Introduction to Information Security
14-741/18-631 Fall 2021
Unit 5, Lecture 3:
Anonymous communications

Hanan Hibshi hhibshi@andrew

This Lecture's Agenda

- **Outline**
  - Motivation
    - Who needs/wants anonymity?
    - Why do they want it?
  - Mechanisms for anonymity
    - Mixnet (Chaum)
    - Anonymizing proxy
  - Practical example: Anonymous routing with Tor
- **Objective**
  - Debunk a couple of myths about anonymous communications
  - Provide you with enough background so that you can make an informed judgment on a **HOT** policy issue
  - Discuss the theory and practice behind a deployed system (Tor) for anonymous communications

The Problem

- **Public networks such as the Internet do not provide anonymity**
  - Packet headers identify recipients
  - Packet routes can be traced
- **Encryption (e.g., SSL) provides secrecy of the payload but not anonymity**
  - In particular, **encryption does not hide routing info**

Motivation: Who Needs Anonymity?

- **Activists in countries or regions where freedom of speech is not guaranteed**
  - Journalists, dissidents
  - Censorship resistant libraries
- **Main argument put forth by Ian Clarke (Freenet's designer)**
  - "We believe that the benefits of Freenet, for example for dissidents in countries such as …, …, …, far outweigh the dangers of pedophilia or terrorist information being distributed over the system" (reported by BBC news online, 9/12/2005)

… but There Are Many More!

- **Socially sensitive communicants**
  - Abuse survivors
  - People with illnesses who want to preserve their privacy
- **Law enforcement**
  - Anonymous tips, crime reporting
- **Corporations**
  - Hiding procurement suppliers/patterns

Anonymity and Privacy

- **Anonymity is very useful in preserving privacy**
  - Would you want your company to know you are looking at monster.com?
  - Would you want your ISP to know which websites you are browsing? (newsflash: they do)
    - Browsing habits are a goldmine for people harvesting private information…

Does Government Need Anonymity?

- **It may, for…**
  - Anonymous crime reporting
  - Intelligence gathering
    - If a lot of help is needed, don't necessary want to know that the source of a request is the government
  - Defense in depth on open and classified networks
    - Origin of the message may be more important than the message itself
  - Dynamic international coalitions
    - Don't want participants in the network to be able to figure the identities of **all** participants (diplomatic conduits)
  - Elections and voting

Myth 1: Anonymous Networks Foster Crime

- **Criminals love anonymity…**

  … but they are not shy of using illegal means toward obtaining it!

  - Stolen identities
  - Fake passports
  - Phone relays
- **Or even subverting legal means**
  - Disposable email accounts, cell phones…
  - …
- **Do they really need anonymous communication primitives?**

Myth 2: Anonymity & Crackers

“Having anonymous communications will facilitate the job of crackers and other script-kiddies that break into our systems, given that they will not be traceable.”

Myth 2: Anonymity & Crackers

"Having anonymous communications will facilitate the job of crackers and other script-kiddies that break into our systems, given that they will not be traceable."

- **They already are not**

(provided they know what they are doing):

- Break into system
- Destroy all logs
- Use system broken into to break into more systems
- Destroy all logs
- etc

Myth 3: Anonymous Networks are Completely Harmless

- **Systems like Tor have been used in some instances for more than questionable purposes**
  - Circulate illegal pornographic material in P2P networks
  - Ransom note on Hotmail
  - Silk Road, Farmers' Market, Sheep, BMR and other black markets
- **And of course…**
  - Copyright infringement
- **According to the Tor advocates, minor, rare, incidents**
- **According to conversations with Tor node operators, mostly minor incidents, but maybe not so rare**
  - Interesting measurement study… (which to some extent has been done)
  - But completely illegal in most countries (wiretapping)

Interesting Policy Questions

- **Does the good coming from the availability of anonymous communications outweigh the bad?**
- **If not, should we make engineering anonymous networks illegal?**
  - But, as we will see, they basically rely on crypto, so…
  - Should we make crypto illegal as well?
  - Should we restrict engineering/design?
- **I can't provide you with any answers here**

  (my own opinion does not matter)
- **Form your own judgment!**

Private Browsing Mode

- **Browsers create a separate temporary session**
  - Browsing history is not saved
  - cookies are cleared
  - data does not stay on the device
- **When is this useful?**
- **When is this not useful?**

- **What about anonymous communication?**

Anonymous from Whom?

- **Sender remains anonymous to the recipient of the message**
- **Recipient remains anonymous to the sender of the message**

⇒ **Need channel and data anonymity**

- **Sender/receiver anonymous to**
  - Observer of network from the outside
  - Network infrastructure

⇒ **Need channel anonymity**

Notes: Anonymous authenticated communication makes perfect sense

Communication Anonymity

- **Many technical approaches**
- **Focus here on (commonly used)**
  - Mixes (a.k.a. mixnets)
    - Originally proposed by David Chaum at UC Berkeley around 1980 for untraceable email
  - Proxies
    - Generally used by web browsing anonymizing services

Chaum Mix (1981)

(Envelopes are sealed using the recipient's public key)

Minnie (Mix)

Alice

Bob

Chaum Mix (1981)

(Envelopes are sealed using the recipient's public key)

Minnie (Mix)

Alice

Bob

Chaum Mix (1981)

(Envelopes are sealed using the recipient's public key)

Minnie (Mix)

Alice

Bob

Chaum Mix (1981)

(Envelopes are sealed using the recipient's public key)

Minnie (Mix)

Alice

Bob

Chaum Mix (1981)

(Envelopes are sealed using the recipient's public key)

Minnie (Mix)

Alice

Bob

Chaum Mix (1981)

(Envelopes are sealed using the recipient's public key)

Minnie (Mix)

Alice

Bob

Chaum Mix

- No one but Minnie knows the author of the original letter
- However, an observer could easily guess it is Alice by observing that Alice sent something to Minnie shortly before Minnie sent it to Bob

Chaum Mix w/ Multiple Participants

Alice

Bob

Carol

Minnie (Mix)

Ed

Nameless guy

Jeff

(Envelopes are sealed using the recipient's public key)

Chaum mix w/ Multiple Participants

Alice

Bob

Carol

Minnie (Mix)

Ed

Nameless guy

Jeff

(Envelopes are sealed using the recipient's public key)

Chaum mix w/ Multiple Participants

Alice

Bob

Carol

Minnie (Mix)

Ed

Nameless guy

Jeff

(Envelopes are sealed using the recipient's public key)

Chaum mix w/ Multiple Participants

Alice

Carol

Nameless guy

Minnie (Mix)

Bob

Ed

Jeff

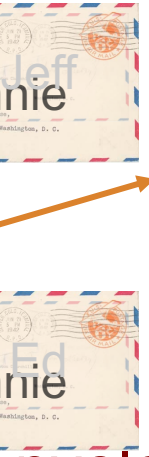
(Envelopes are sealed using the recipient's public key)

Chaum mix w/ Multiple Participants

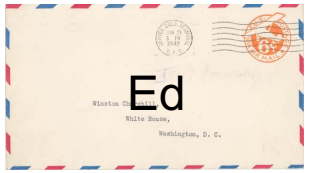
Alice

Carol

Nameless guy



Minnie (Mix)



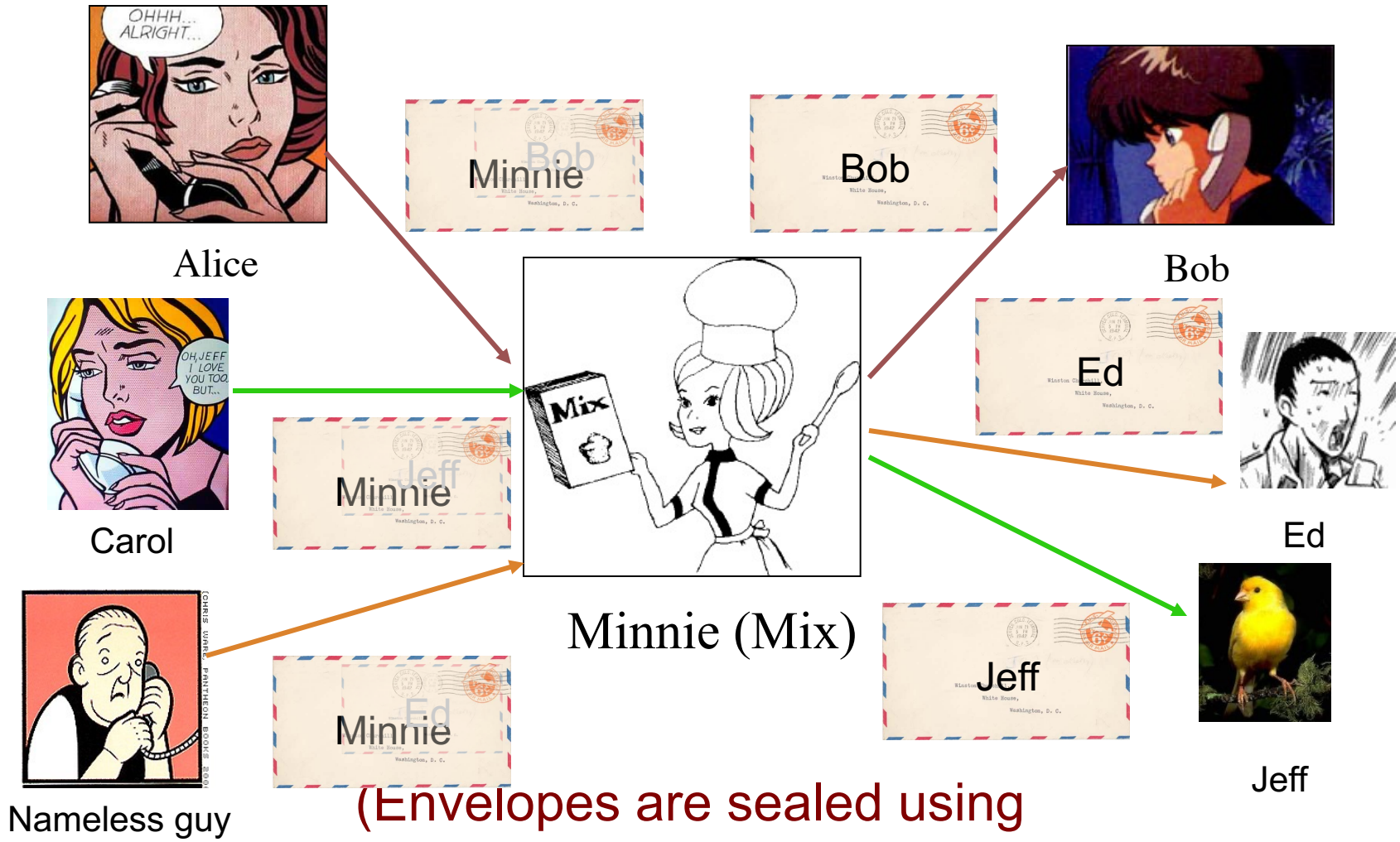
Bob

Ed

Jeff

(Envelopes are sealed using the recipient's public key)

Chaum mix w/ Multiple Participants



Chaum mix w/ Multiple Participants

- Mix (Minnie in the example) reorders messages (e.g., in lexicographic order)
- Only Minnie knows who is talking to whom (but she doesn't know the content of the message)
- Note that Minnie can actually be part of the people talking if she can use another mix herself (e.g., if Alice can perform the functions of a mix)

Challenge #1

- What if Alice sends 7 messages for Bob, Carol 3 messages for Jeff, and the nameless guy 1 message to Ed?

Challenge #1

- What if Alice sends 7 messages for Bob, Carol 3 messages for Jeff, and the nameless guy 1 message to Ed?
- One can figure out who is talking to whom by simply counting the number of messages coming in and out of the mix for each input and each output

Dummies

- **What if Alice sends 7 messages for Bob, Carol 3 messages for Jeff, and the nameless guy 1 message to Ed?**
- **One can figure out who is talking to whom by simply counting the number of messages coming in and out of the mix for each input and each output**
- **One way of solving the problem is to have the mix output 7 messages to Bob, Ed, and Jeff…**
  - Dummy messages for padding

Challenge #2

- Minnie knows who is talking to whom
- What if Minnie is malicious?

Challenge #2

- Minnie knows who is talking to whom
- What if Minnie is malicious?
- Use a cascade of mixes = a mixnet

Mixnet

Mix 1

Mix 2

Mix 3

Bob,
Ed,
Jeff,
…

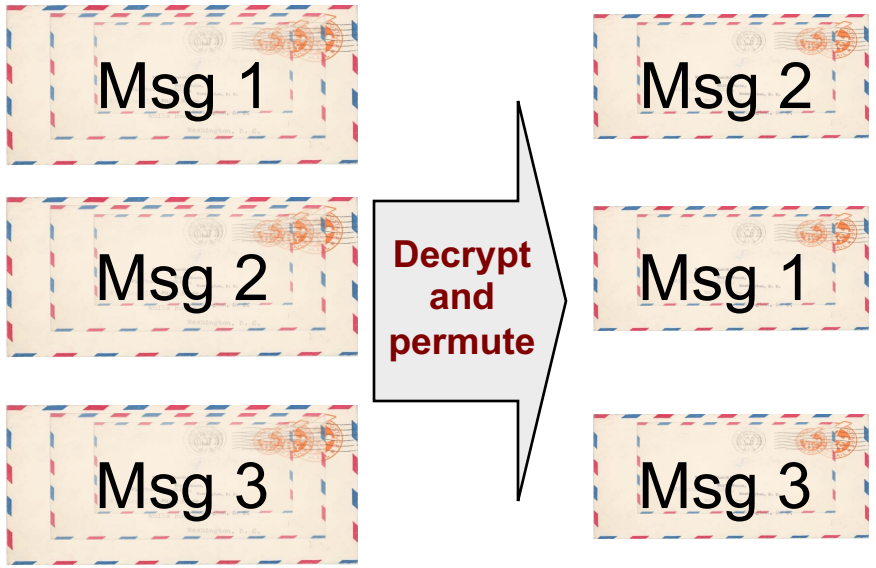
Mixnet

Mix 1

Mix 2

Mix 3

Bob,
Ed,
Jeff,
…



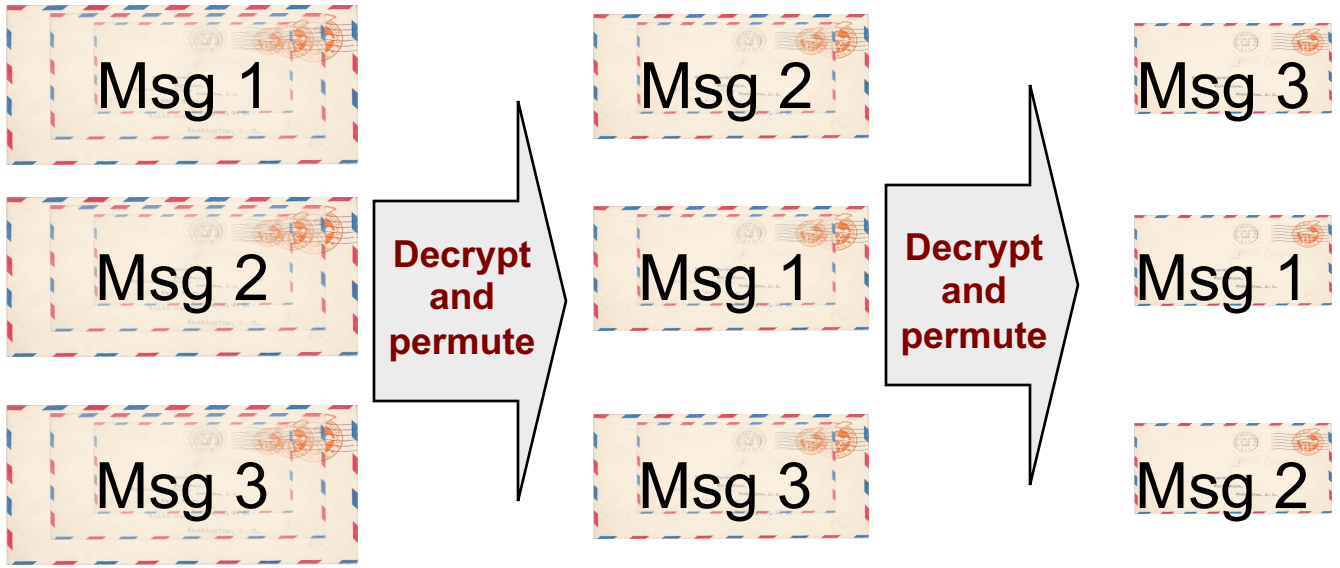
Mixnet

Mix 1

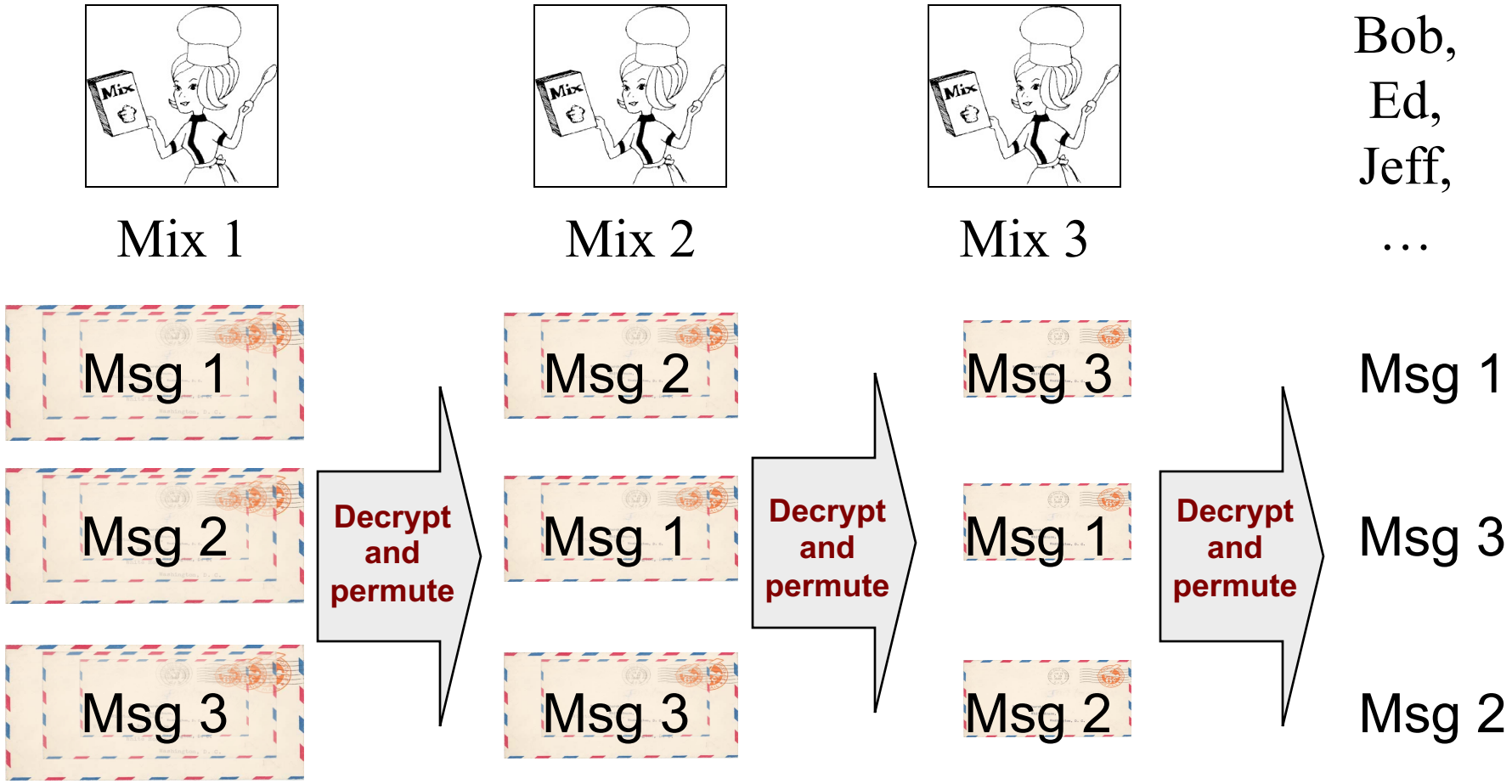
Mix 2

Mix 3

Bob,
Ed,
Jeff,
…



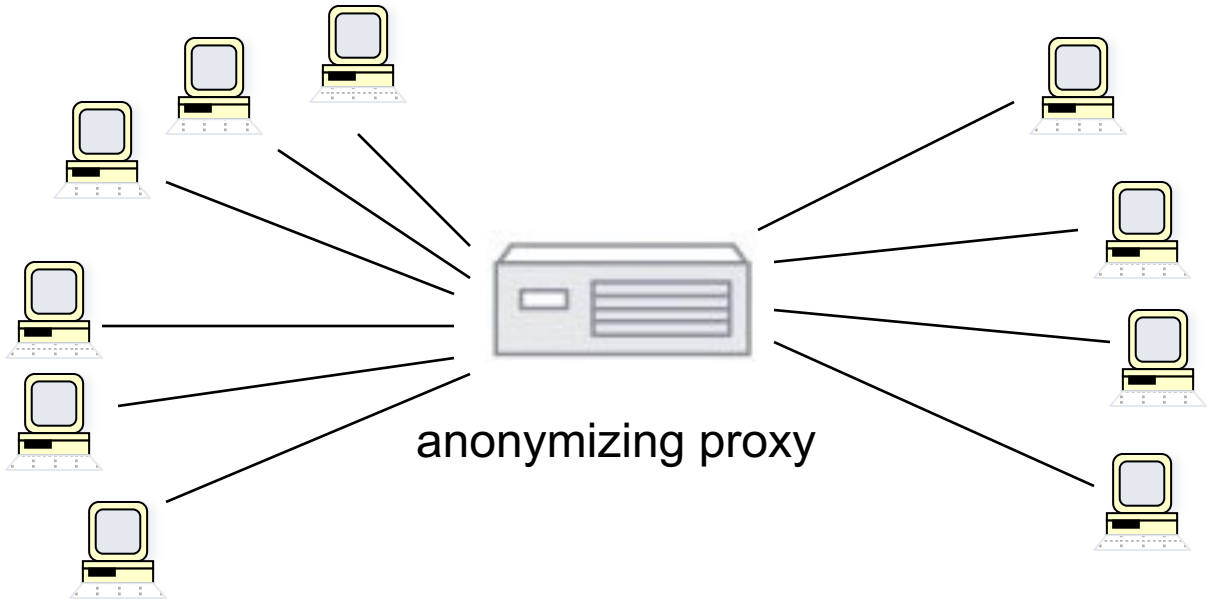
Mixnet


Mix 1
Mix 2
Mix 3
Bob,
Ed,
Jeff,
…
Msg 1
Msg 2
Msg 3
Decrypt and permute
Msg 2
Msg 1
Msg 3
Decrypt and permute
Msg 3
Msg 1
Msg 2
Decrypt and permute
Msg 1
Msg 3
Msg 2

Mixnets

- **Advantages**
  - Only one honest server is needed to preserve anonymity
  - Can be fully distributed
    - e.g., can be used in peer-to-peer architectures
- **Drawbacks**
  - Mixnets introduced for email and other high latency applications
  - Each layer of message requires expensive public key cryptography
  - What about remote login, chat, web browsing, and other low latency applications?

(Basic) Anonymizing Proxy



- Conceptually much simpler solution
- Channels appear to come from proxy, not true originator

Anonymizing Proxy

- **Advantages**
  - Simple
  - Focuses a lot of traffic
    - Very good for anonymity
  - No complex encryption primitives required
    - Appropriate for web transactions, etc.
- **Drawbacks**
  - Single point of failure
  - Vulnerable to attacks
  - Limited in scale?

Virtual Private Networks

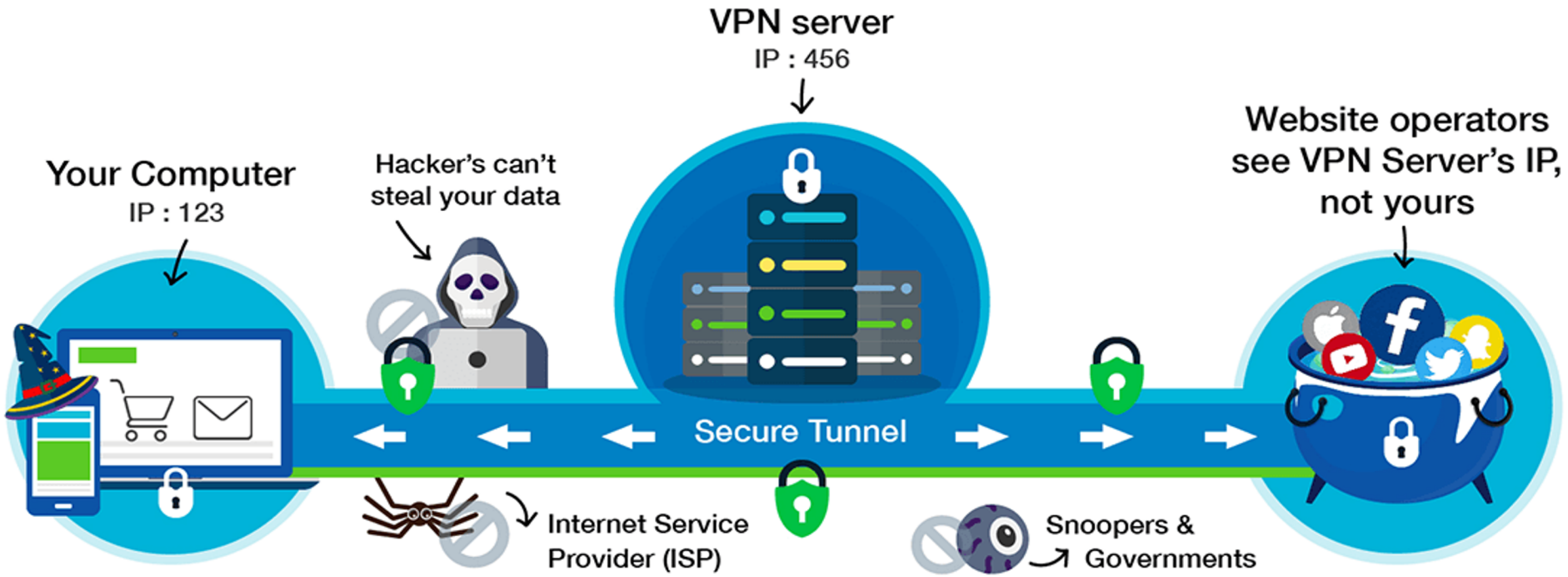


image credit: https://blog.360totalsecurity.com

Understanding VPNs

- VPNs encrypt communication in transit
- Hides your IP address from others
- Good for confidentiality especially on public networks
  - From eavesdroppers
- Is the user anonymous on the network?

- Always look for latest VPN recommendations (e.g. from NSA, CISA)

Onion Routing

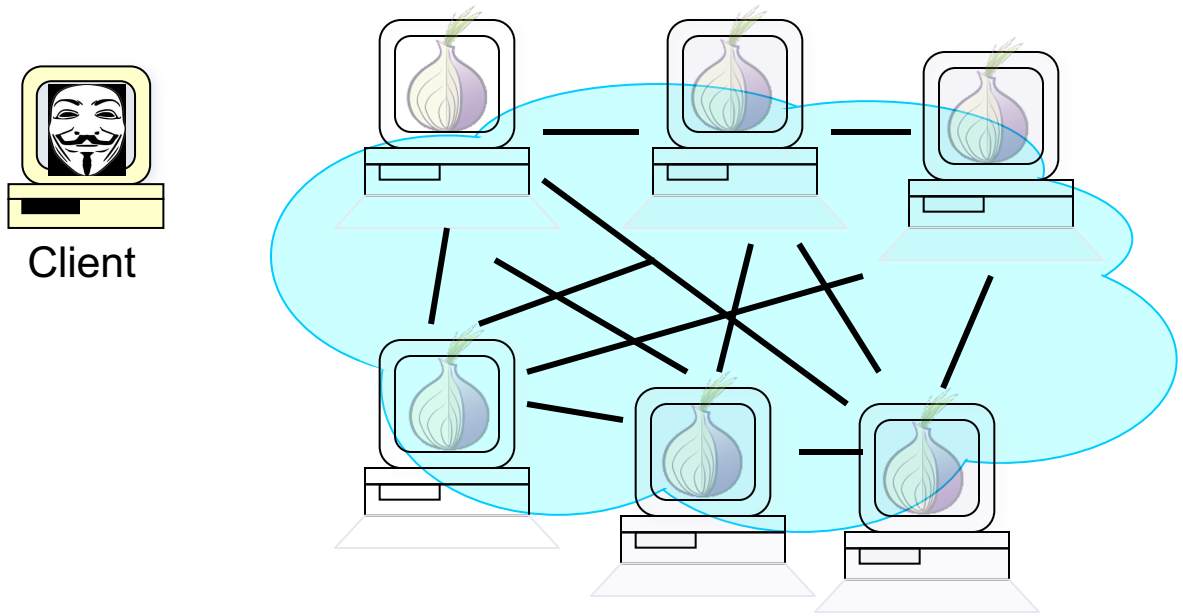
- **An infrastructure provides anonymity (traffic analysis resistant)**
- **Main idea: combine advantages of mixes and proxies**
- **Use public key crypto to establish circuits**
  - Like mixnets
- **Use symmetric key crypto to move data**
  - Like SSL/TLS based proxies

Tor

- **The Onion Router , Tor's Onion Routing**
  - Deployed anonymize overlay network (Running since October 2003)
- **Three main functions of interest to us**
  - Circuit establishment
  - Circuit usage
  - Hidden services

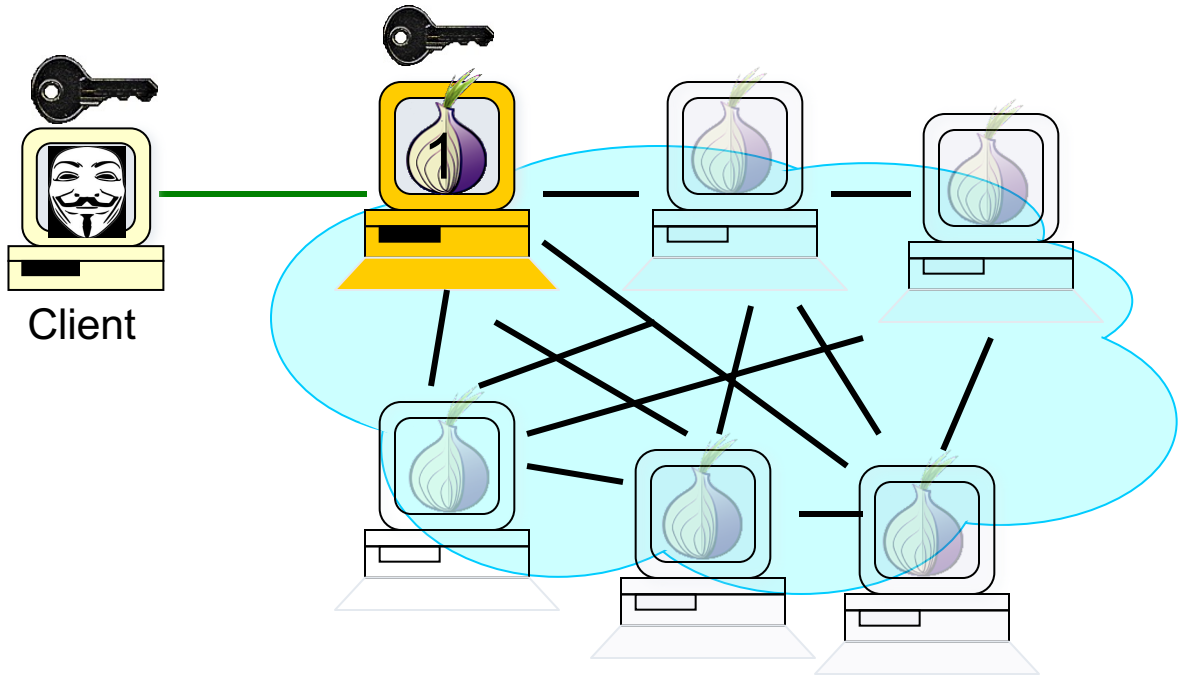
How Does Tor Work? [Dingledine et al., 2004]

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



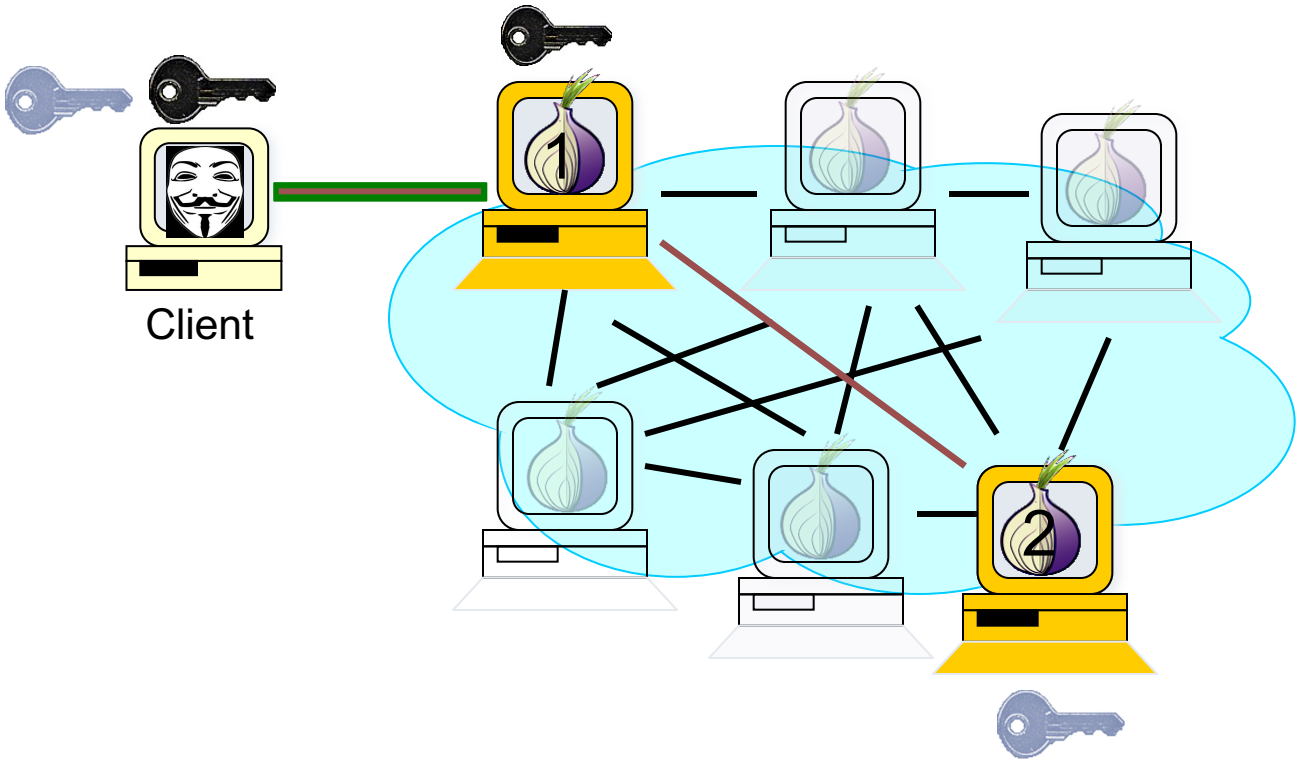
How Does Tor Work? [Dingledine et al., 2004]

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



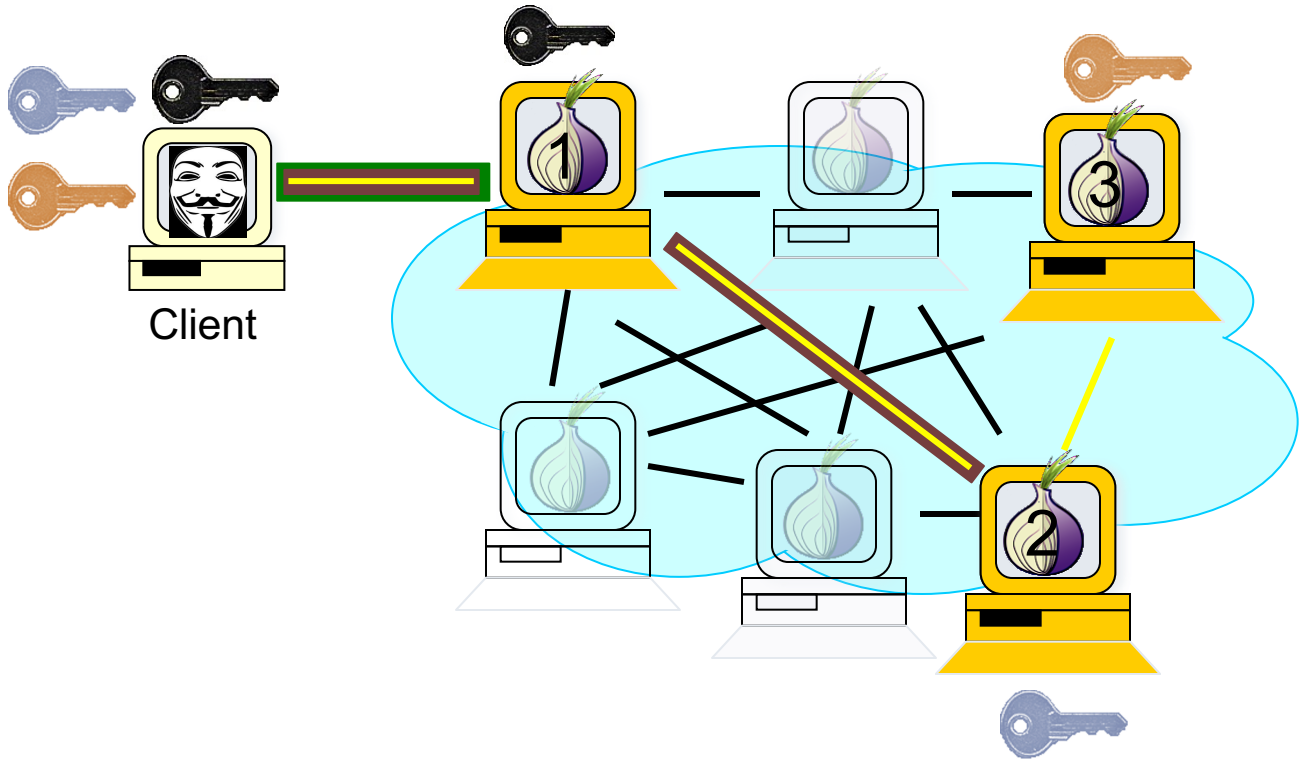
How Does Tor Work? [Dingledine et al., 2004]

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



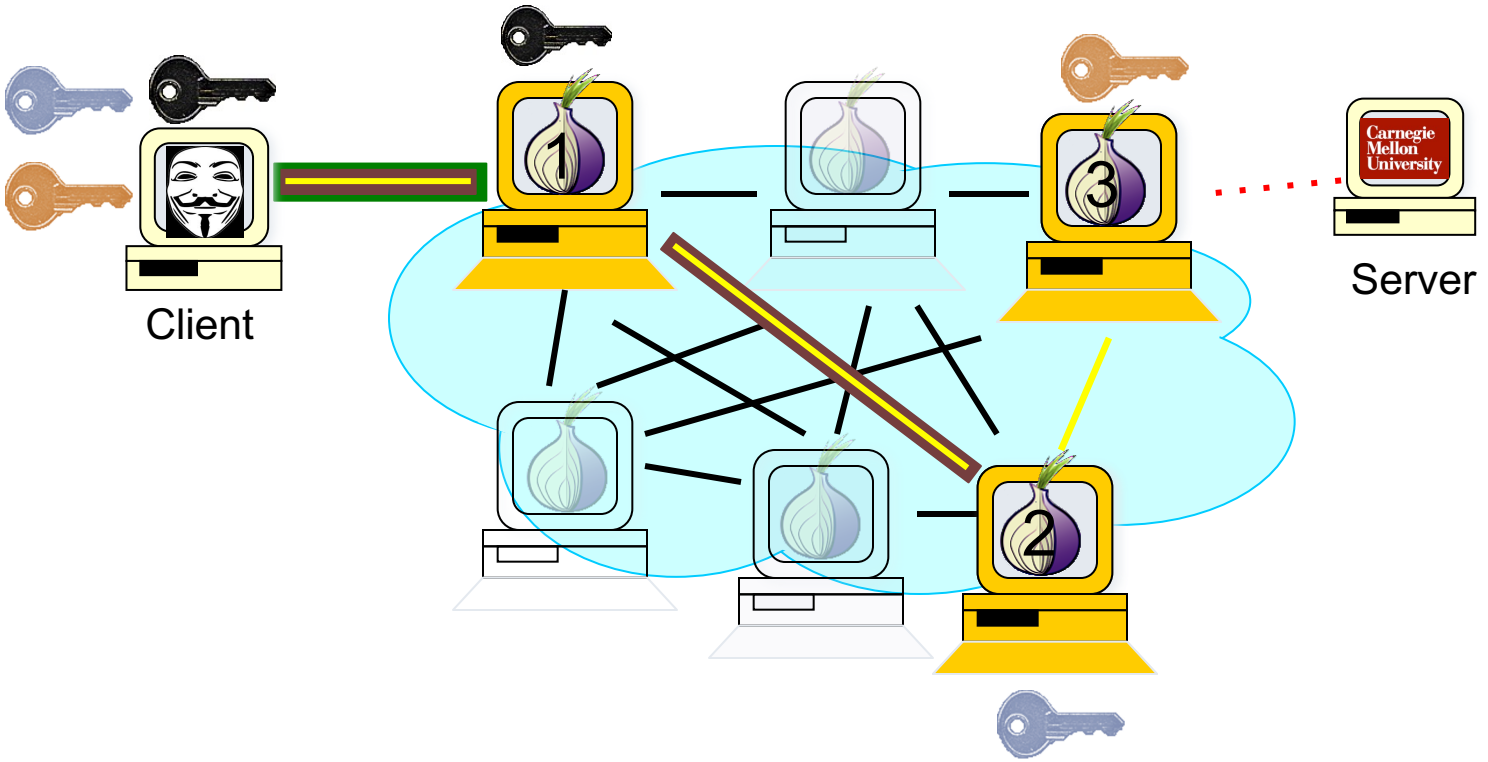
How Does Tor Work? [Dingledine et al., 2004]

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



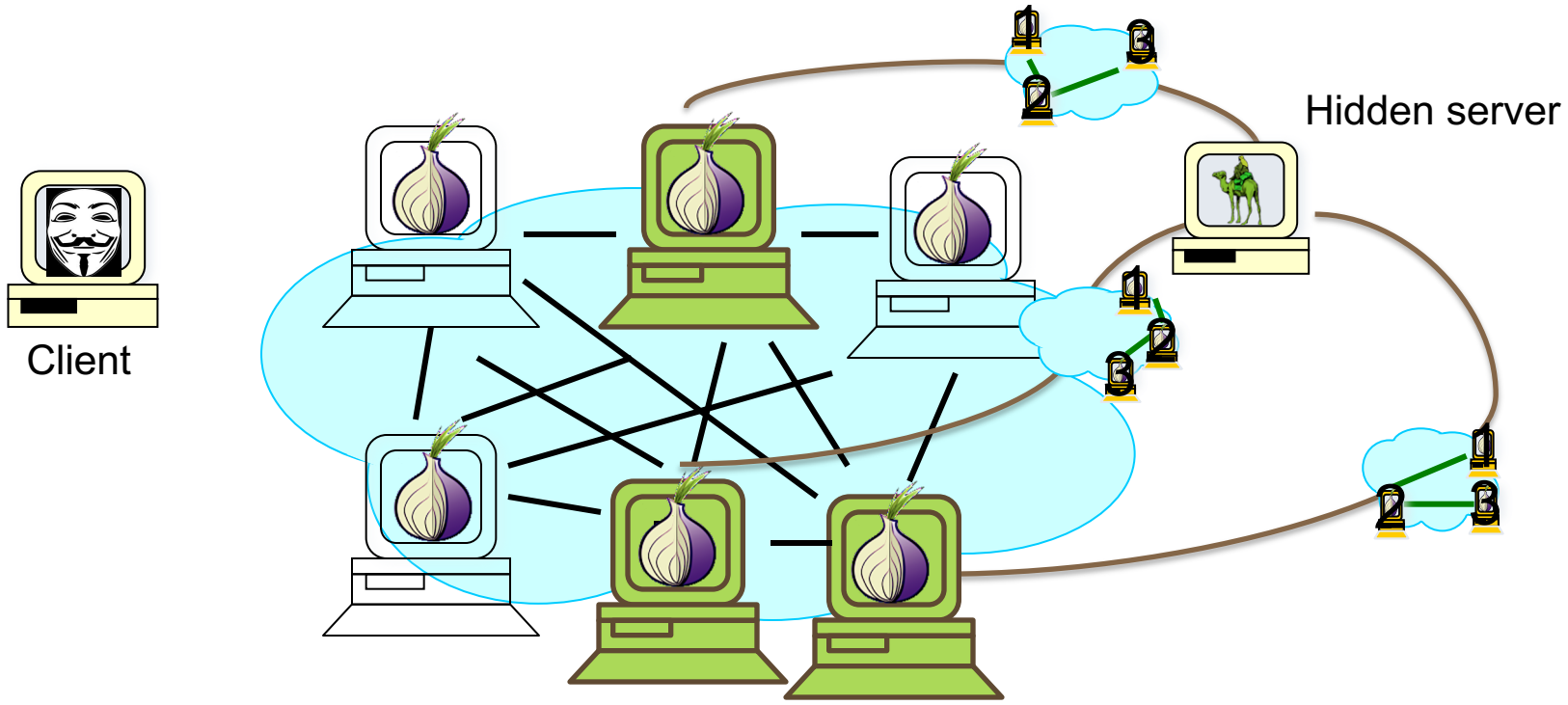
How Does Tor Work? [Dingledine et al., 2004]

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



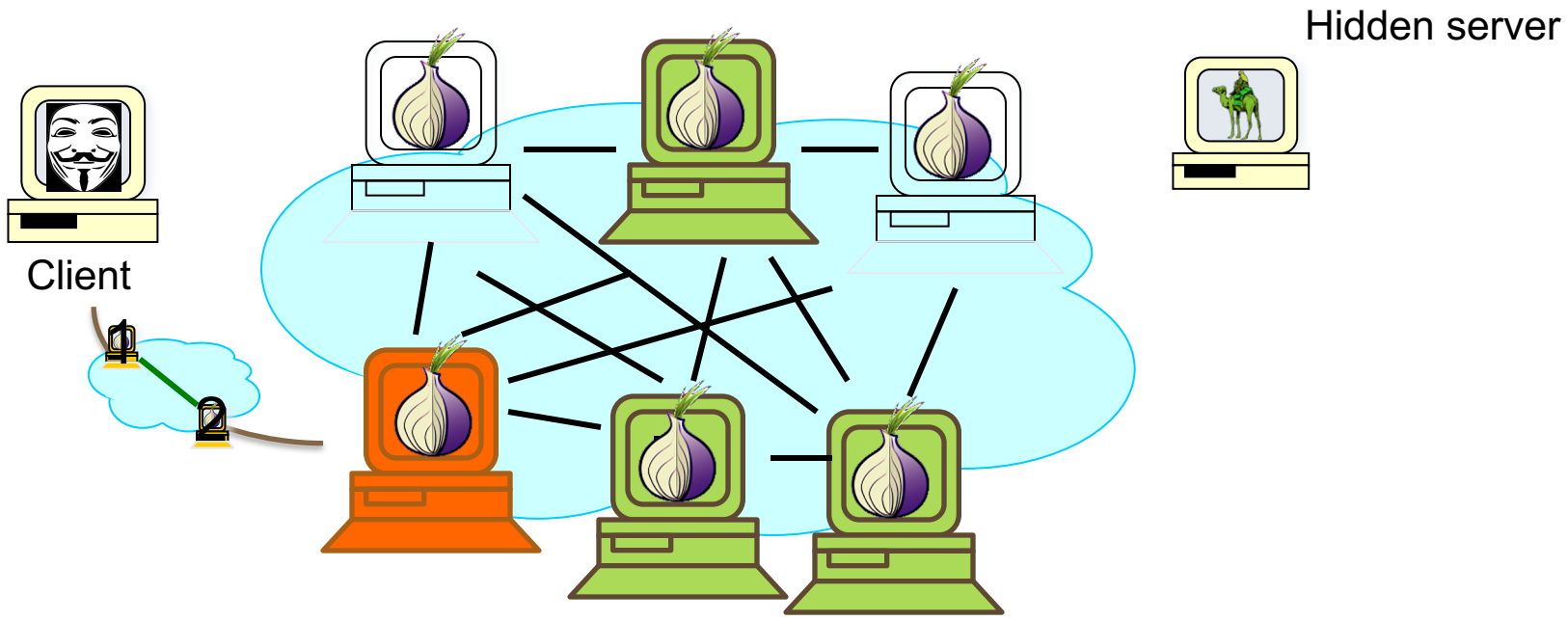
Tor: Onion Services (Hidden Services)

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



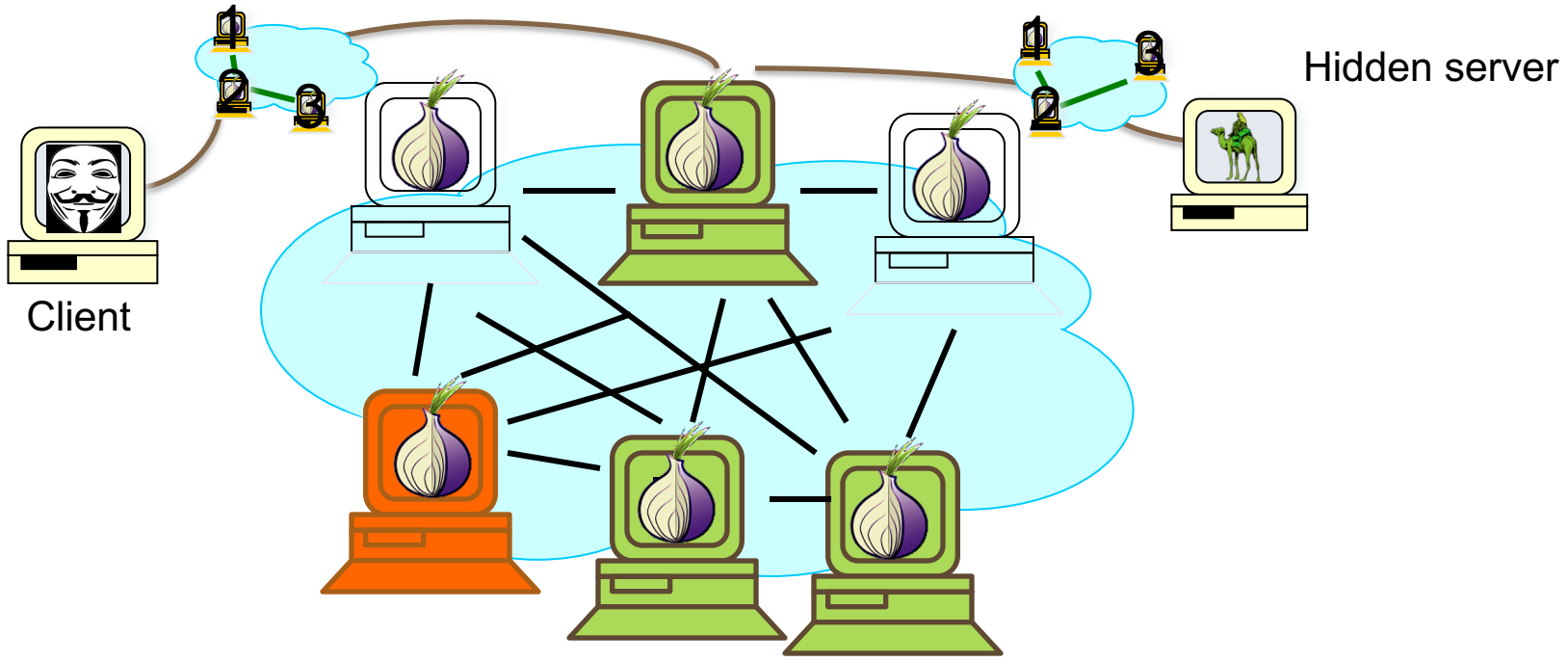
Tor: Onion Services (Hidden Services)

- 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: Onion Services (Hidden Services)

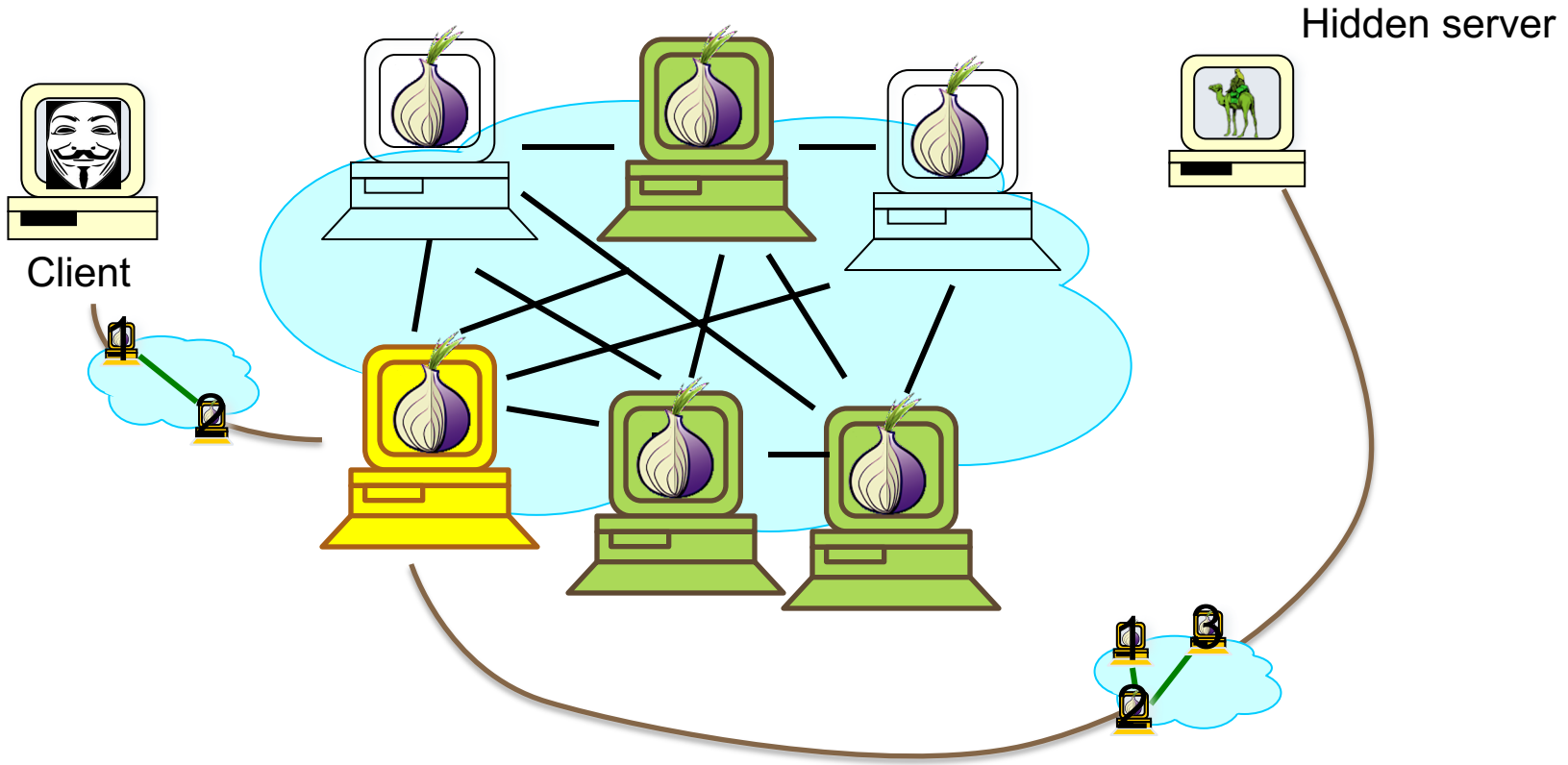
- **Client tells hidden server about Rendez-Vous Point by contacting one of the Introduction Points and asking them to relay message to server**



Tor: Onion Services (Hidden Services)

https://2019.www.torproject.org/docs/onion-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)



Tor Bootstrapping

- **Directory servers**
  - Maintain list of which onion routers are up, locations, keys, exit policies, etc.
  - Control which nodes can join network
    - Important to guard against Sybil attacks and related problems
- **Effort to decentralize process**
  - Research challenge

Other Anonymous Networks

- **Freenet**
  - Peer-to-peer network
  - Similar in concept to Tor
  - Files split in multiple pieces, pieces may use different circuits
- **Mixminion**
  - Anonymous mailer
  - Plug-in for email clients (e.g., mutt)
- **Nym**
  - Anonymous mail service
  - Proxy based
- **Anonymizer.net**
  - Anonymous web browsing
  - Proxy based
  - Has existed for > 10 years
- **…**

Take Away Slide

- **Encryption does not ensure anonymity**
  - Traffic analysis always possible
- **Anonymous networks try to prevent traffic analysis**
  - Have many desirable uses (law enforcement, freedom of speech, etc)
  - Have also some extremely undesirable uses (ransom note, spam)
- **Combination of mixnets and proxies**
  - Clever use of cryptography
  - Try to find again good balance between public key crypto (slow but convenient) and symmetric key crypto (fast but harder to set up)
- **Deployed mechanisms are readily available**
  - You are more than encouraged to try some…
  - … just don't send me ransom notes!

Confused? Try this interactive tool!

- **“How HTTPS and Tor Work Together to Protect Your Anonymity and Privacy”**
  - https://www.eff.org/pages/tor-and-https