Usable Interfaces for Anonymous Communication

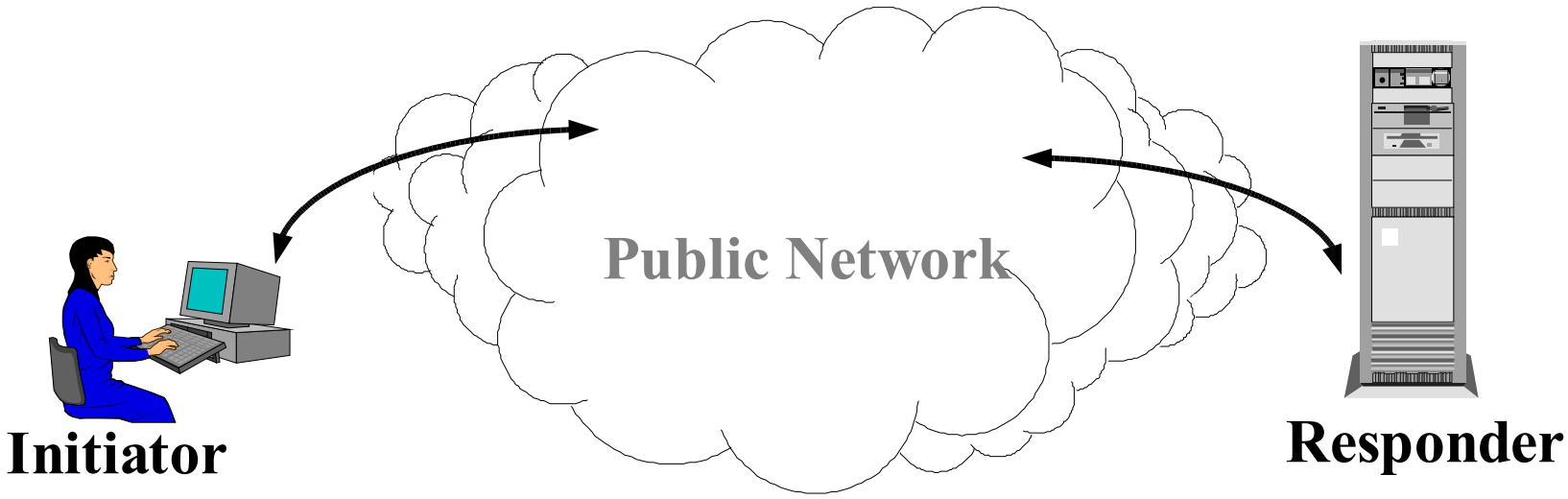
Roger Dingledine
Free Haven Project
Electronic Frontier Foundation

http://tor.eff.org/

8 July 2005

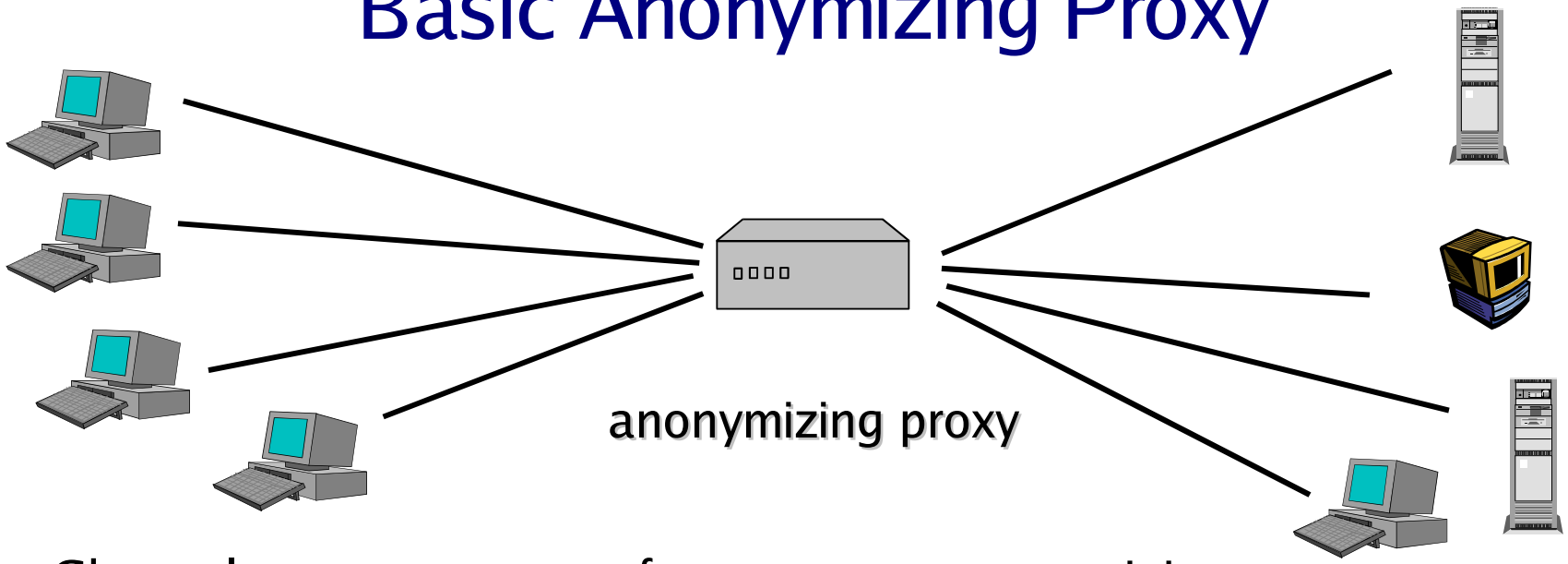
Public Networks are Vulnerable to Traffic Analysis

- In a Public Network (Internet):
- Packet (message) headers identify recipients
- Packet routes can be tracked



Encryption does *not* hide routing information.

Basic Anonymizing Proxy



- Channels appear to come from proxy, not true originator
- Appropriate for Web connections, etc.:
  SSL, TLS, SSH (lower cost symmetric encryption)
- Examples: The Anonymizer
- Advantages: Simple, Focuses lots of traffic for more anonymity
- Main Disadvantage: Single point of failure, compromise, attack

Who uses Tor?

- Journalists, Dissidents, Whistleblowers
- Censorship resistant publishers/readers (news sites, chess sites)
- Socially sensitive communicants: cancer, etc
- Ordinary citizens (protection from profiling, from your boss/neighbor/school)
- Law Enforcement (anonymous tips, researching places safely)
- Corporations (procurement, road warriors, competitive analysis)
- Governments (soldiers, intelligence agencies)

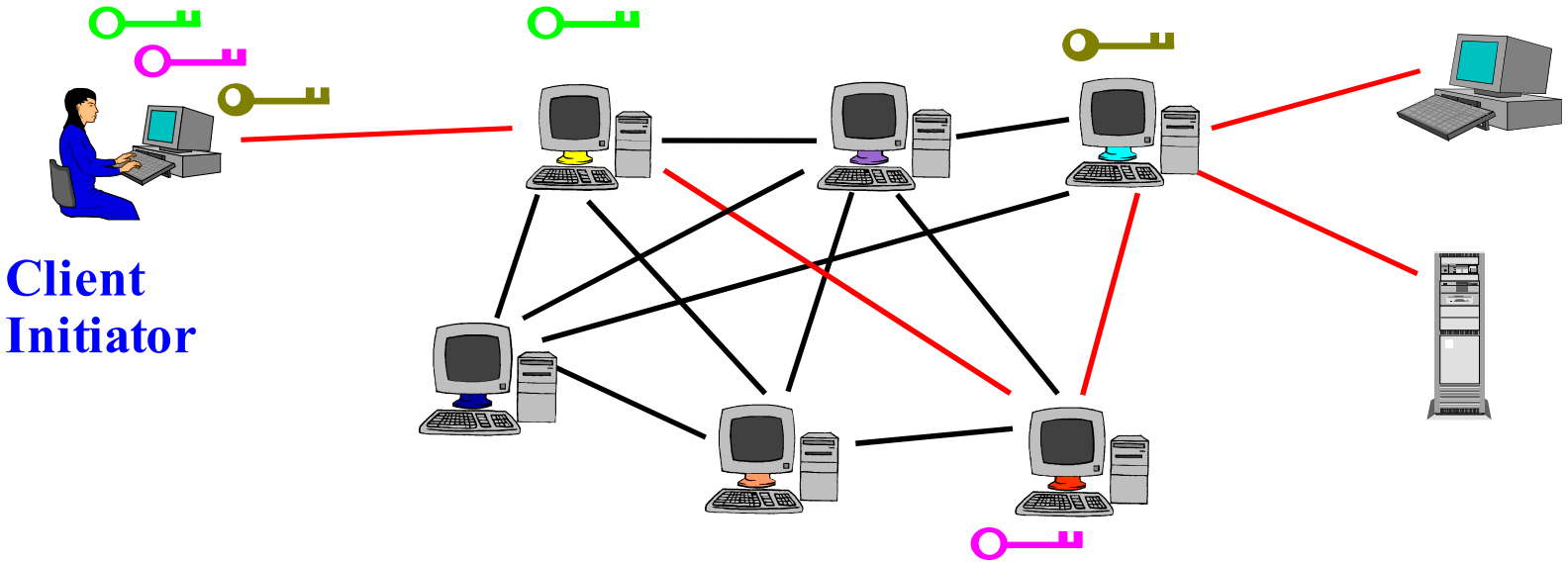
Focus of Tor is anonymity of the communication pipe,
not what goes through it

Numbers and Performance

- Running since October 2003
- 250 nodes on five continents (North America, South America, Europe, Asia, Australia)
- Volunteer-based infrastructure
- Fifty thousand+ (?) users
- Nodes process 1-90 GB / day application cells
- Network has never been down

Tor Circuit Usage

- Client Proxy establishes session key + circuit w/ Onion Router 1
- Proxy tunnels through that circuit to extend to Onion Router 2
- Etc
- Client applications connect and communicate over Tor circuit



The Tor Client

- Works like a socks proxy. So you just configure your applications to use it.
- This is great, when it works. It runs in the background, you never need to see it.
- But: when it stops working, what has gone wrong?
- And: if it's working “too” well, are you really using it?

EFF Tor Gui Contest!

- Details coming soon.
- Two phases:
  - Part one: sketches (September)
  - Part two: implementation (January)
- Winners announced at SOUPS 2006?

The Tor controller

- Client listens on a local port
- Other application(s) can connect and talk to it.
- Learn about status, get event messages (bandwidth used, logs, new servers we just learned about)
- Read and change config options
- Choose paths for each request (think about the satellite map from *Sneakers*)
- Launch Tor, put it on the system tray, shut it down, etc.
- Auto-configure applications to use / stop using it.

Use case 1: “it doesn't work”

- Don't have a working directory yet
- Can't get a working directory
- Your Internet connection is not on
- The Tor network is busted
- The exit node you picked is broken
- ...

Use case 2: “it works too well”

- How do you know if your applications aren't using it?
- Need feedback
  - Bandwidth graph?
  - Look at unencrypted stuff leaving the network?

Green bubble in system tray

- Flashes, turns red, etc if you need to know something.
- Leverage how people deal with network connection problems already.
- Bandwidth graph: show Tor usage, but also **non**-Tor usage. Show by port/application for experts? Because some things should go over Tor and some shouldn't. Let user configure which apps are which.

Etc

- Feedback should not just be informative, but give you meaningful choices for addressing problems. The other apps we recommend don't do this!
- Need to lower the barrier to being a **server**. Even experienced users really want this.
- Would be good to do configuration changes via web interface, like privoxy does.
- (Require all users to use Firefox if they want to configure Tor?)

Let people pick/see their paths

- They want this to exit in different countries, etc – censorship resistance, not anonymity.
- But give them good defaults.
- And give them some intuition about security issues.
- “Mental model” -- Tor has multiple hops, many users don't expect/realize this.

Etc

- “sockscap” interface: drag-and-drop application to “torify” it.
- A single Tor client may have many users. So plenty of work for next year too.
- Need user studies!