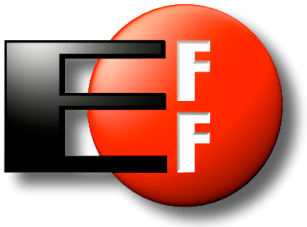


How Sysadmins Can Protect Free Speech and Privacy on the Electronic Frontier

KEVIN BANKSTON
EFF Staff Attorney

bankston@eff.org
http://www.eff.org

Presented to USENIX LISA
December 9, 2005

The Electronic Frontier Foundation

The Internet: Free Speech Engine vs. Surveillance Machine

- Speakers usually rely on third-parties--like you--to enable their Internet speech activities.
- Those activities generate third-party records.
- More people are using third-parties to store their own records.
- Much less legal protection than records they keep themselves.
- More and easier ways for the government to secretly obtain those records since the USA PATRIOT Act.
- So what's the problem?

The Electronic Frontier Foundation

Free Speech and Privacy: 2 Great Tastes that Taste Great Together

- Anonymity fosters free speech--just ask Publius, or your local librarian
- Privacy in association fosters free speech--just ask the NAACP or the ACLU
- Lack of privacy chills speech--*if* the speaker knows about it
- The First Amendment can be used to protect privacy--*if* the user knows in time to act.
- The Fourth Amendment?

The Electronic Frontier Foundation

Basics of Communications Privacy Law: Wiretapping & Eavesdropping

- N.Y. v. Berger and U.S. v. Katz in 1967
  - The Fourth Amendment protects the privacy of your f2f conversations and phone calls--if you have a "reasonable expectation of privacy" (so close the door)
- The Wiretap Act of 1968
  - Congress follows Supreme Court's lead and provides statutory framework for interception "super-warrants"

The Electronic Frontier Foundation

Basics of Communications Privacy Law: "Pen-Traps" and Stored Records

- U.S. v. Miller, 1976: No Fourth Amendment protection in your bank records
- Smith v. Maryland, 1979: No Fourth Amendment in your phone records; live interception of dialing information doesn't require a warrant

The Electronic Frontier Foundation

The Electronic Communications Privacy Act of 1986

- Updated the Wiretap Act to include electronic communications, not just phone calls
- Provided (minimal) privacy protection against pen registers and trap and trace devices
- Provided (moderate) privacy protection for records held by communications and remote computing providers to the public--but which providers and records count?
- Provided (pretty good) privacy protection for your stored communications

The Electronic Frontier Foundation

The USA PATRIOT Act and the Internet

- Extended Pen-Traps to the Internet--but what's "routing/addressing/signaling" info and what's content?
- Lowered protection for IP logs and detailed transactional information: can now get someone's "whole online profile" with a subpoena rather than a court order--no notice, and the provider can be gagged
- Reduced controls on national security-related surveilleance like FISA and NSLs--see recent revelations of abuse and overuse
- The bottom line: users can't rely on the law to protect their online privacy--they have to rely on you!

The Electronic Frontier Foundation

But What Can I Do? I'm Only a Sysadmin.

- Only a sysadmin? Please.
- Educate the Civilians About the Tech, and Yourself About the Law.
- Minimize Your Logs.
- Be the Surveillance Gatekeeper (or Squeaky Wheel).
- Support Anonymizing Technologies.

The Electronic Frontier Foundation

Minimize Your Logs

- Don’t be a packrat--only keep what you really need
- OSP Best Practices at www.eff.org/osp
  - Maintain written policies addressing data collection and retention.
  - Collect the minimum amount of information necessary to provide OSP services.
  - Store information for the minimum time necessary for operations.
  - Effectively obfuscate, aggregate and delete unneeded user information.
  - Develop procedures for dealing with legal information requests and providing notice to users…

The Electronic Frontier Foundation

Be the Surveillance Gatekeeper

- They can't do it without your help--that gives you leverage
- Negotiate to keep government software and hardware off of your system--the Carnivore problem
- You don't have to redesign your system to allow surveillance! At least, not yet…
- Lobby for legal challenges (you *can* call a lawyer)
- Give notice wherever possible

The Electronic Frontier Foundation

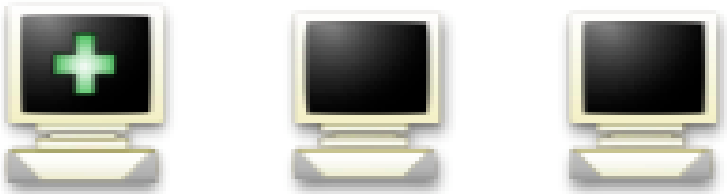
Support Anonymizing Technologies Like Tor

- Run a server!
- Help code!
- Let your users use Tor--don't blacklist unnecessarily

How Tor Works: 1

How Tor Works: 2

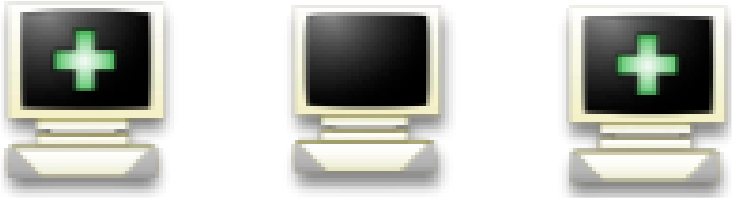
Alice



Step 2: After getting a list of Tor nodes, Alice's Tor client knows which machines can be used.

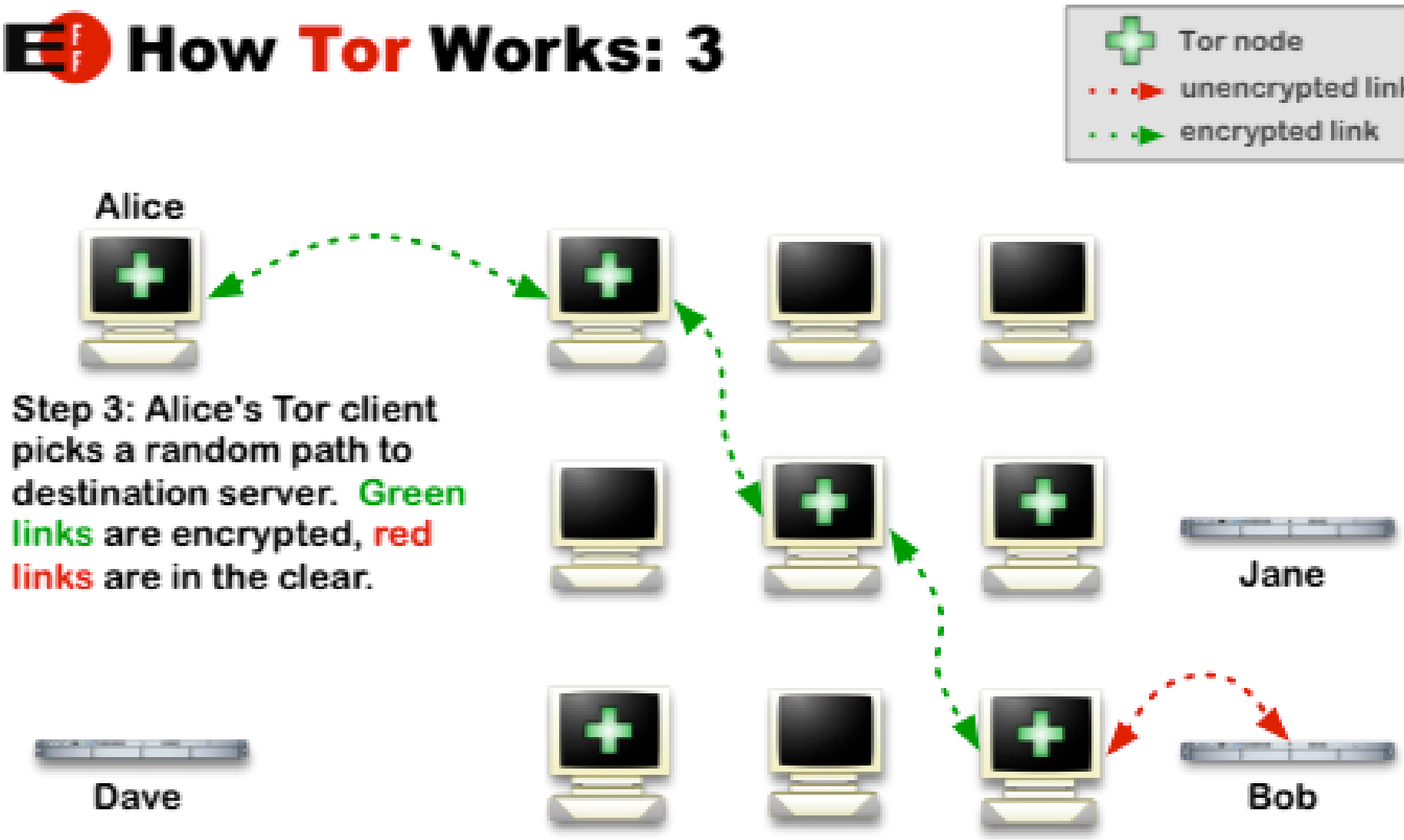
Jane

Dave

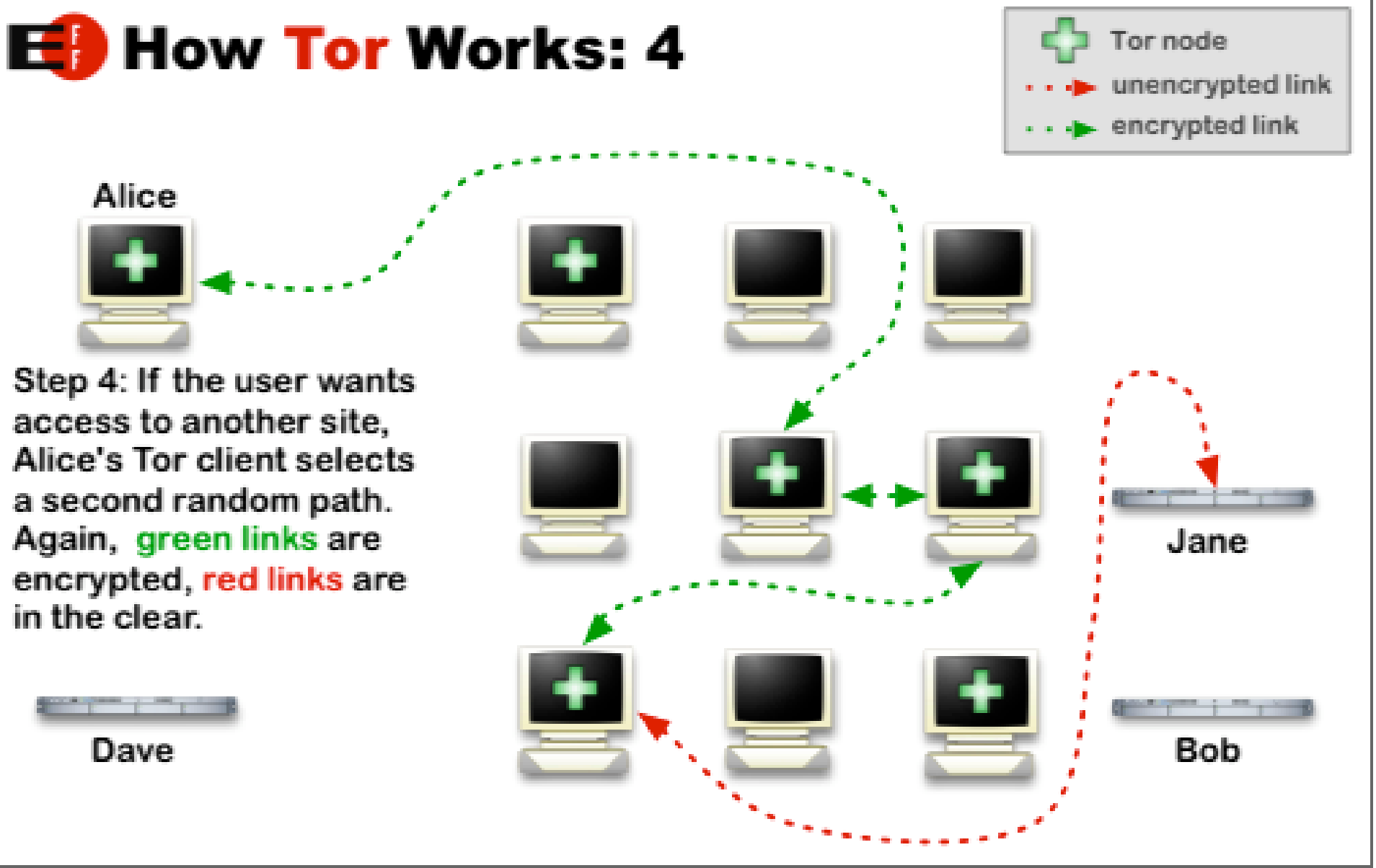


Bob

How Tor Works: 3



How Tor Works: 4



The Electronic Frontier Foundation

One more thing you can do…

JOIN EFF!

www.eff.org/support

Thanks!

Kevin Bankston, EFF Staff Attorney
bankston@eff.org