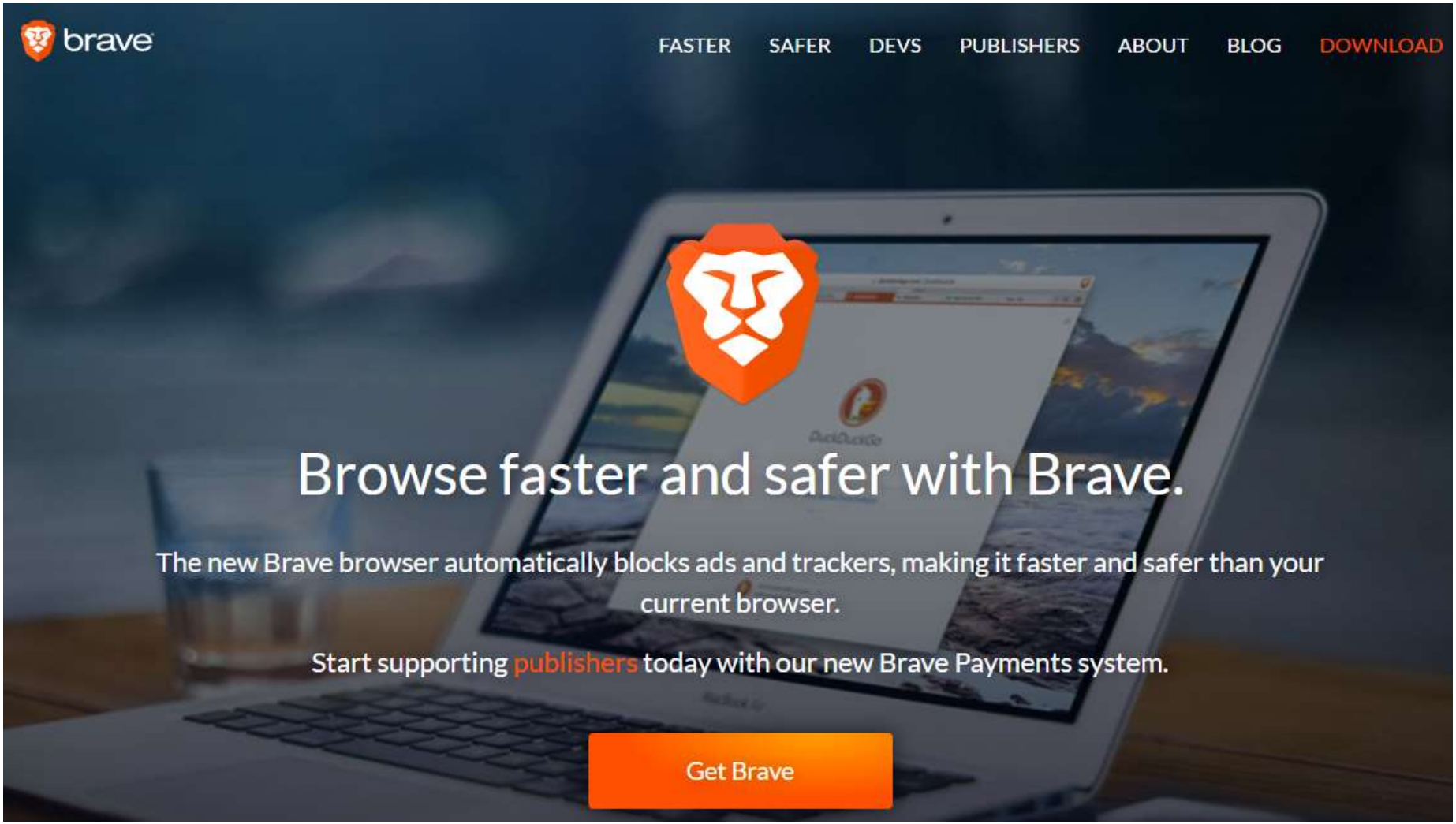
Private Browsing

Private Browsing

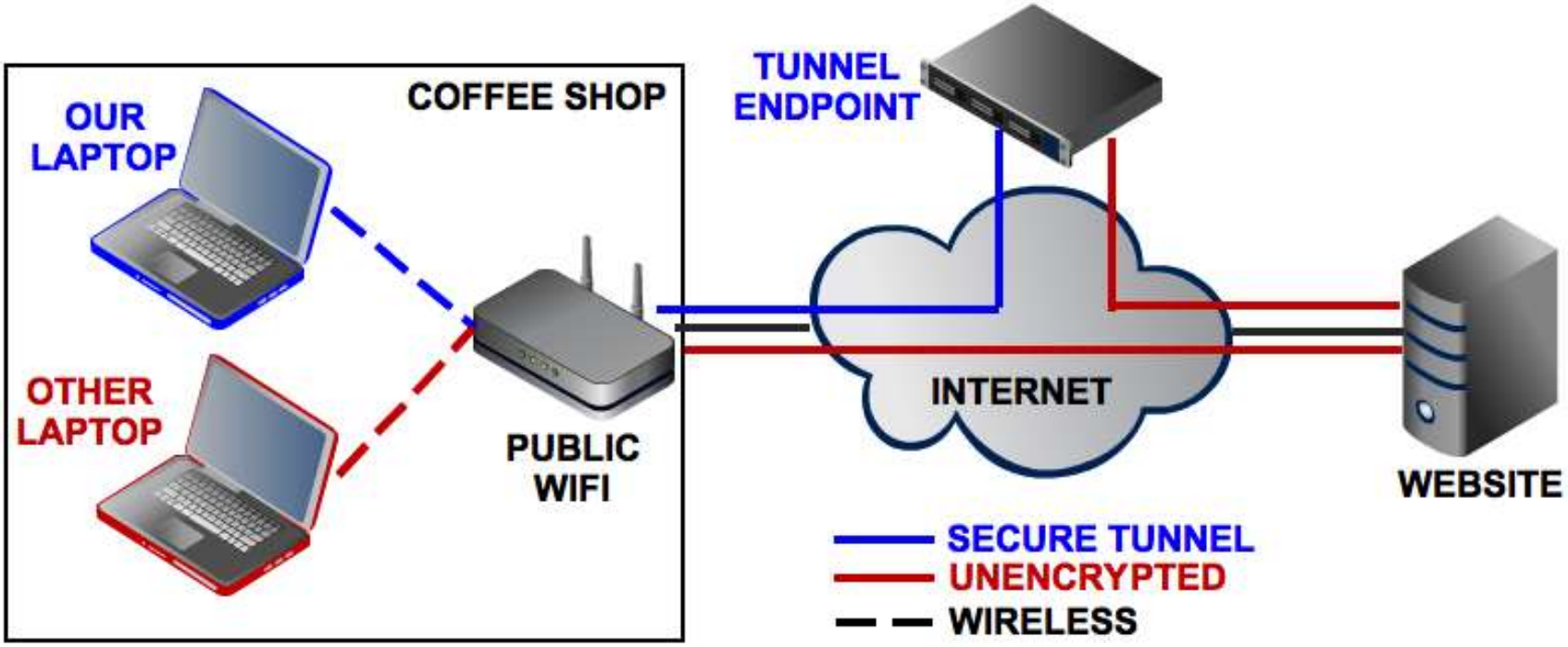


NoScript

Brave

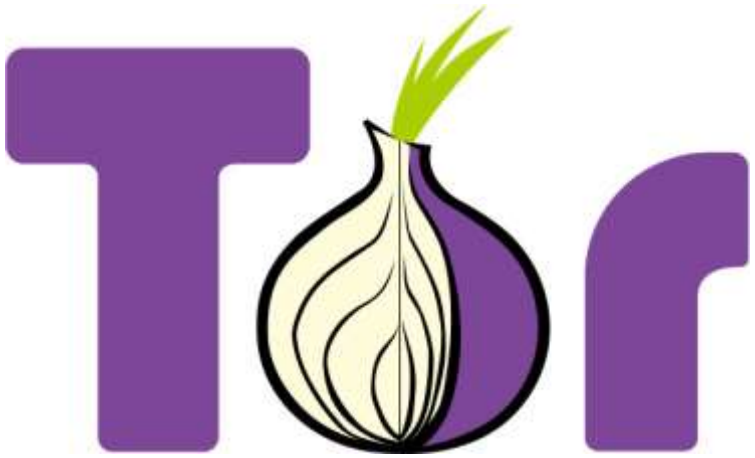

brave
FASTER
SAFER
DEVS
PUBLISHERS
ABOUT
BLOG
DOWNLOAD
Browse faster and safer with Brave.
The new Brave browser automatically blocks ads and trackers, making it faster and safer than your current browser.
Start supporting publishers today with our new Brave Payments system.
Get Brave

Virtual Private Networks (VPNs)

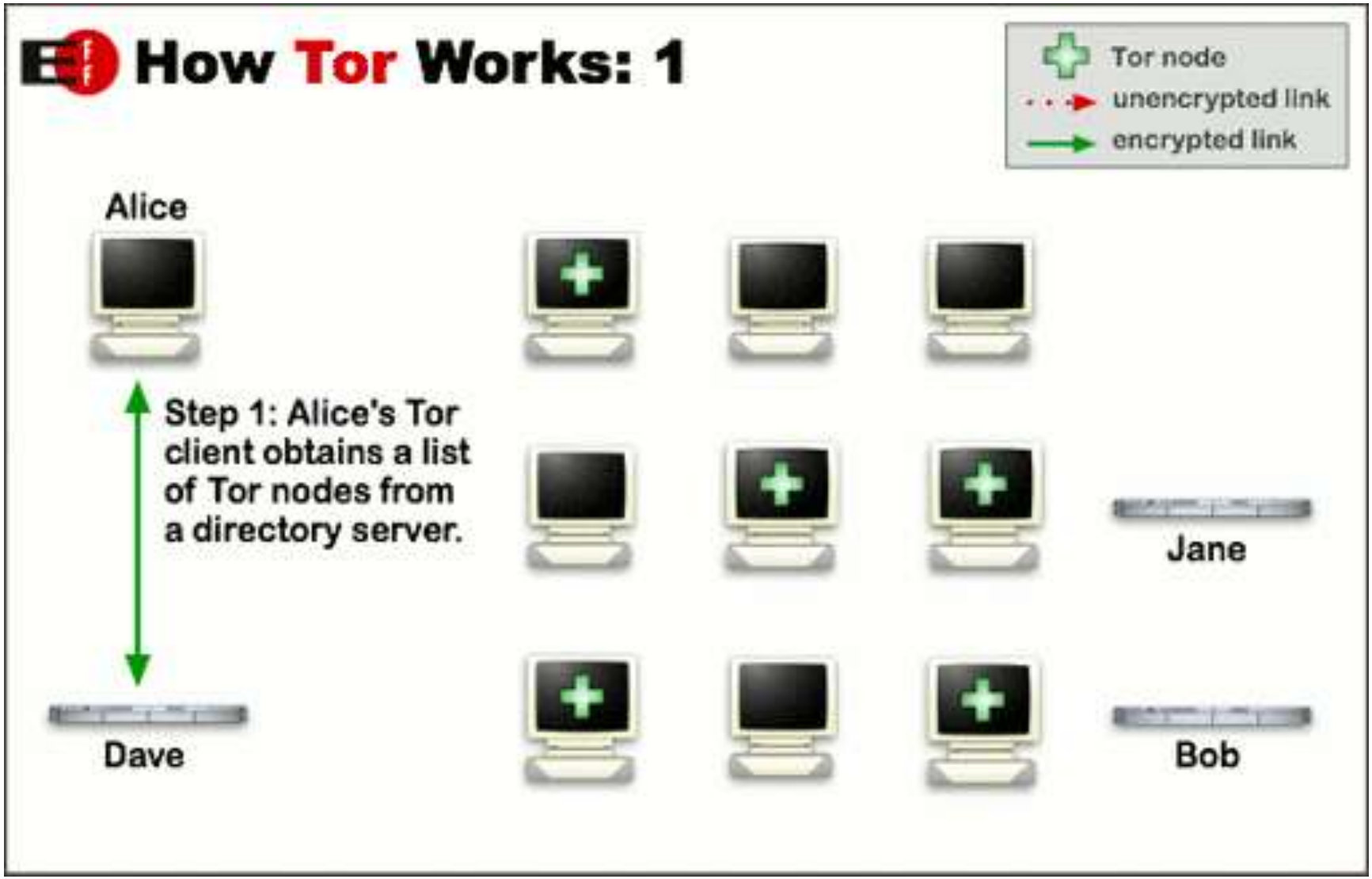


Overview of Tor

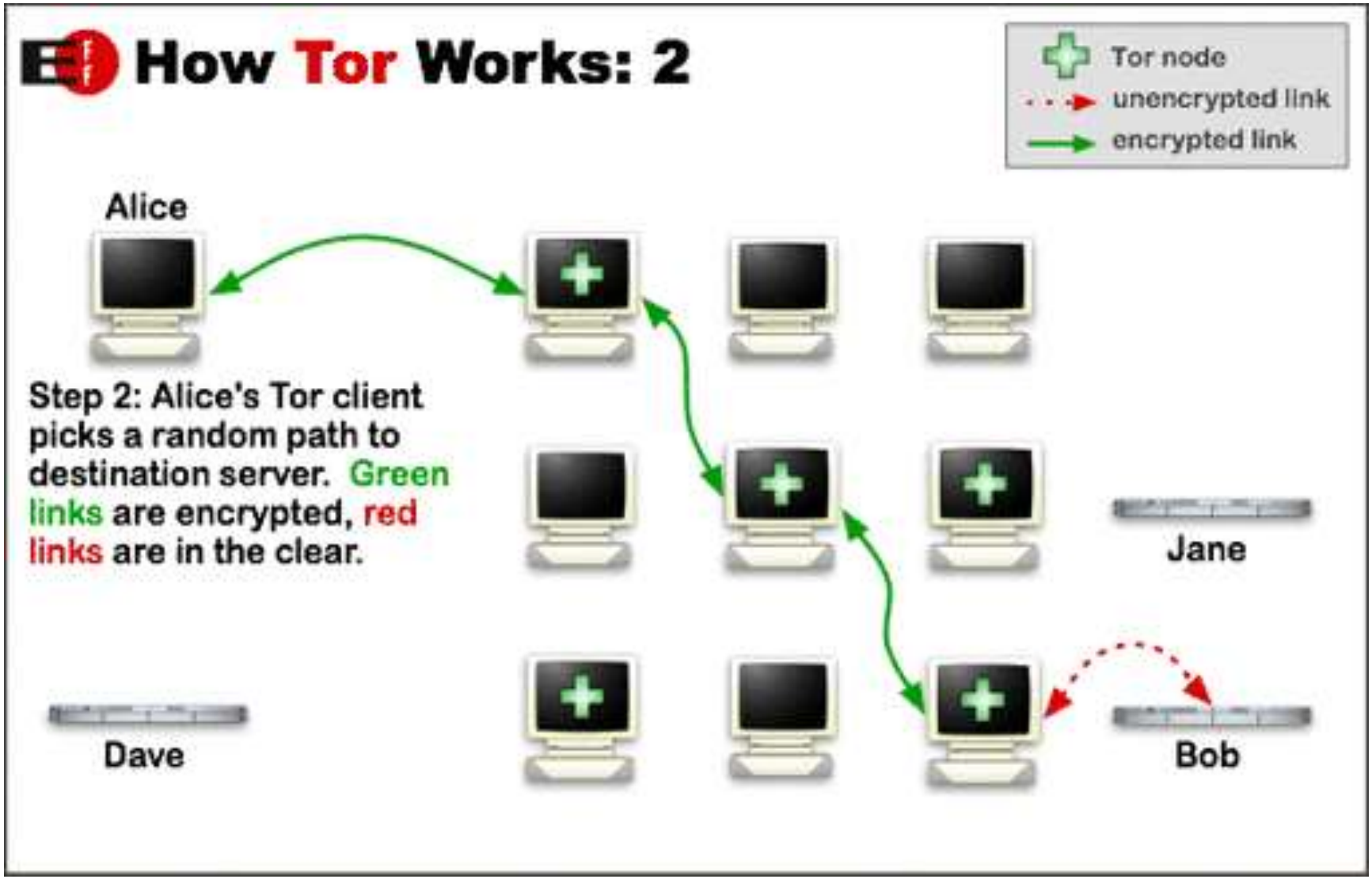
- The Onion Router (Tor)
  - Onion routing introduced by U.S. Naval Research Labs ~ 20 years ago
  - Dingledine, Matthewson, Syverson introduced Tor in a USENIX Security paper in ‘04



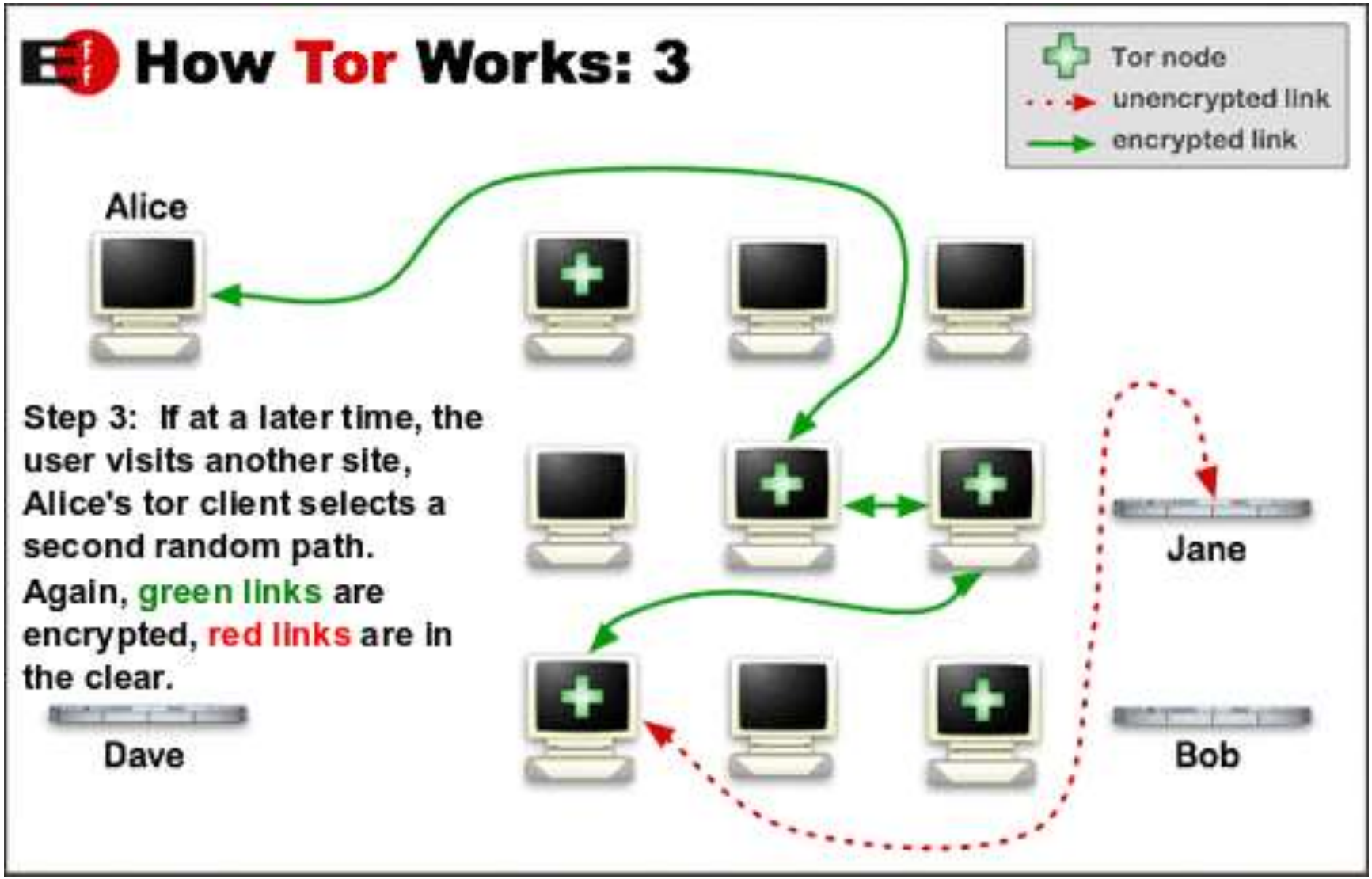
How Tor works (graphics from EFF)



How Tor works (graphics from EFF)



How Tor works (graphics from EFF)



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 deanonymize 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

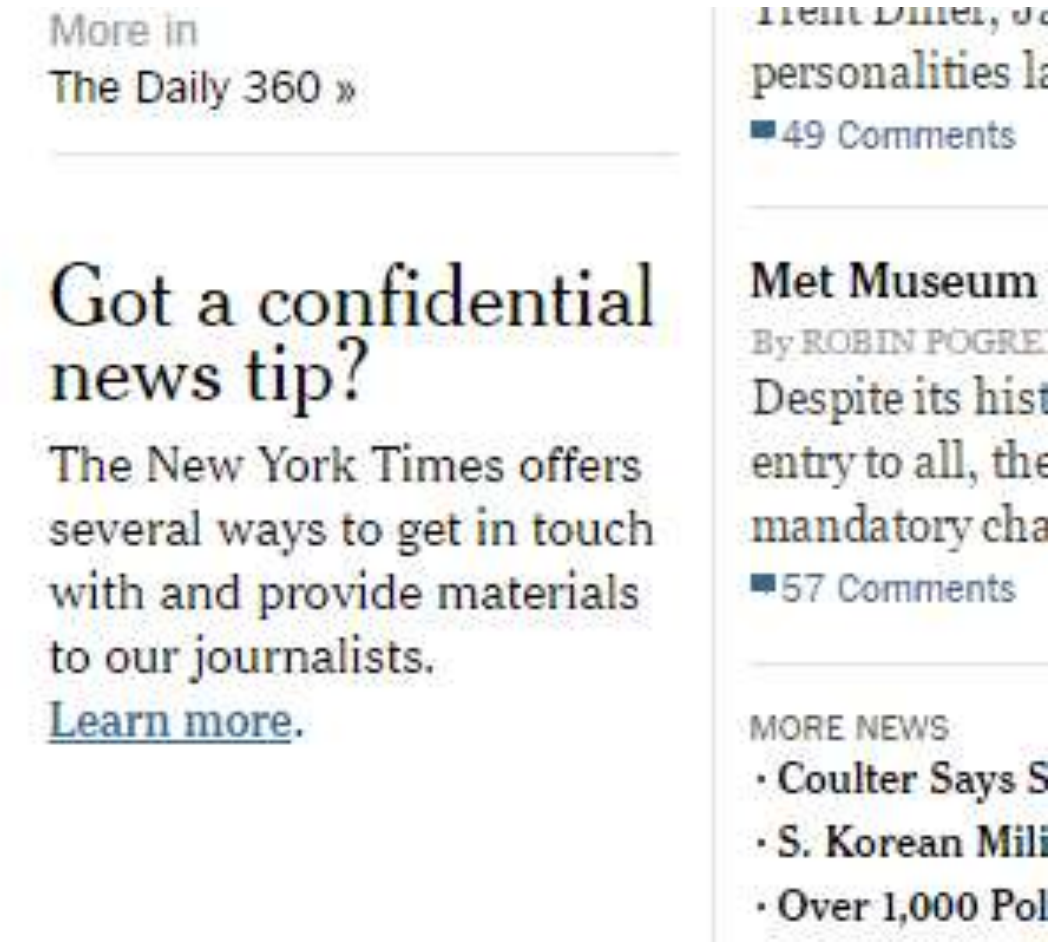
Academic literature on journalists

- McGregor et al., “Investigating the Computer Security Practices and Needs of Journalists,” USENIX Security 2015.
- Gaw et al., “Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted Email,” CHI 2006.

Guides to leaking and protesting

- https://www.nytimes.com/newsgraphics/2016/news-tips
- http://www.theglobeandmail.com/technology/the-paranoid-computer-users-guide-to-privacy/article18928710/
- https://ssd.eff.org/en/module/attending-protests-united-states

NY Times's leak instructions



More in
The Daily 360 »

Got a confidential news tip?

The New York Times offers several ways to get in touch with and provide materials to our journalists.
Learn more.

personalities la
49 Comments

Met Museum
By ROBIN POGRE
Despite its hist
entry to all, the
mandatory cha
57 Comments

MORE NEWS
· Coulter Says S
· S. Korean Mili
· Over 1,000 Pol

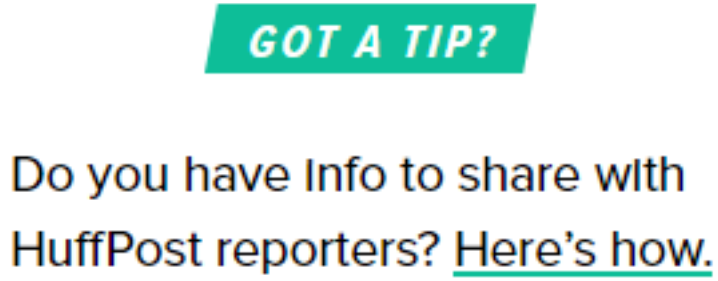
The New York Times

Got a confidential news tip?

Do you have the next big story? Want to share it with The New York Times? We offer several ways to get in touch with and provide materials to our journalists. No communication system is completely secure, but these tools can help protect your anonymity. We've outlined each below, but please review any app's terms and instructions as well. Please do not send feedback, story ideas, pitches or press releases through these channels. For more general correspondence visit our contact page.

WhatsApp **Signal** **Email** **Postal Mail** **SecureDrop**

Huffpost's leak instructions



Need privacy?

If you're concerned that being a source for a story poses a significant risk, take precautions:

- **Know your risks**. No form of communication is 100 percent safe from all observers. Make a plan about what you'll do if the wrong person finds out you contacted us.
- **Do not contact us from your work computer or phone**. Your bosses can track your use of these devices. The same goes for your personal mobile phone, if you've ever installed apps from your employer — even if you later uninstalled them.
- Consider using **postal mail**. We're at "HuffPost, PO Box 28154, Washington, DC 20038-8154." Send from a public mailbox and don't write a return address. Only we can read your message (unless a court provides a warrant).
- Use the same **encrypted email** service we do. Create a new protonmail.com account — separate from your other email accounts — and use it to write us at huffpostscoops@protonmail.com. As long as you write to our Protonmail address from your Protonmail address, only we or someone who knows your password can read your message. Read more about Protonmail.
- **Use your browser's "incognito" or "private browsing" mode**. Some sites (including, potentially, your employer's) can access your browser history and see what websites you've visited. An incognito window masks this data. Open a new incognito browser window to contact us, and close it immediately afterward. If