22- Making Anonymity Tools Usable

Lorrie Cranor, Blase Ur, and Rich Shay

April 2, 2015

05-436 / 05-836 / 08-534 / 08-734
Usable Privacy and Security

Carnegie Mellon University
CyLab

institute for SOFTWARE RESEARCH

Engineering & Public Policy

Today!

- General discussion of anonymity
- An introduction to Tor
- Attempts to help users achieve anonymity
- A design activity to communicate guarantees to users

Why is anonymity valuable?

Why do people criticize censorship?

Press censorship in practice

Techniques for censoring the Internet

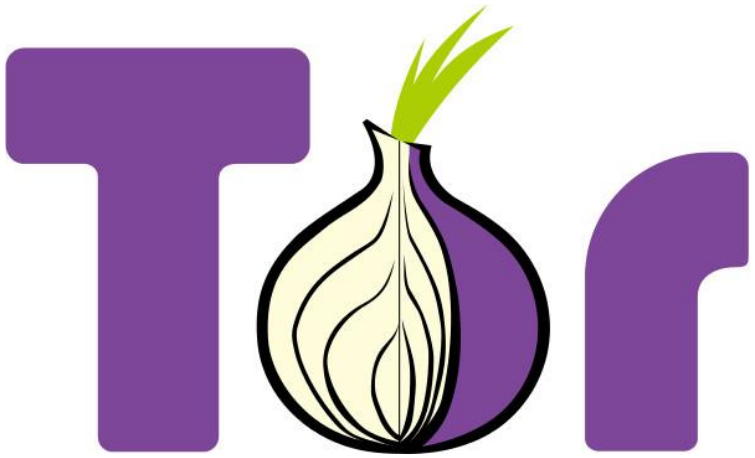
- Methods (see, e.g., Aryan et al. FOCI '13):
  - DNS hijacking / prefix hijacking
  - HTTP header (host and keyword) filtering
  - Connection throttling on SSH
  - Physical threats
  - Dropping HTTPS / TLS traffic
  - IP, Keyword, DNS poisoning
  - Deep packet inspection
  - Active probes against Tor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

Techniques for being anonymous

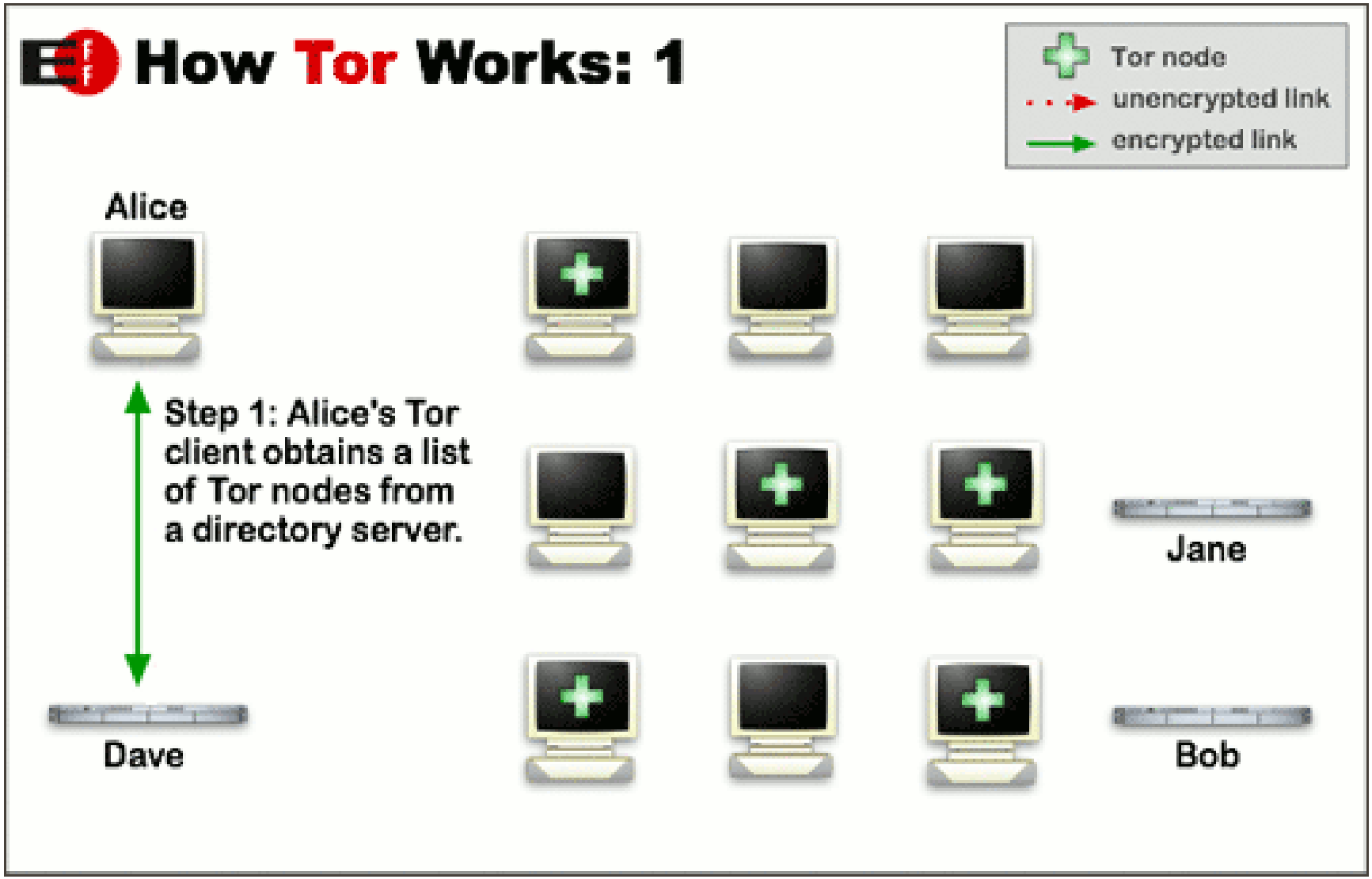
- Encrypt everything
- Use onion routing to communicate
- OTR messaging
- Don’t use services that track you

Overview of Tor

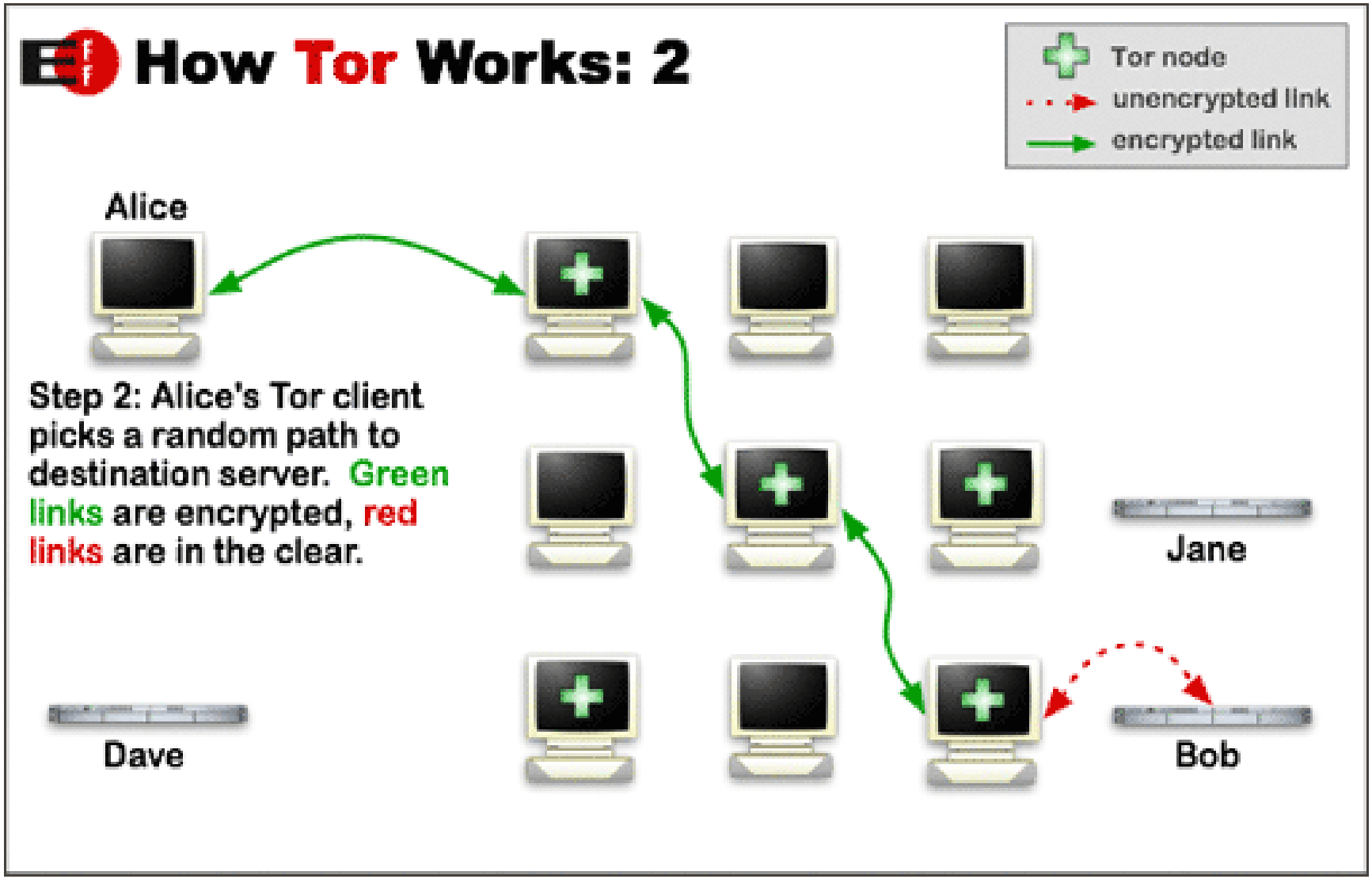
- The Onion Router (Tor)
  - Onion routing introduced by U.S. Naval Research Labs ~ 20 years ago
  - Dingledine, Matthewson, Syverson introduced Tor in a USENIX Security paper in ‘04



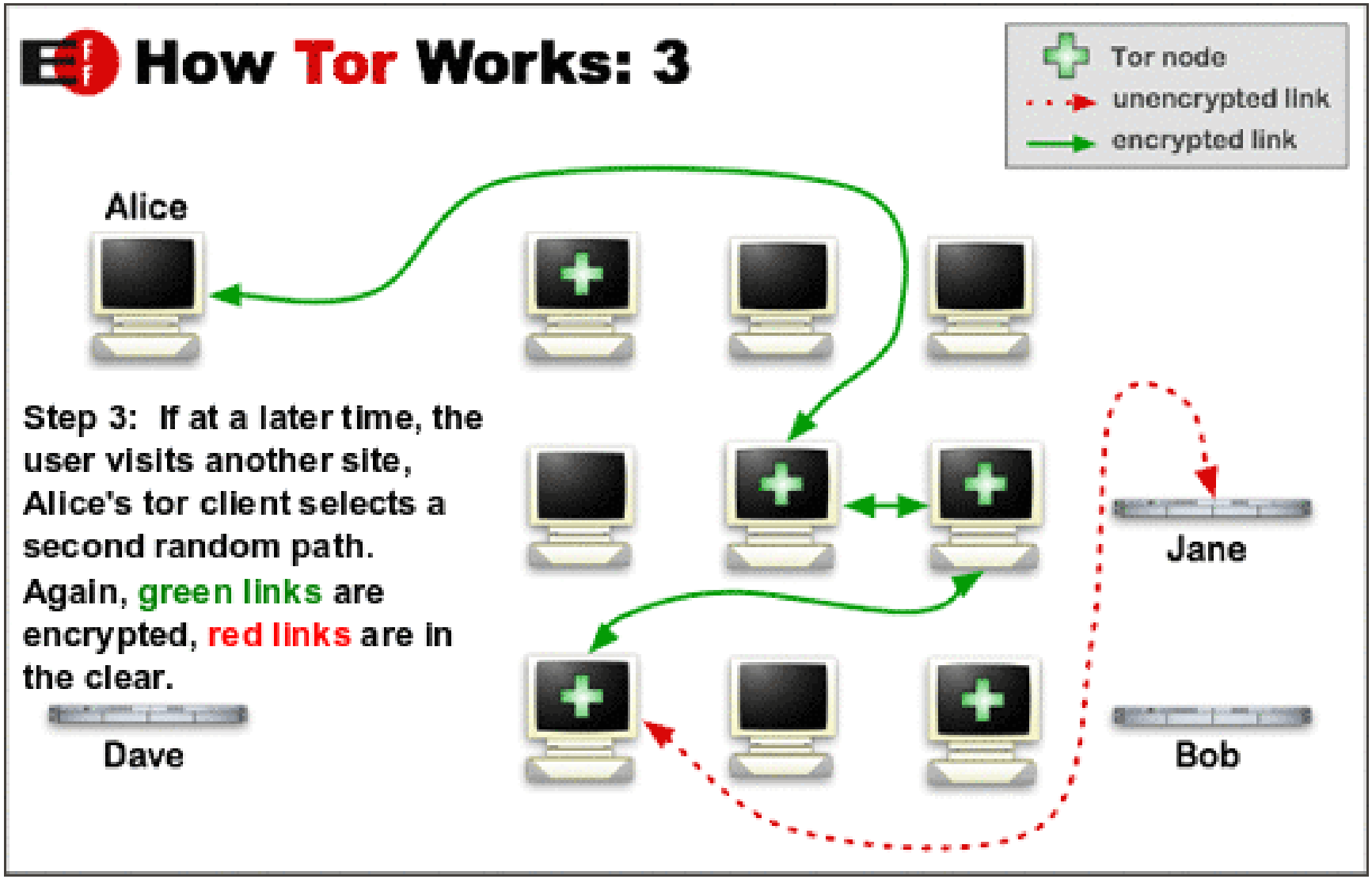
How Tor works (graphics from EFF)



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)

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

Design activity

- Imagine you have a friend, Rich, who is unfortunately poor in his ability to communicate anonymously
- Tell him everything he needs to know to browse the web anonymously and submit information to a whistleblower site
  - What should he be worried about?
  - What guarantees does he have?
- Deliverable: outline of your advice