Anonymization Networks

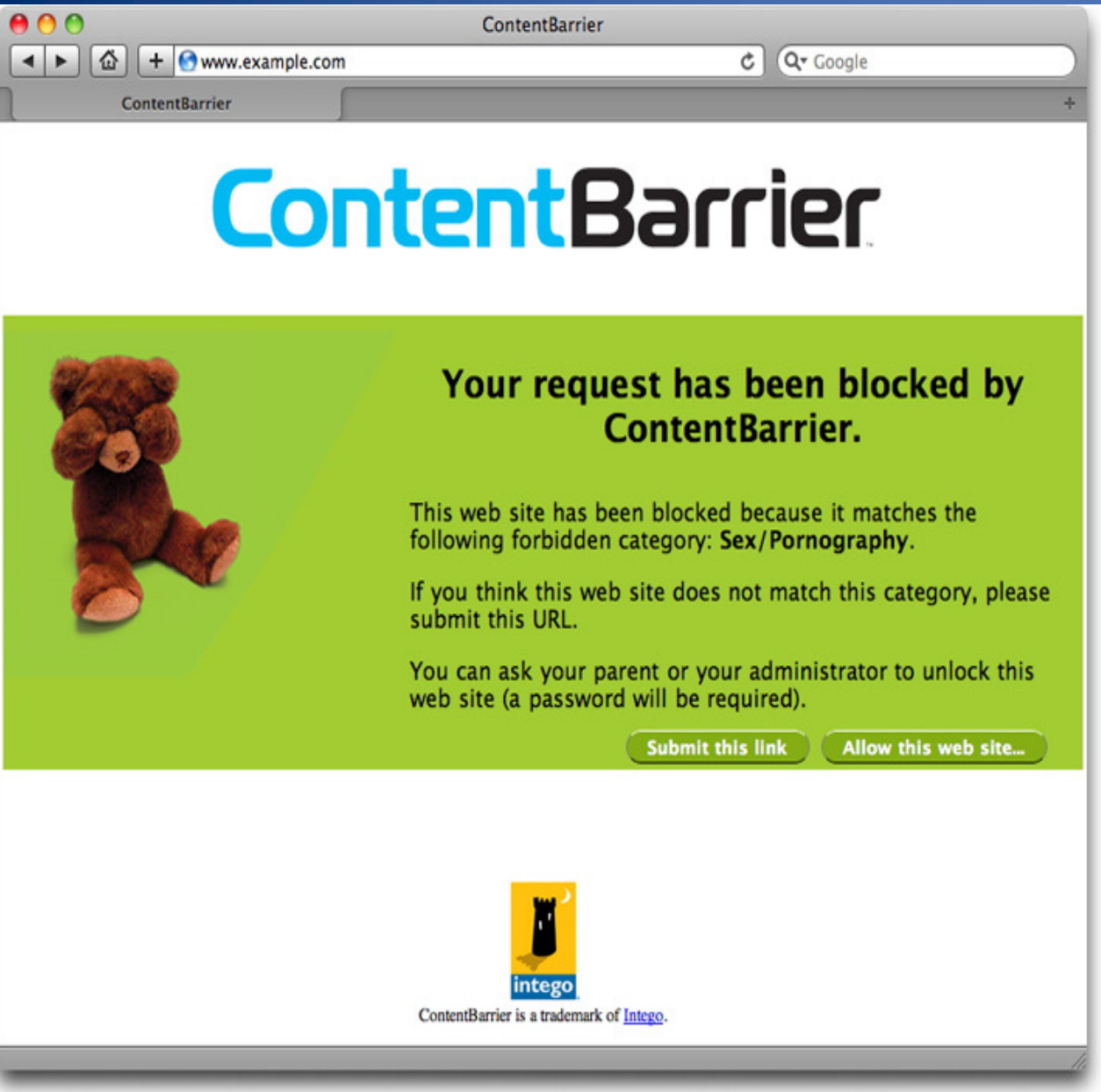
CS 1660: Introduction to Computer Systems Security

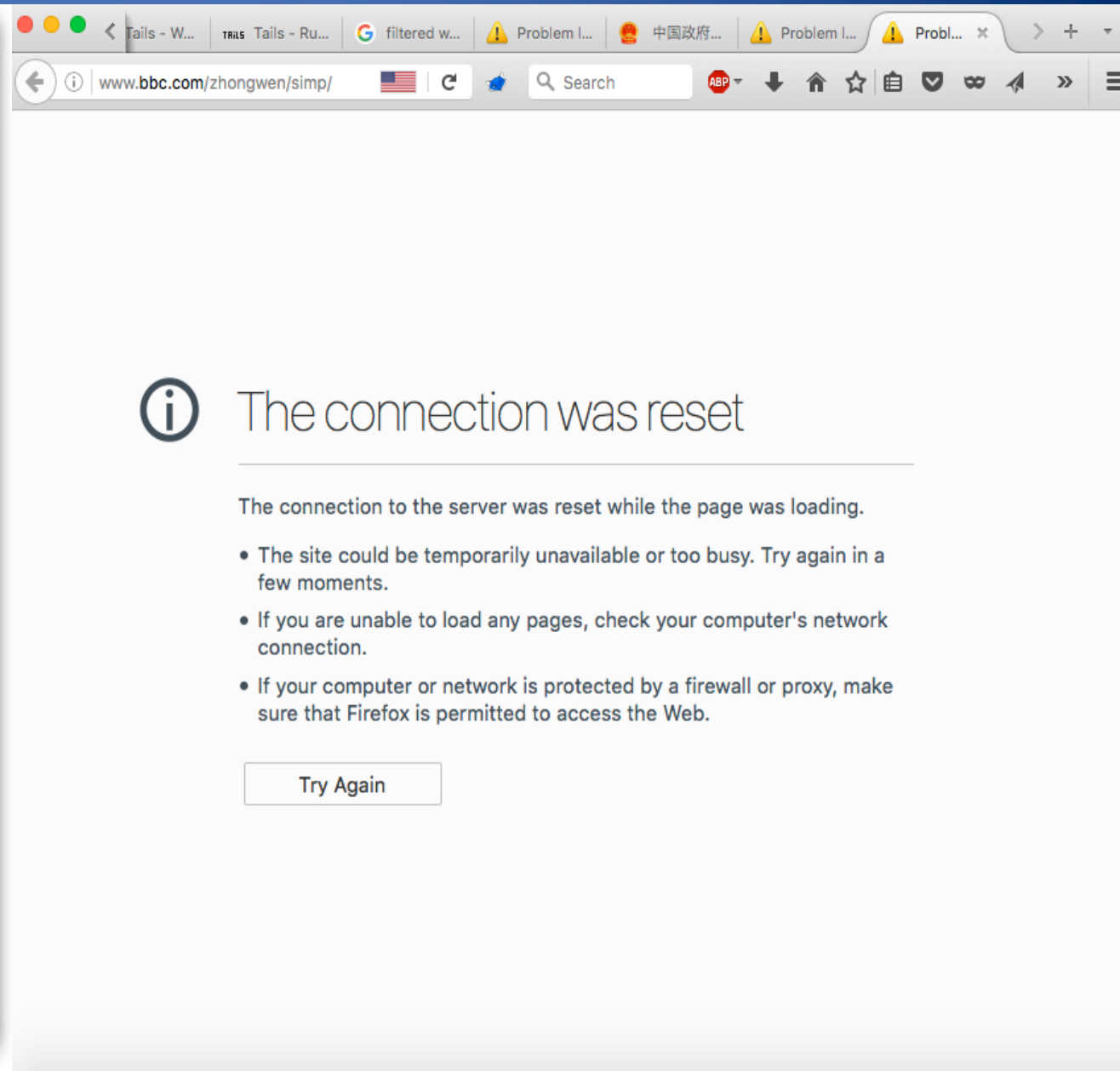
ANONYMIZATION NETWORKS

Internet Censorship

- Control or suppression of the publishing or accessing of information on the Internet
- Carried out by governments or by private organizations either at the behest of government or on their own initiative
- Individuals and organizations may engage in self-censorship on their own or due to intimidation and fear.
- Comparitech Internet Censor map 2022
  - https://www.comparitech.com/blog/vpn-privacy/internet-censorship-map/

Filtering vs. Censoring

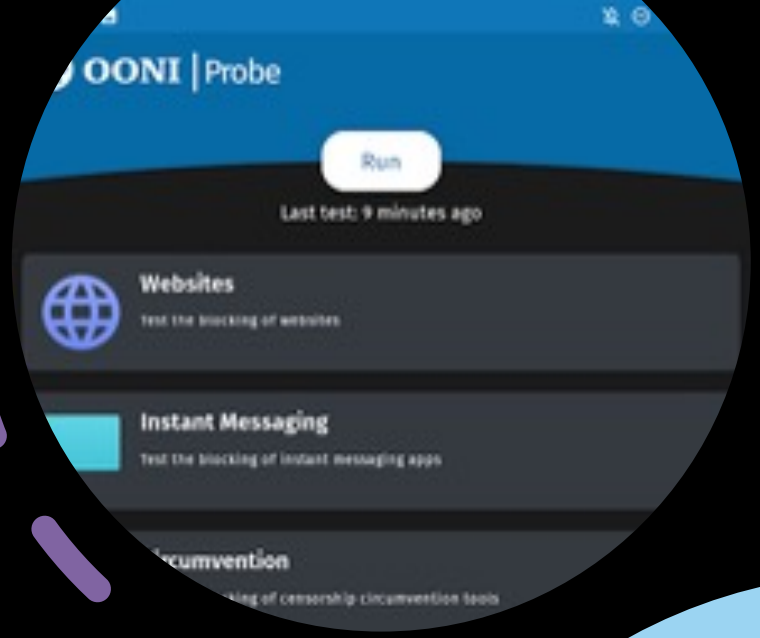




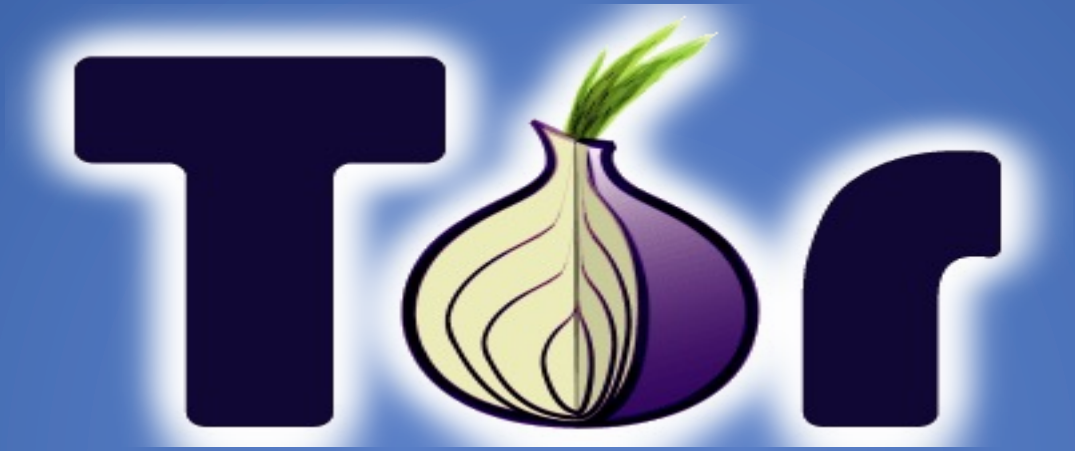
Censoring Techniques

- DNS blacklist
  - DNS does not resolve domain names or returns incorrect IP addresses, e.g., www.google.com returns 'page not found‘
- IP blacklist
  - For sites on a blacklist, the censoring system prevents connection attempts
- Keyword blacklist
  - The censoring system scans the URL string (e.g., search terms) and interrupts the connection if it contains keywords from a blacklist

OONI



- **Open Observatory of Network Interference**
- a project that monitors internet censorship globally
- https://ooni.org/



The Onion Router

Overview

- First the US Naval Research Laboratory, then the EFF and now the Tor Project (www.torproject.org)
- Access normal Internet sites anonymously, and Tor hidden services.
- Locally run SOCKS proxy that connects to the Tor network.
- *"Tor is free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as traffic analysis."* [TOR project website]

Anonymity

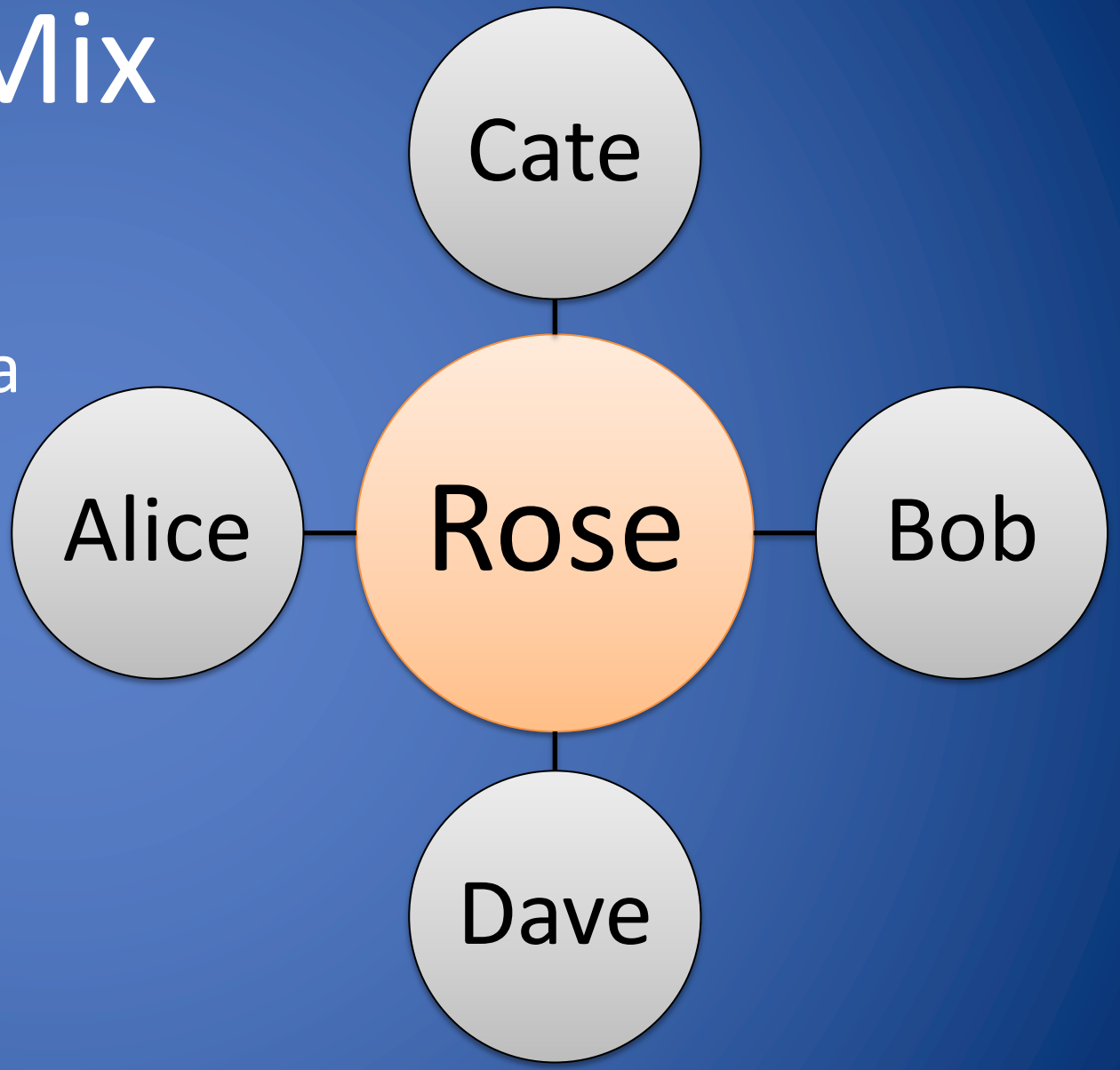
- Preventing identification within a group
  - E.g., departmental VPN, home NAT router
  - Group should be as large as possible
- Preventing association of action and identity
  - E.g., distributed denial of service by hidden attacker

Mix

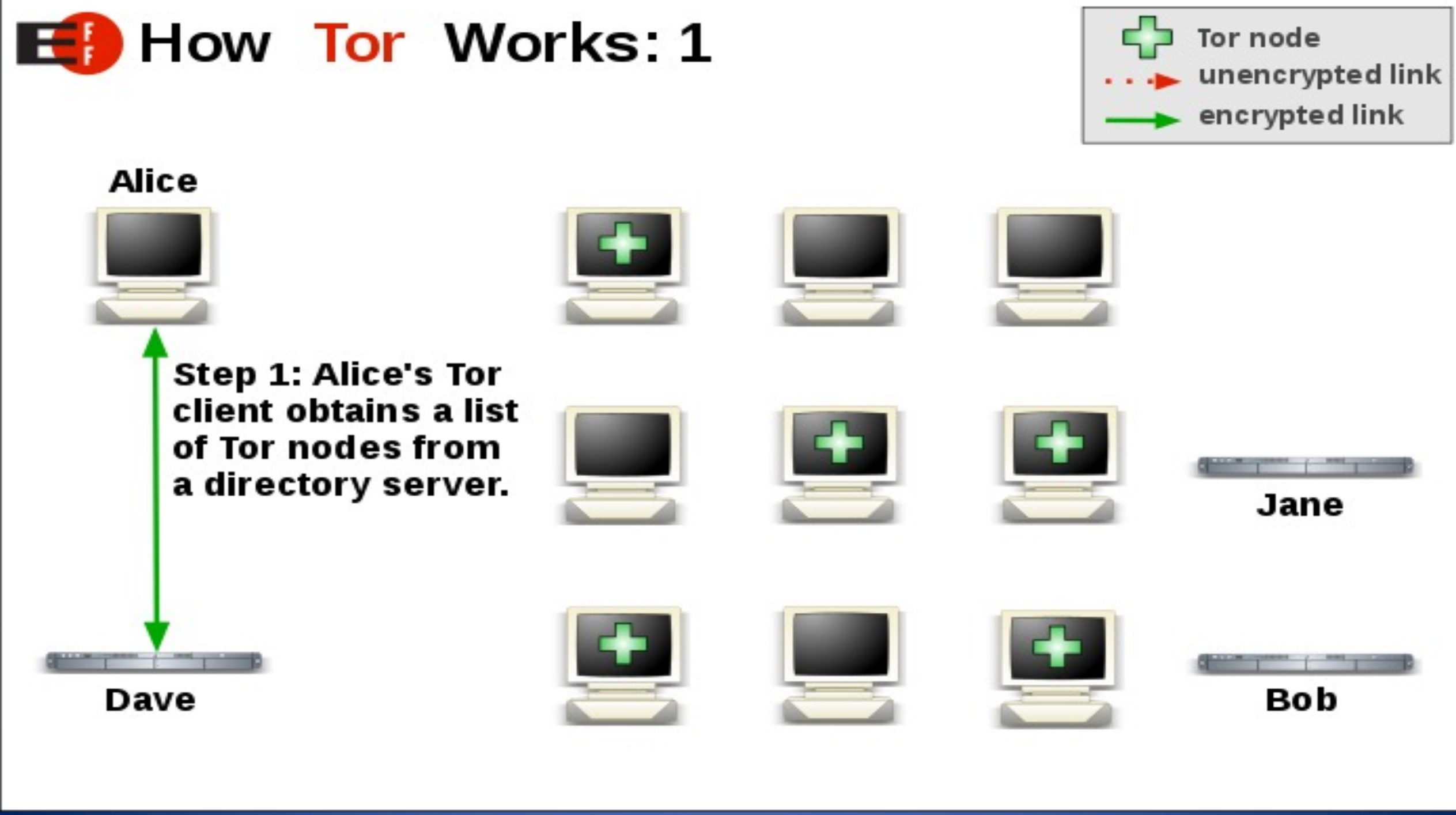
- Trusted router, Rose
- Public-key encryption
- Message from Alice to Bob via Rose

$$E_{KR}(Bob, E_{KB}(M))$$

- Precautions
  - Fixed message size
  - Continuous communication
  - Dummy messages
  - Chain of mixes

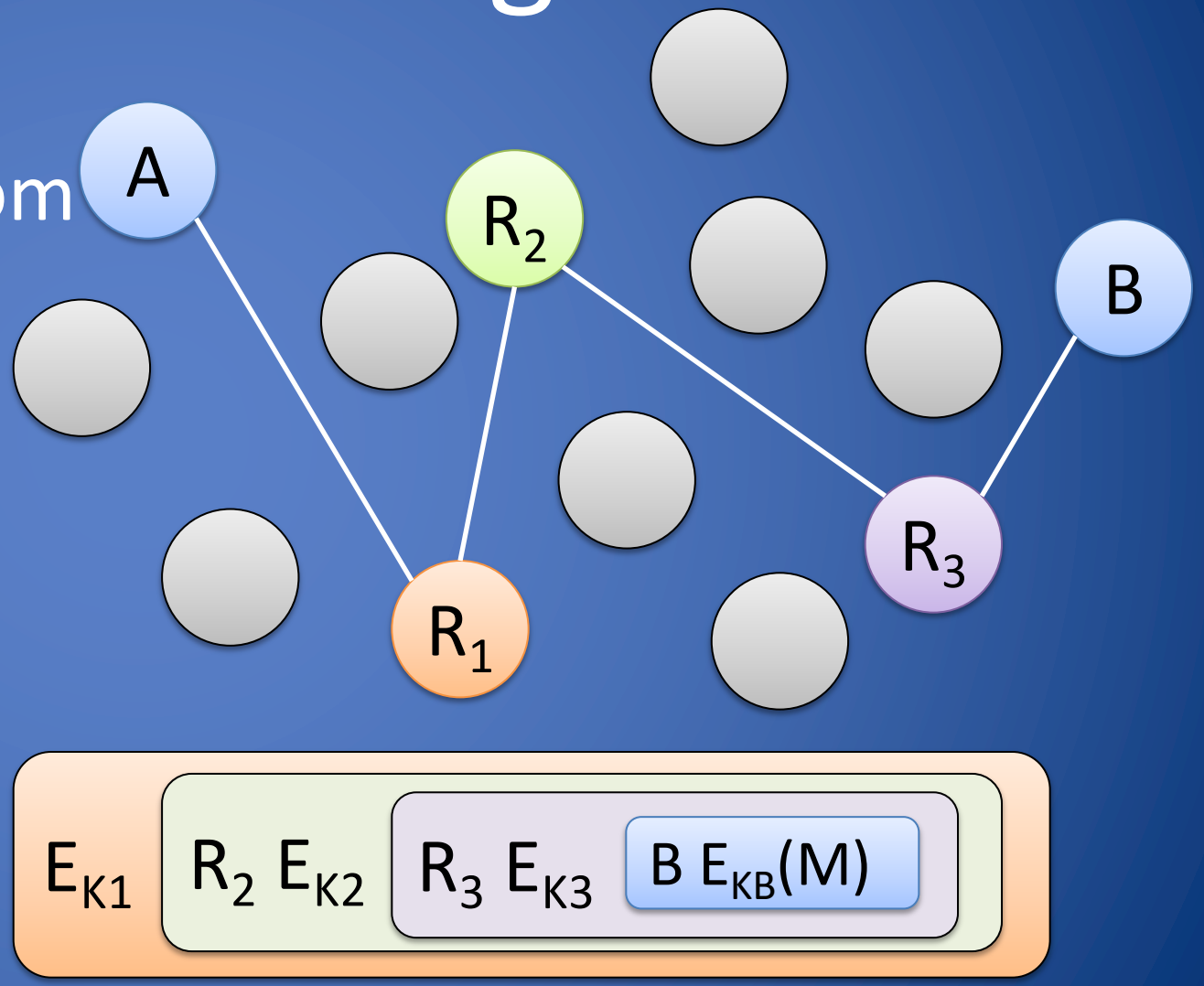


How Tor Works: 1

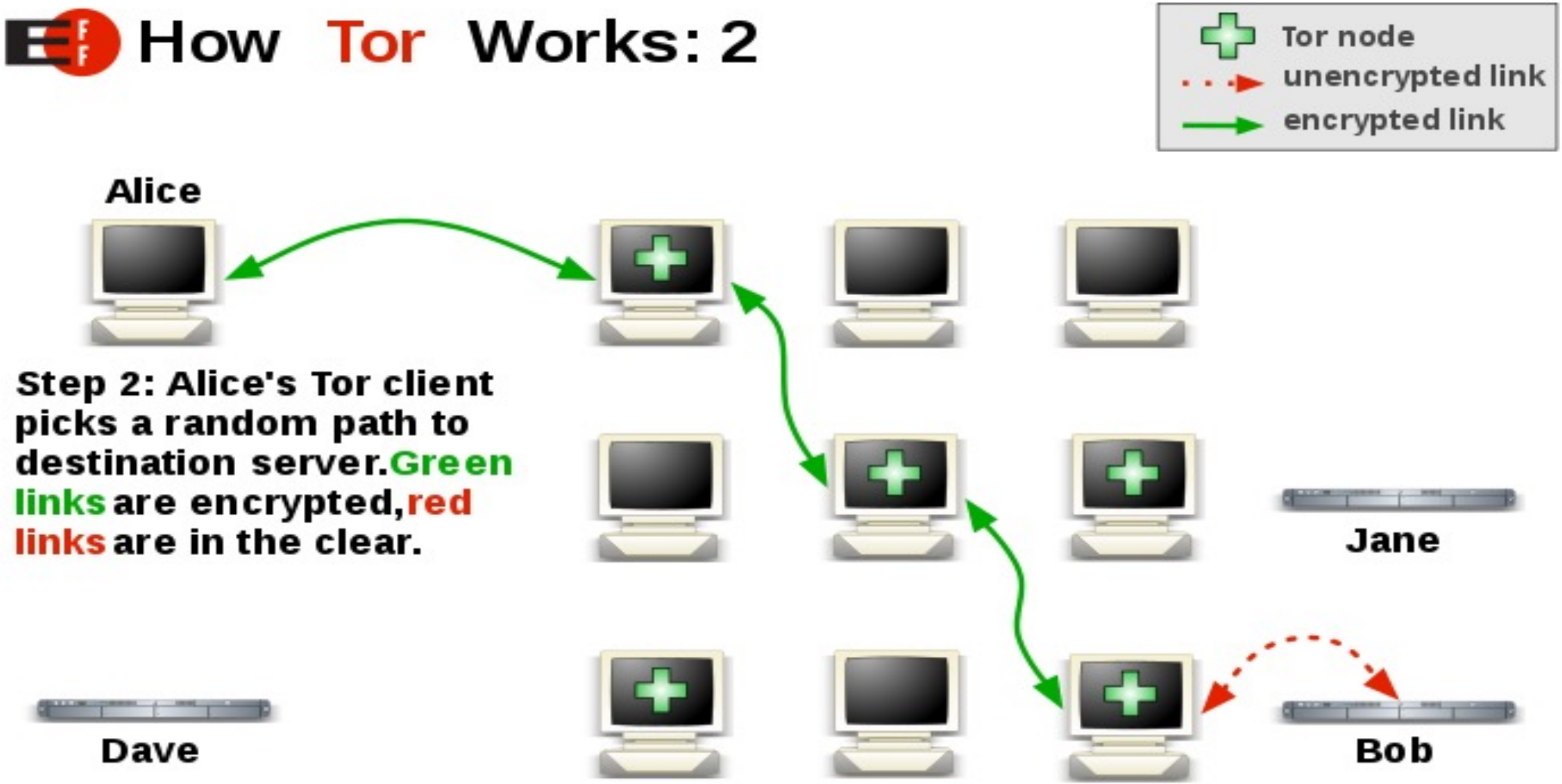


Onion Routing

- Group of routers
- Message sent via random sequence of routers
- Layered encryption
  - Build onion inside out
- Routing
  - Peel onion outside in
- Each router knows previous and next

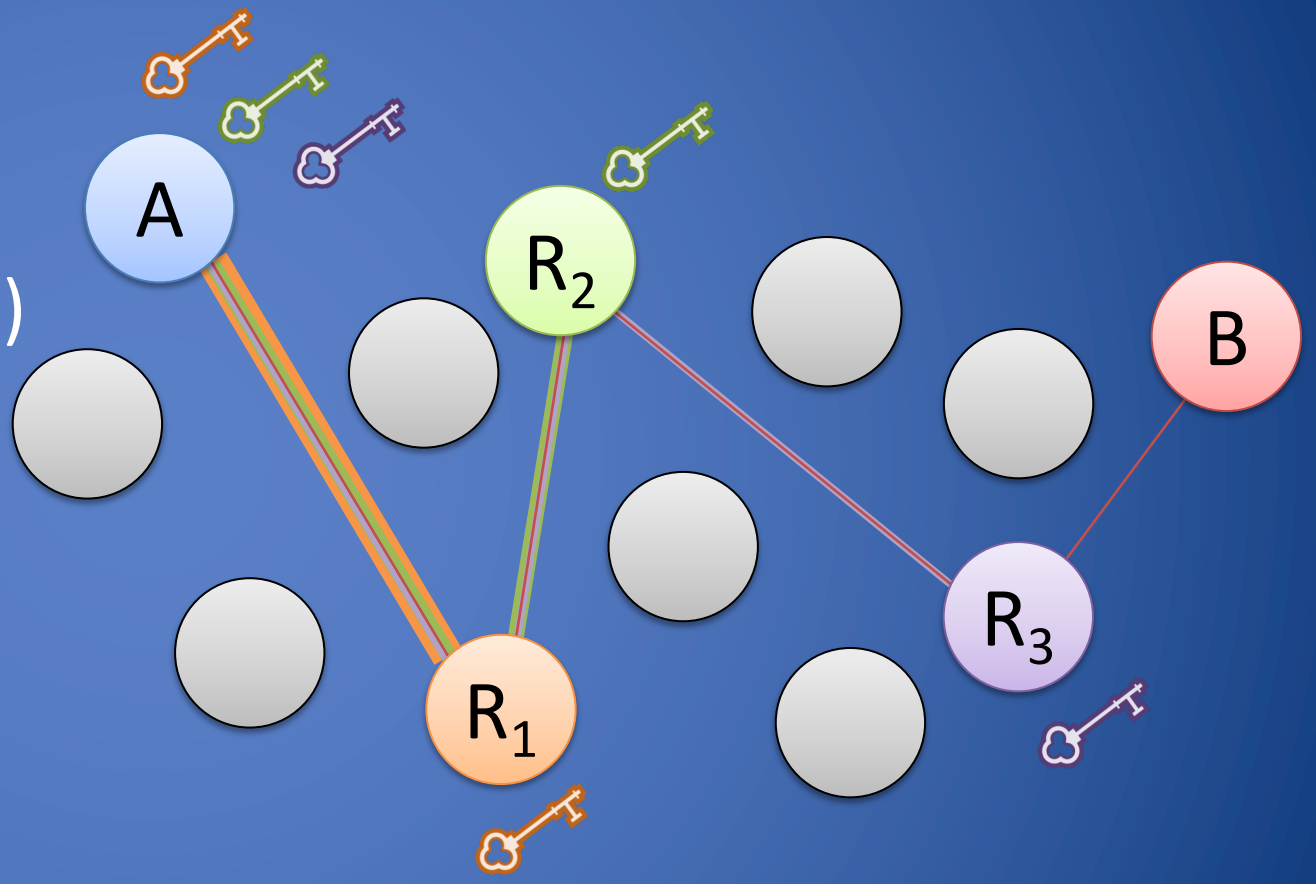


How Tor Works: 2

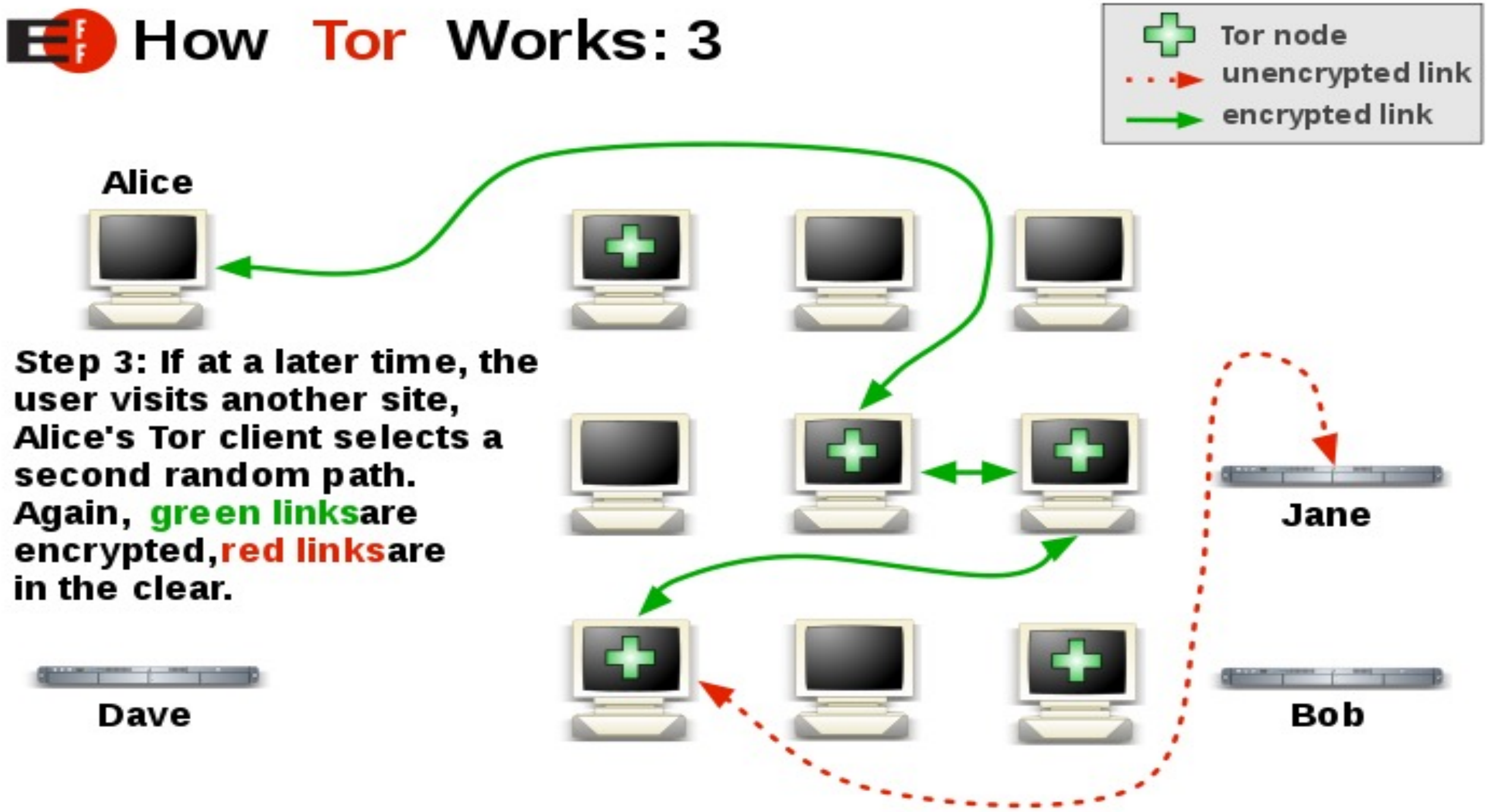


Onion Routing in Practice

- Do not encrypt final hop
  - Encryption may be done by application (e.g., https)
- Source sets up
  - Random circuit (route)
  - Symmetric keys shared with routers
- Data tunneled to final router over circuit



How Tor Works: 3



Types of relays on the Tor network

- **Guard and Middle relay**(non-exit relays)
  - –Guard relay first relay in the chain of 3 relays building a Tor circuit
  - – Middle relay acts as an intermediate hop between the Guard and exit
- **Exit relay**
  - –Final relay in a Tor circuit
  - –Eg: A website will see the exit relay IP instead of the real IP address of the Tor user
  - –Greatest legal exposure and liability of all the relays

DEMOS

- www.eff.org/pages/tor-and-https
- torproject.org
- Guard, middle, Exit nodes
- Exit nodes list
  - https://check.torproject.org/torbulkexitlist

Applications/Sites

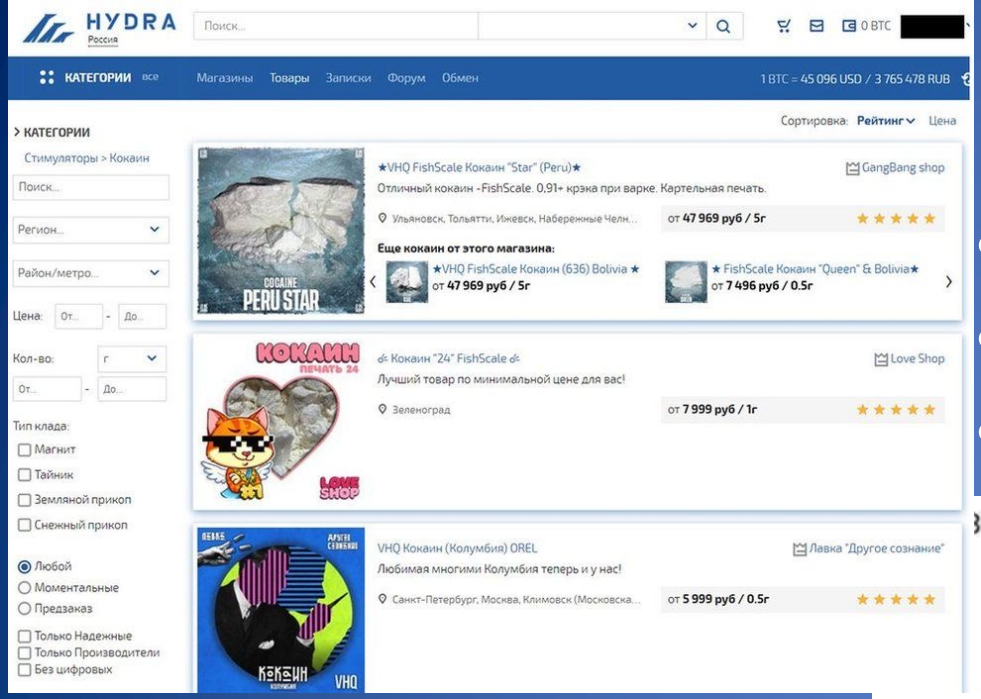
- Hidden services
  Normally websites, but can be just about any TCP connection

- Tor Hidden Service Example (Hiddenwiki) :
  http://zqktlwi4fecvo6ri.onion
- Duckduckgo.com - 3g2upl4pq6kufc4m.onion
- Facebook www.facebookcorewwwi.onion/

- .onion TLD:
  - non-mnemonic,
  - 16-character alpha-semi-numeric hashes
  - automatically generated based on a public key when a hidden service is configured
  - “vanity address” possible with expensive computation

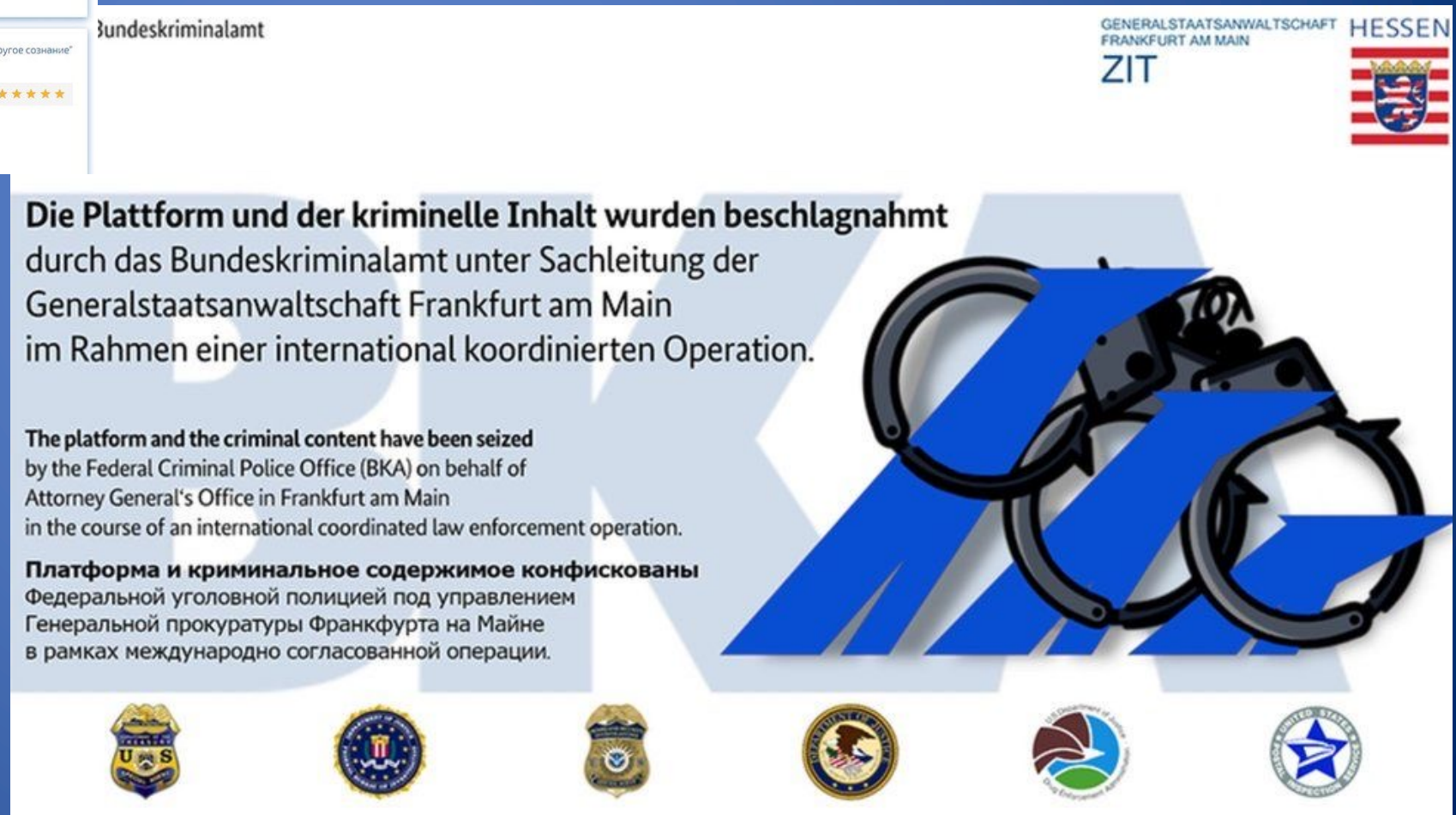
Hydra shutdown

- Started in 2015
- $5 billion in transactions
- 17 million customers & 19k seller accounts

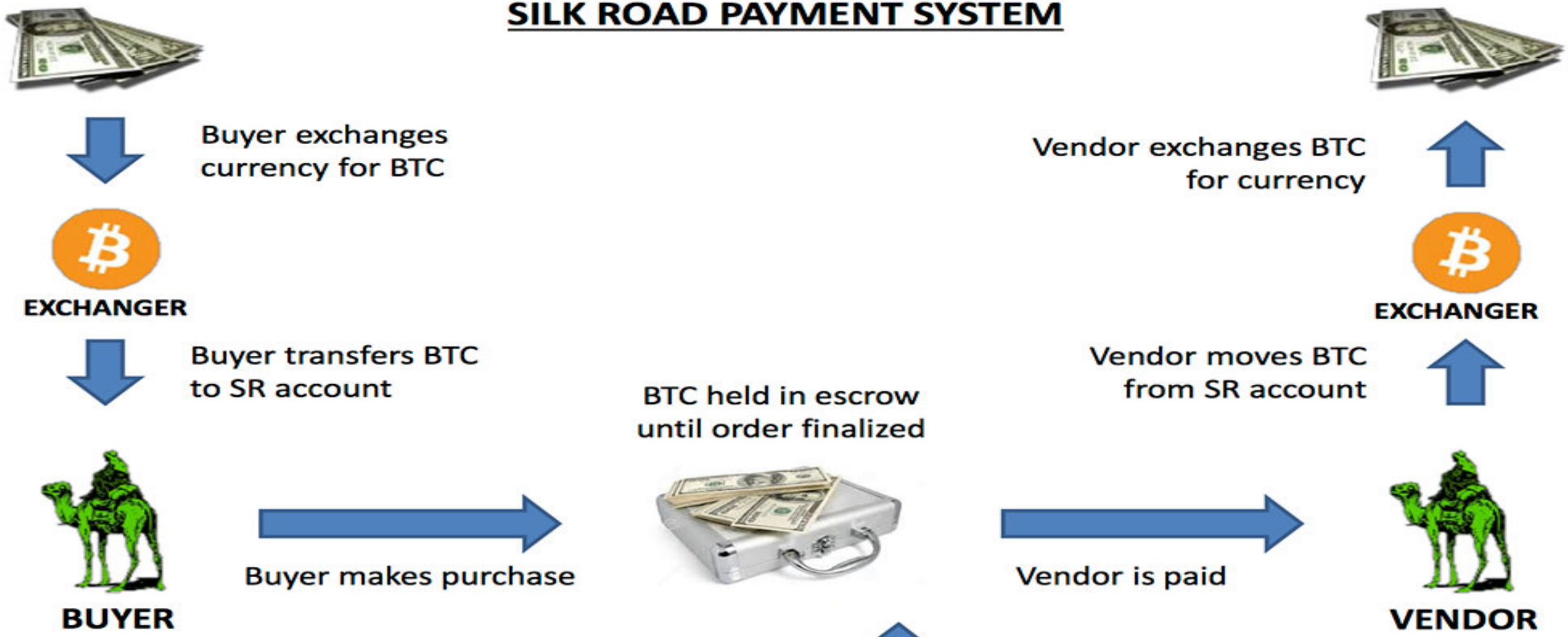


- 4/4/2022

an operation by German Federal Criminal Police (BKA)



4/22/23



Hidden marketplace

Source: https://en.wikipedia.org/wiki/Silk_Road_(marketplace)

GOVERNMENT EXHIBIT 113 A
14 Cr. 68 (KBF)

TOR Analysis

Advantages

- Tunnel, through a SOCKS proxy, allows to work any protocol.
- Three nodes of proxying, each node not knowing the one before last, makes very difficult to find the source.

Problems

- Slow (high latency)
- Exit node?
- Semi-fixed Infrastructure: possible to block all Tor relays listed in the Directory. Bridged node.
- Fairly easy to tell someone is using it from the server side
  http://www.irongeek.com/i.php?page=security/detect-tor-exit-node-in-php

Identify TOR traffic

Default configuration:

- Local
  9050/tcp Tor SOCKS proxy
  9051/tcp Tor control port
  8118/tcp Privoxy
- Remote
  443/tcp and 80/tcp mostly
  Servers may also listen on port 9001/tcp, and directory information on 9030

Clicker Question (2)

How To Block Tor? Attackers can block users from connecting to the Tor network, in which way?

A. Blocking the directory authorities
B. Blocking all the relay IP addresses in the directory
C. Filtering based on Tor's network fingerprint
D. Preventing users from finding the Tor software
E. All the above

Clicker Question (2) - Answer

How To Block Tor? Attackers can block users from connecting to the Tor network, in which way?

A. Blocking the directory authorities
B. Blocking all the relay IP addresses in the directory
C. Filtering based on Tor's network fingerprint
D. Preventing users from finding the Tor software
E. All the above

Bridge relays

- Rather than signing up as a normal relay, you can sign up as a special “bridge” relay that is not listed in any directory.
- No need to be an “exit” (so no abuse worries), and you can rate limit if needed
- Integrated into Vidalia (GUI)
- https://bridges.torproject.org/ will tell you a few based on time and your IP address
- Mail bridges@torproject.org from a gmail address and you’ll receive a few in response

Tails

- Privacy for anyone anywhere
- Linux live distro focused on Privacy
- Use the Internet anonymously and circumvent censorship
  - Tor network
- Leave no trace
  - No persistent data on the computer you are using unless you ask it explicitly
- Use state-of-the-art cryptographic tools
  - E.g., https everywhere addons

What We Have Learned

- Password-based file encryption
- Sharing encrypted files
- Container encryption and hidden containers
- Drive encryption
- Cold boot attack
- Anonymization network
- Filtering vs. Censoring
- The Onion Router (TOR)
- Hidden Service (Dark web)
- Bridge Relays