21- Making Anonymity Tools Usable

Lujo Bauer, Nicolas Christin and Abby Marsh

March 30, 2016

05-436 / 05-836 / 08-534 / 08-734 / 19-534 / 19-734
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

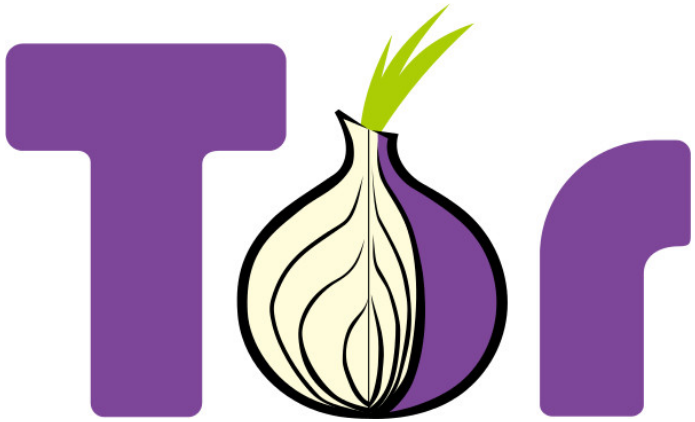
- Methods (see, e.g., Aryan et al. FOCI '13):
  - DNS hijacking / prefix hijacking
  - HTTP header (host and keyword) filtering
  - Connection throttling on SSH
  - Physical threats
  - Dropping HTTPS / TLS traffic
  - IP, Keyword, DNS poisoning
  - Deep packet inspection
  - Active probes against Tor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

Tor

- Tor
  - "The Onion Router"
  - "Tor's Onion Routing"
- Deployed anonymizing overlay network
  - Running since October 2003
  - 6,000+ relays, 3,000+ bridges on five continents
    - Nodes are regular PCs for the most part ran by volunteers
  - In excess of 2,000,000 users (2015)
- Three main functions of interest to us
  - Circuit establishment
  - Circuit usage
  - Hidden services



How does Tor work?

[Dingledine et al., 2004]

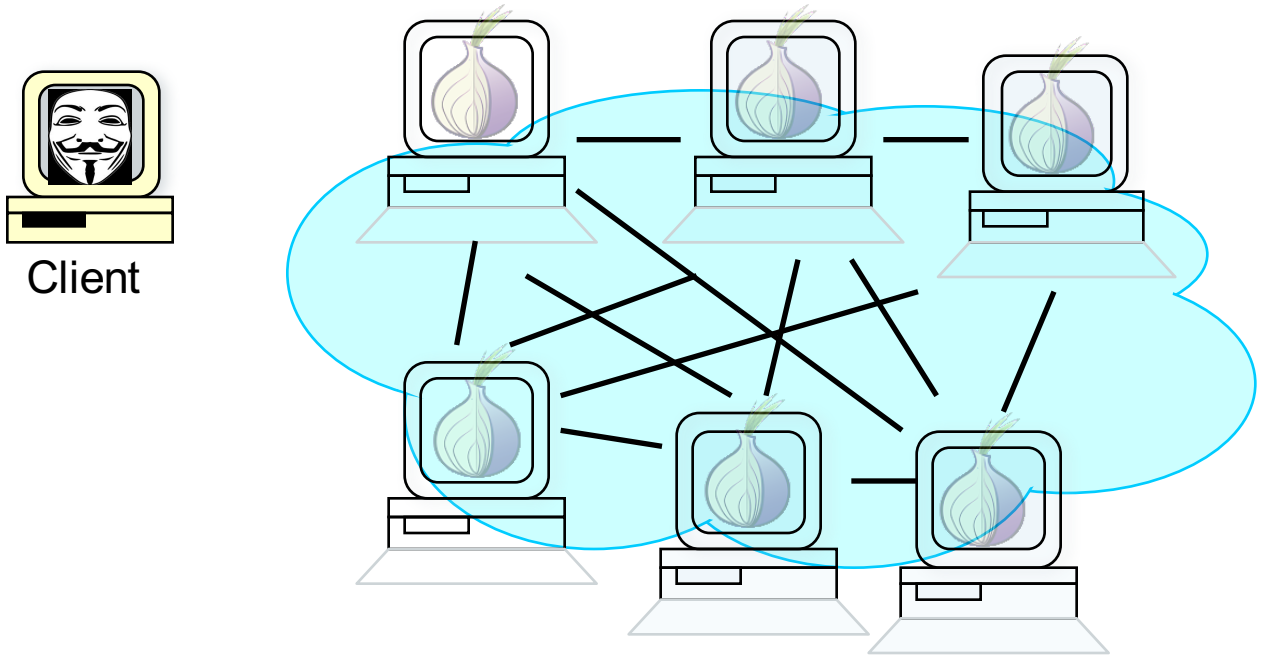
- Client first gets IP address of possible Tor entry nodes from directory server

Client

How does Tor work?

[Dingledine et al., 2004]

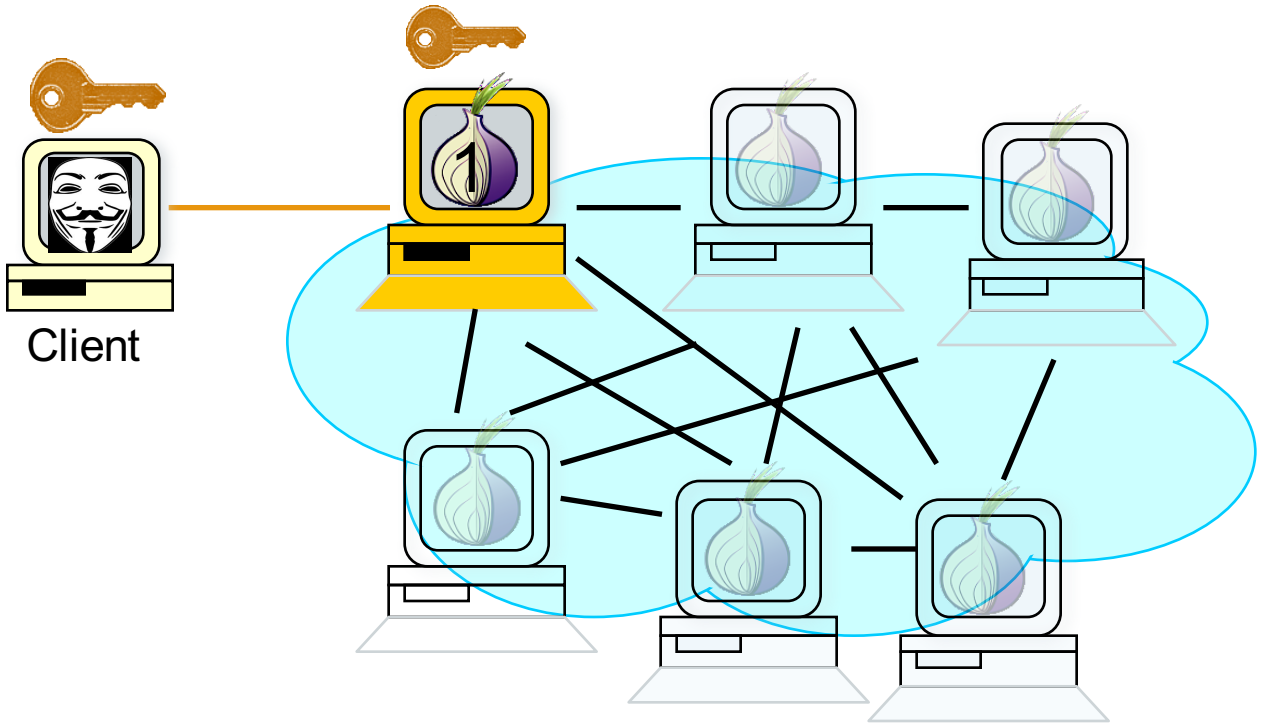
- Client first gets IP address of possible Tor entry nodes from directory server



How does Tor work?

[Dingledine et al., 2004]

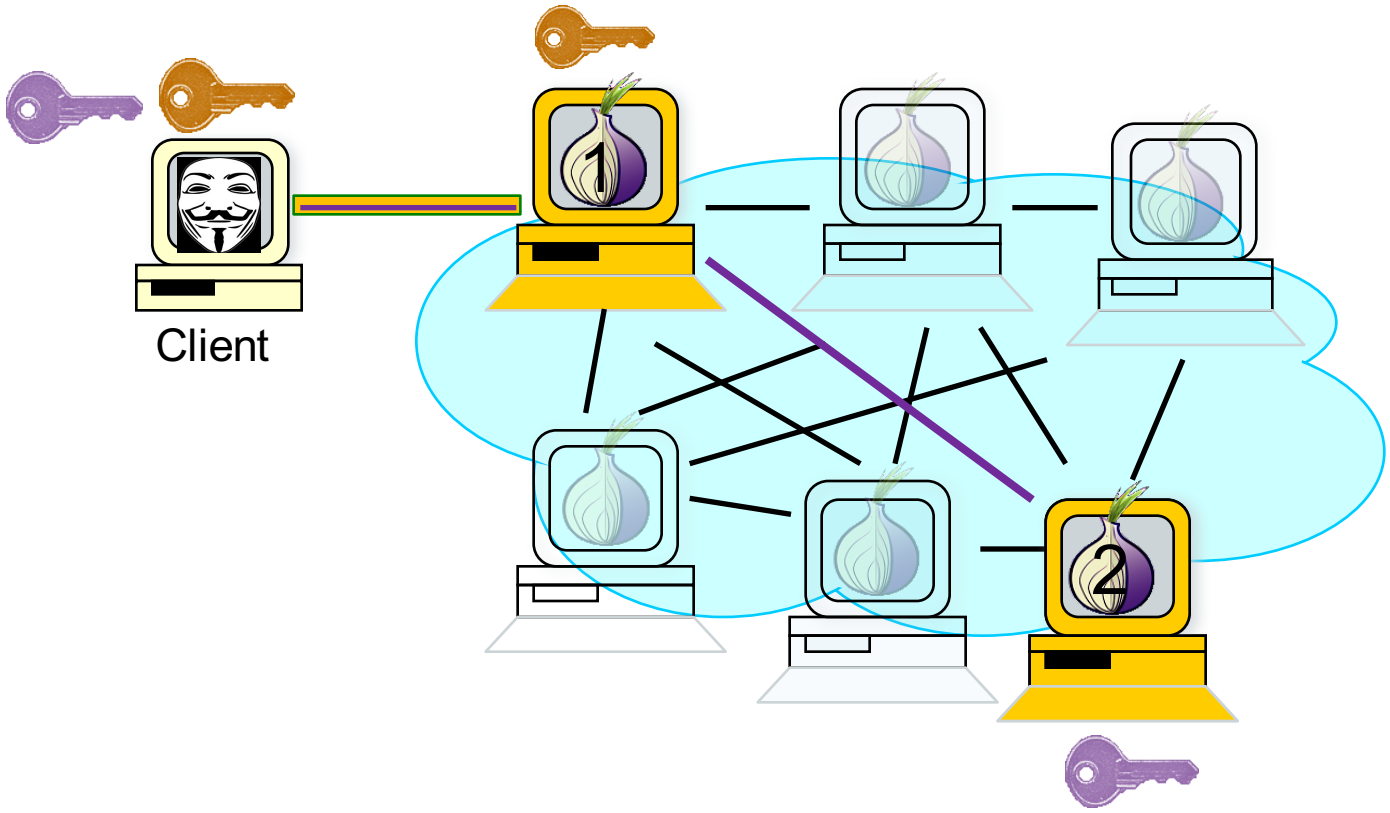
- Client proxy establishes session key+circuit w/ Onion Router 1



How does Tor work?

[Dingledine et al., 2004]

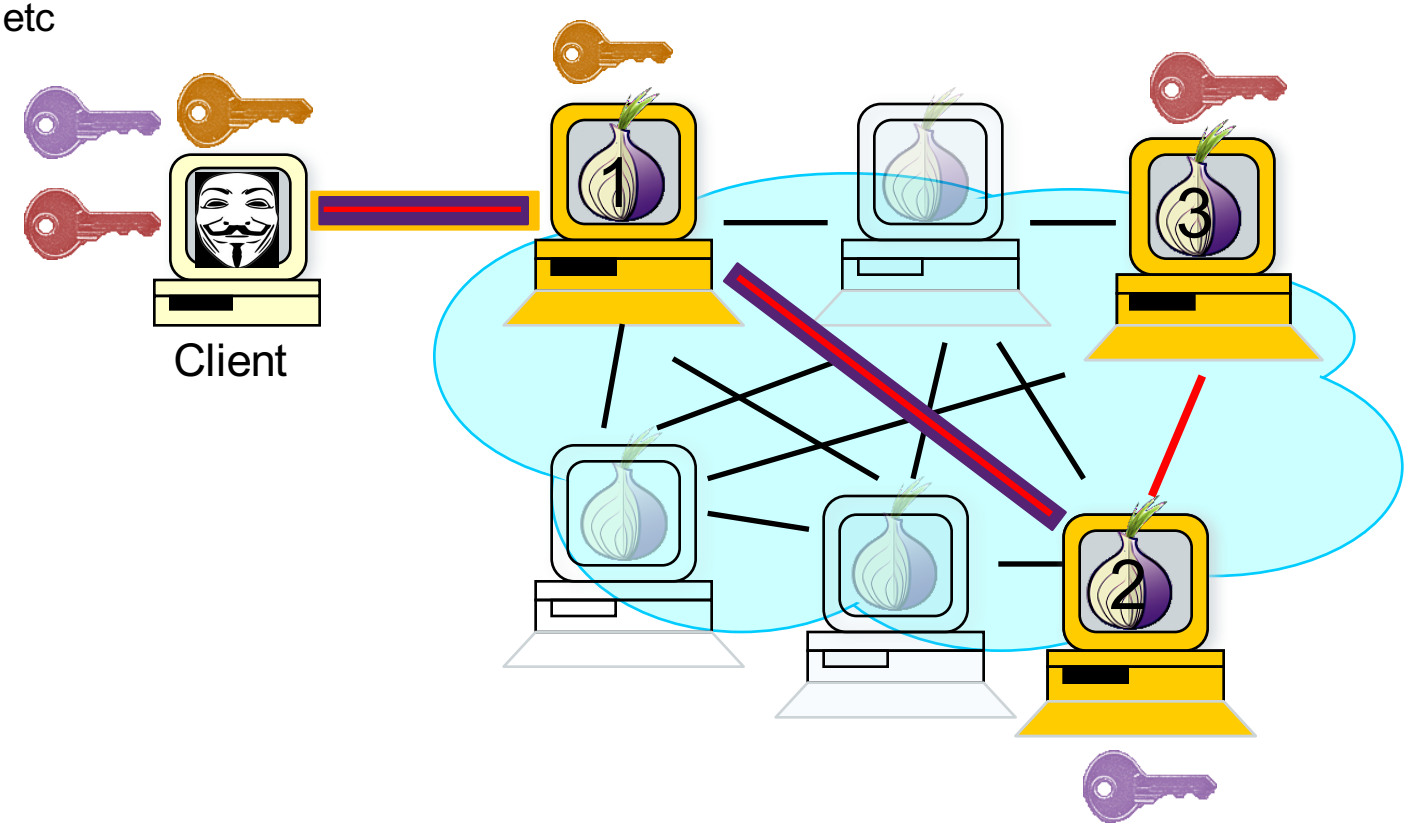
- Client proxy establishes session key+circuit w/ Onion Router 1
- Proxy tunnels through that circuit to extend to Onion Router 2



How does Tor work?

[Dingledine et al., 2004]

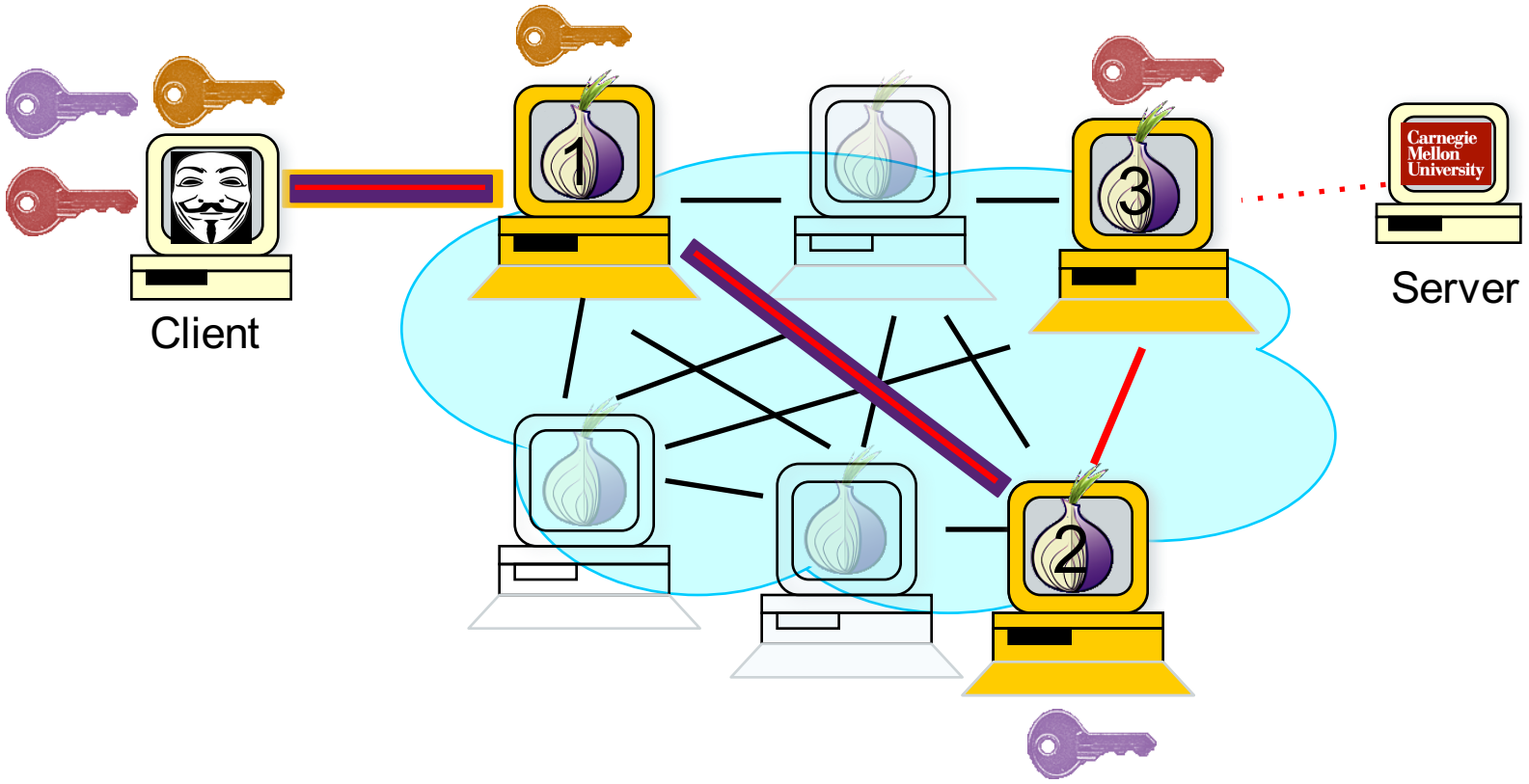
- Client proxy establishes session key+circuit w/ Onion Router 1
- Proxy tunnels through that circuit to extend to Onion Router 2
- etc



How does Tor work?

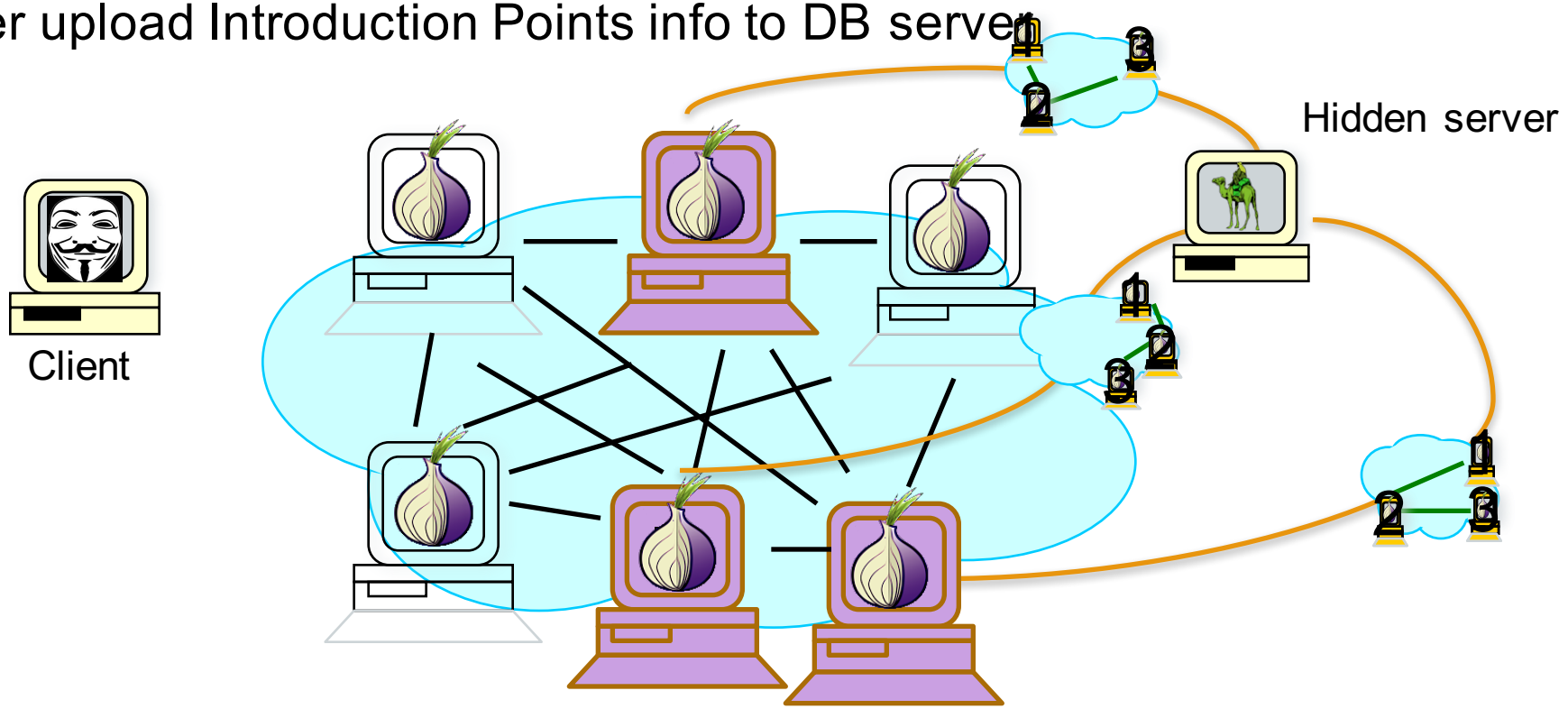
[Dingledine et al., 2004]

- Once circuit is established, applications connect and communicate over Tor circuit



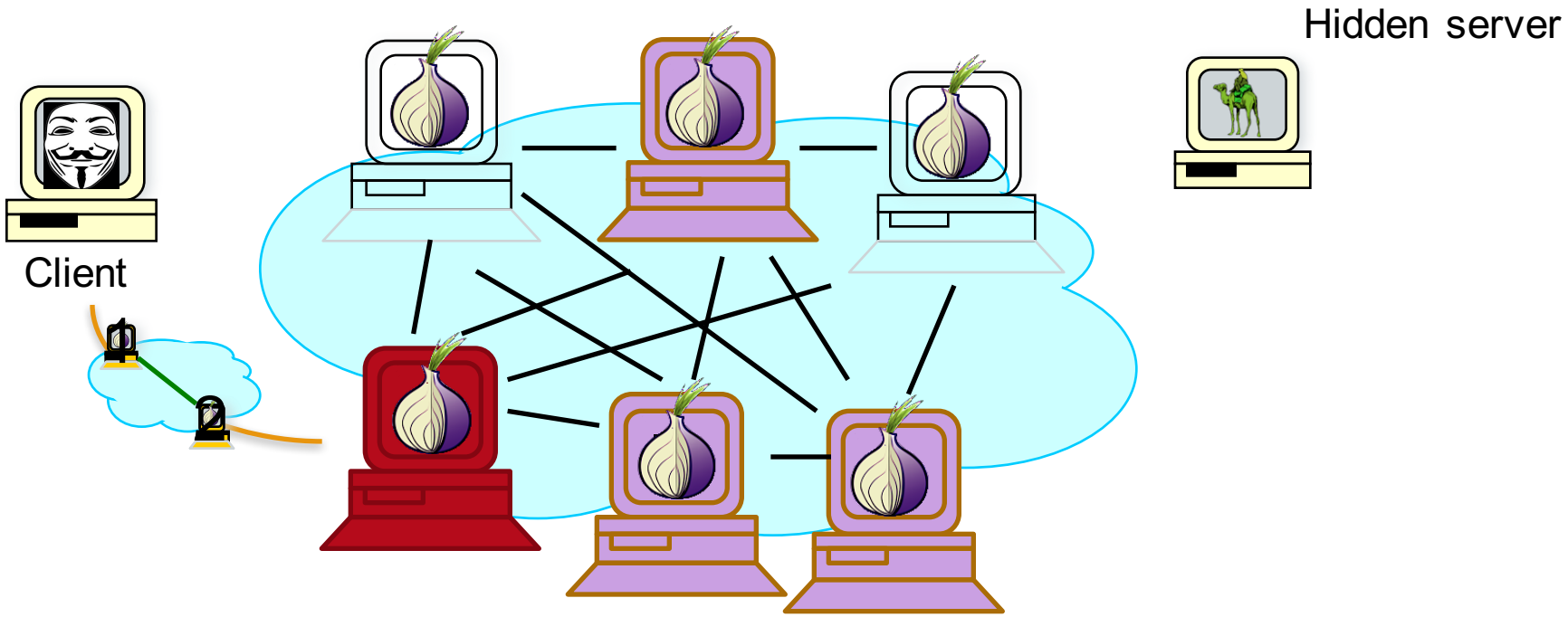
Tor: hidden services

- Hidden server uses Tor to contact 3 “introduction points” (Tor relays)
- Server upload Introduction Points info to DB server



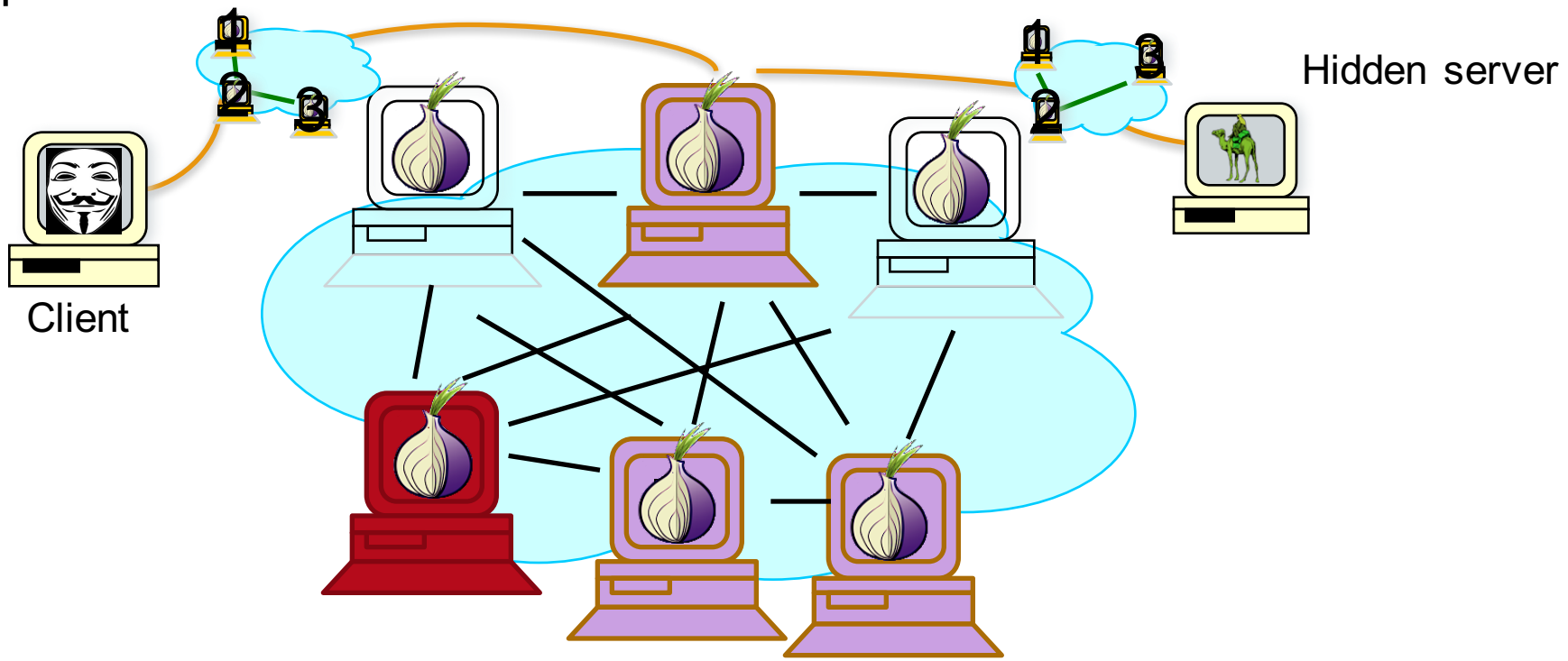
Tor: hidden services

- Client hears about hidden server, gets introduction points from DB
- Client sets up rendez-vous point (3rd node of a circuit built by client)



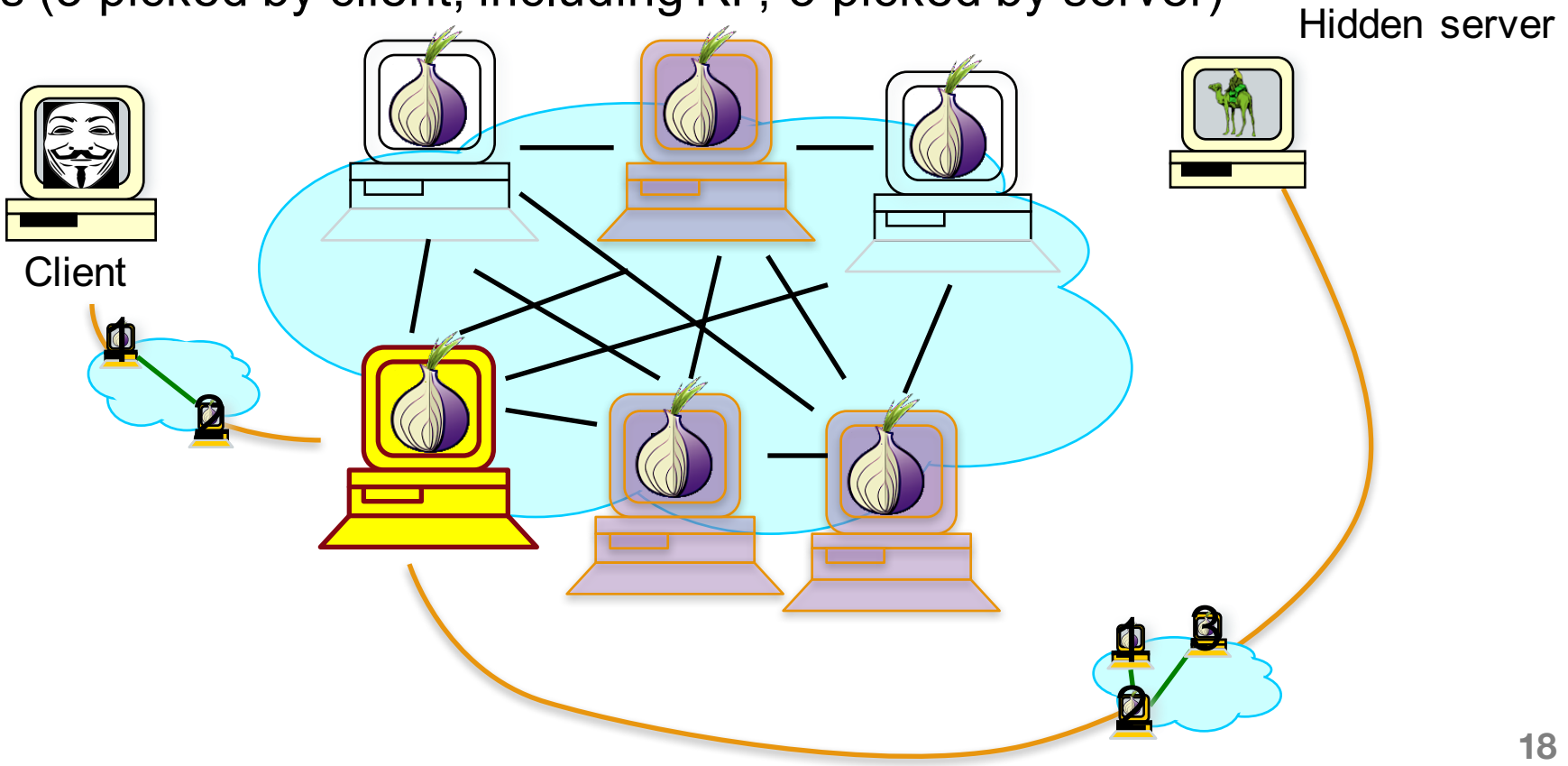
Tor: hidden services

- Client tells hidden server about Rendez-Vous Point by contacting one of the Introduction Points and asking them to relay message to server



Tor: hidden services

- Client communicate with hidden server through rendez-vous point from then on
- 6 hops (3 picked by client, including RP, 3 picked by server)



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