CS 114: Network Security

Lecture 17 - Anonymous Communication

Prof. Daniel Votipka
Spring 2023

(some slides courtesy of Prof. Micah Sherr)

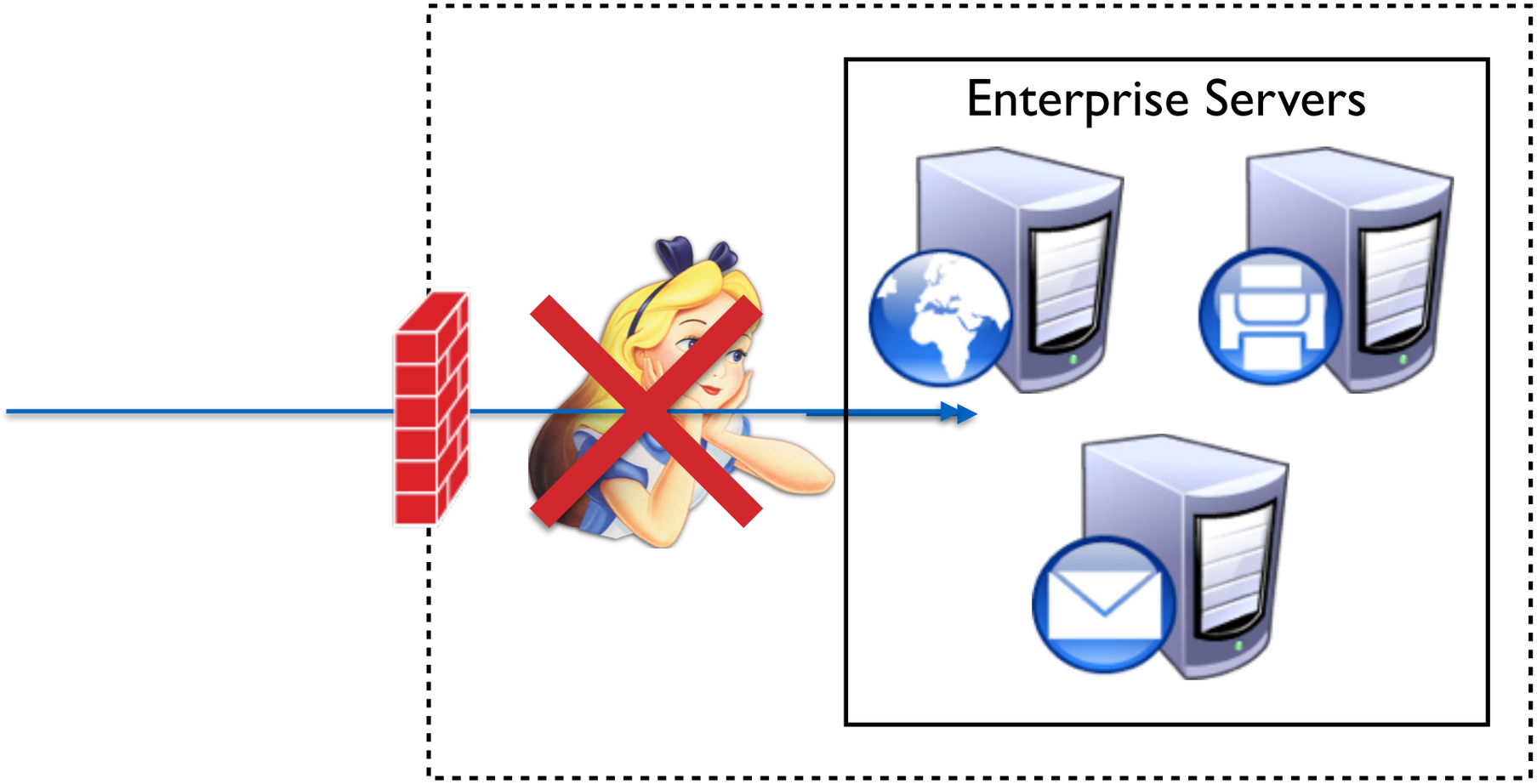
Plan for today

- Administrivia
- VPN Review
- Anonymous Communication
- Overview
- Network Overlays
  - Anonymizing Proxies
  - Crowds
  - Tor

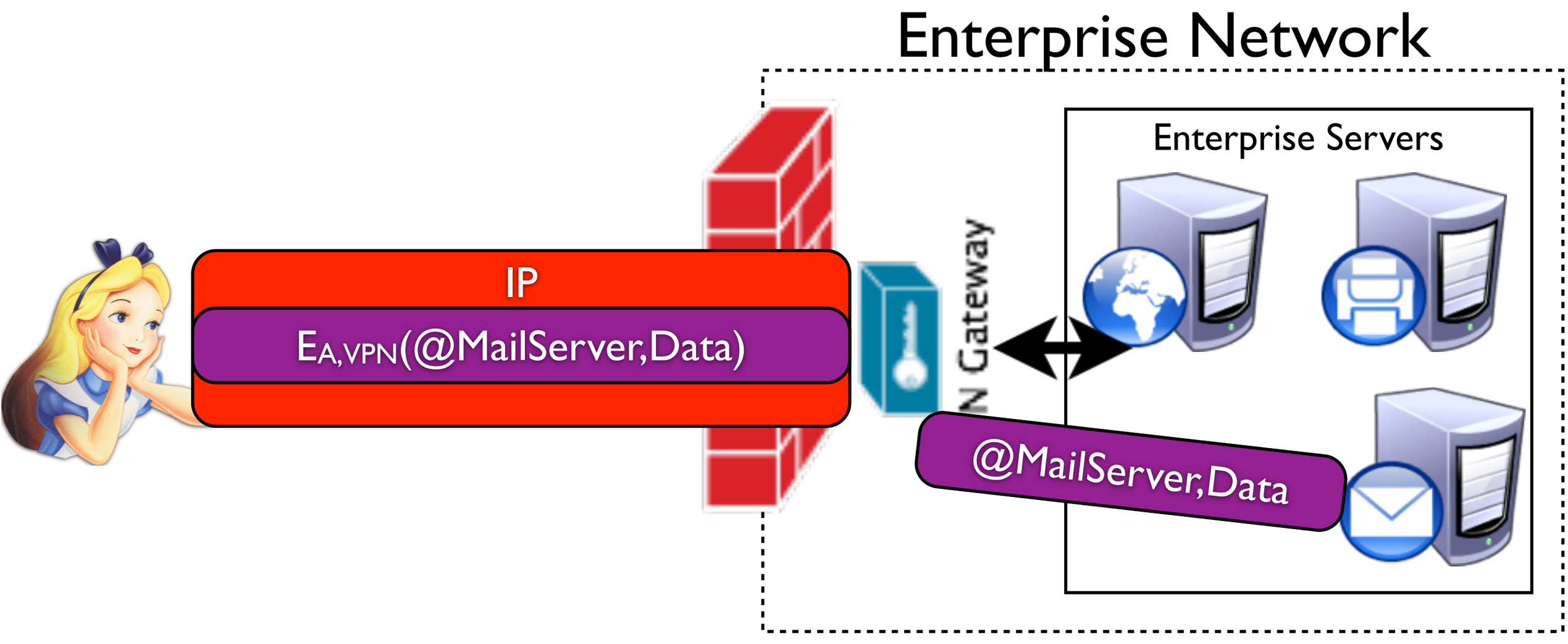
Administrivia

- HW1, part 3 is due Thursday at midnight!
  - You do not need to create a server
- Nirvan Tyagi: *"Privacy-Preserving Accountability Online"*
  - @ 3pm on Thursday in 270 JCC

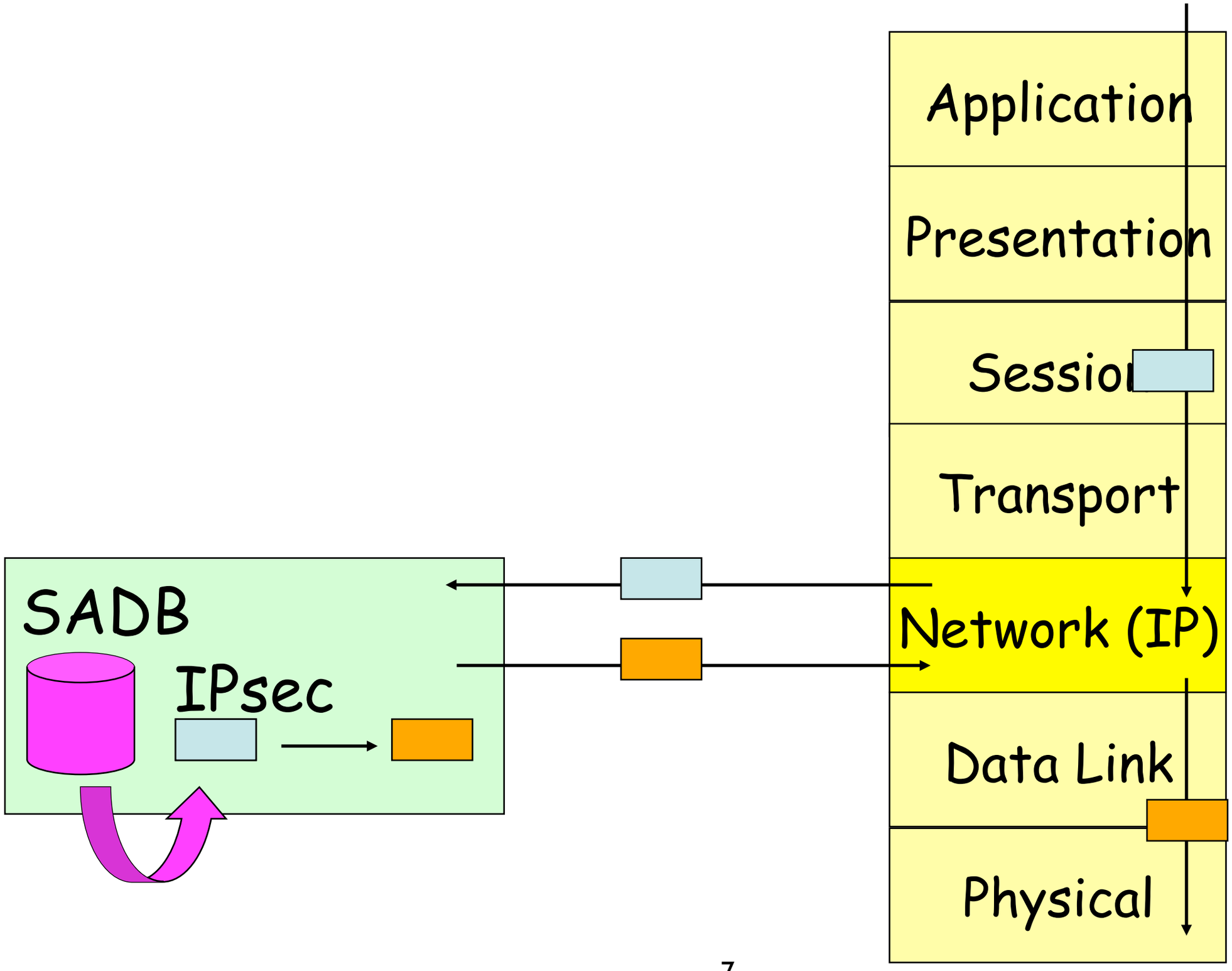
VPN Review


Enterprise Servers

VPN Tunneling

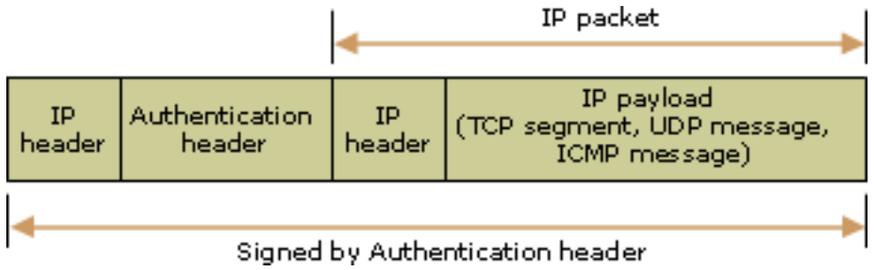


IPsec: Packet Handling

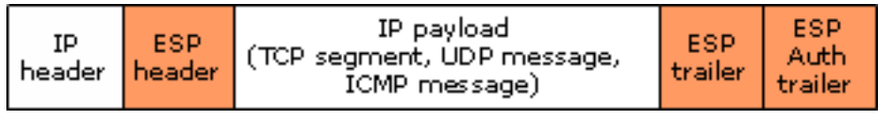


AH Transport Mode

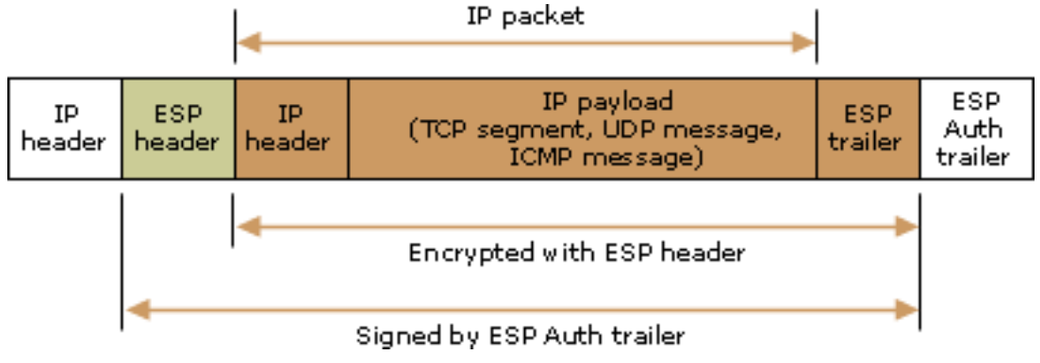
AH Tunnel Mode



ESP Transport Mode



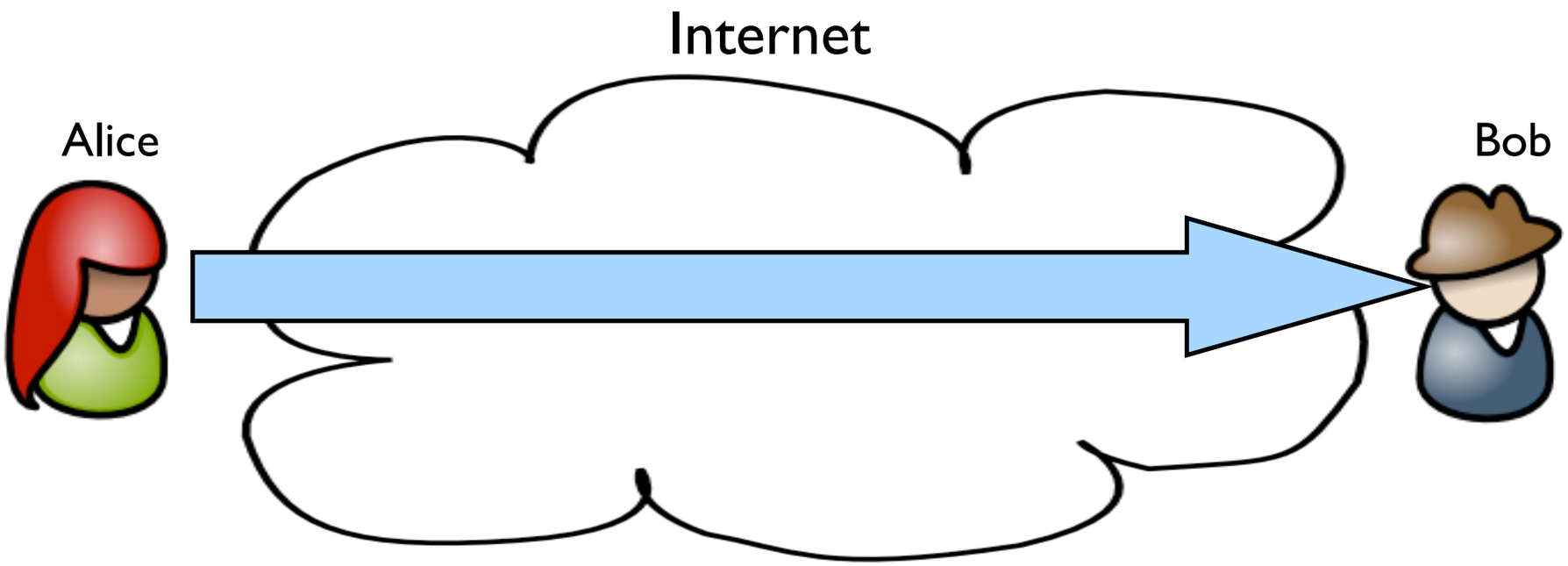
ESP Tunnel Mode



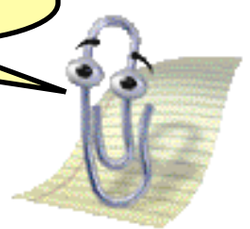
Plan for today

- Administrivia
- VPN Review
- Anonymous Communication
  - Overview
  - Network Overlays
    - Anonymizing Proxies
    - Crowds
    - Tor

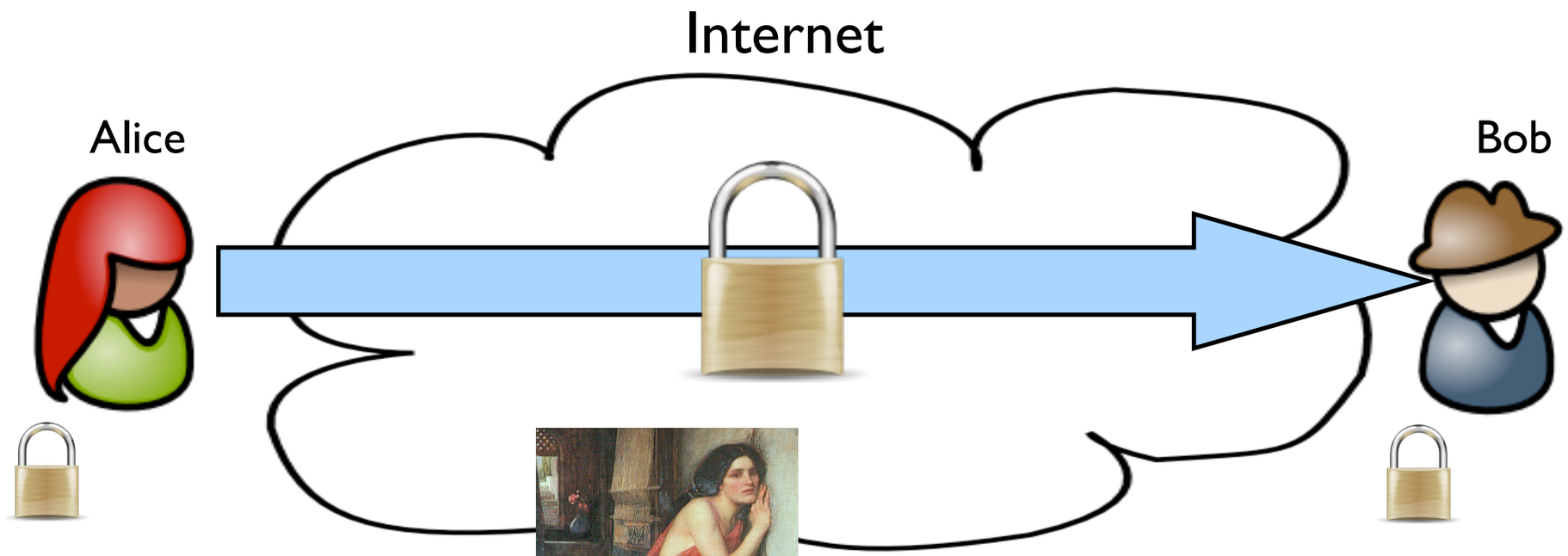
Problem: Alice and Bob want to communicate on the Internet

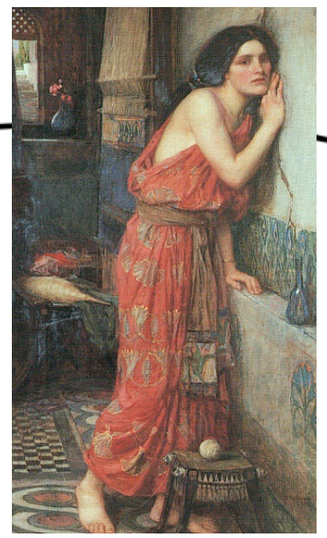


Solution:
Send IP packets



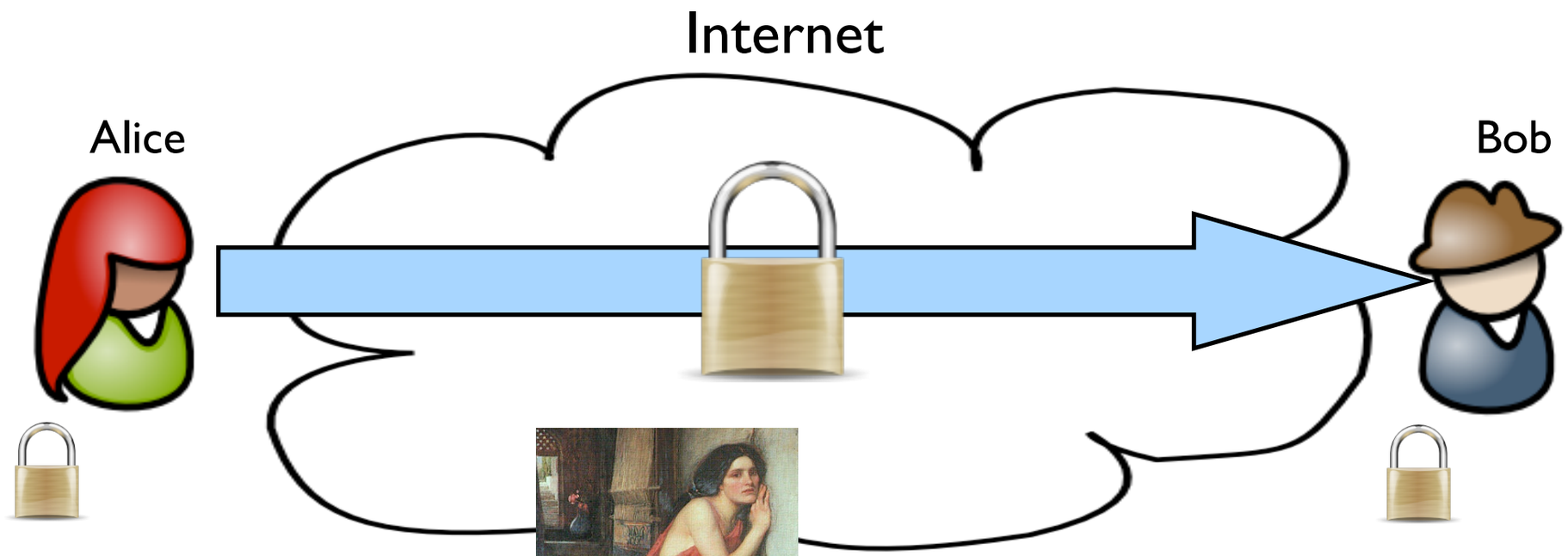
Problem: Alice and Bob want to communicate on the Internet **privately**

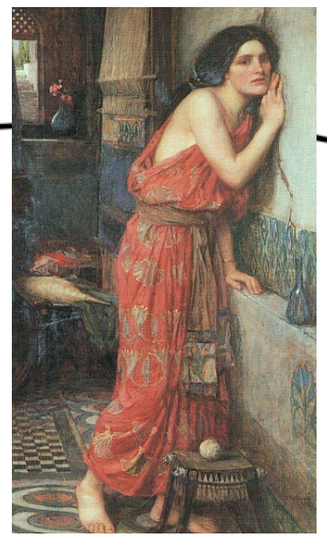




Solution:
Encrypt payloads

Problem: Alice and Bob want to communicate on the Internet privately and **anonymously**



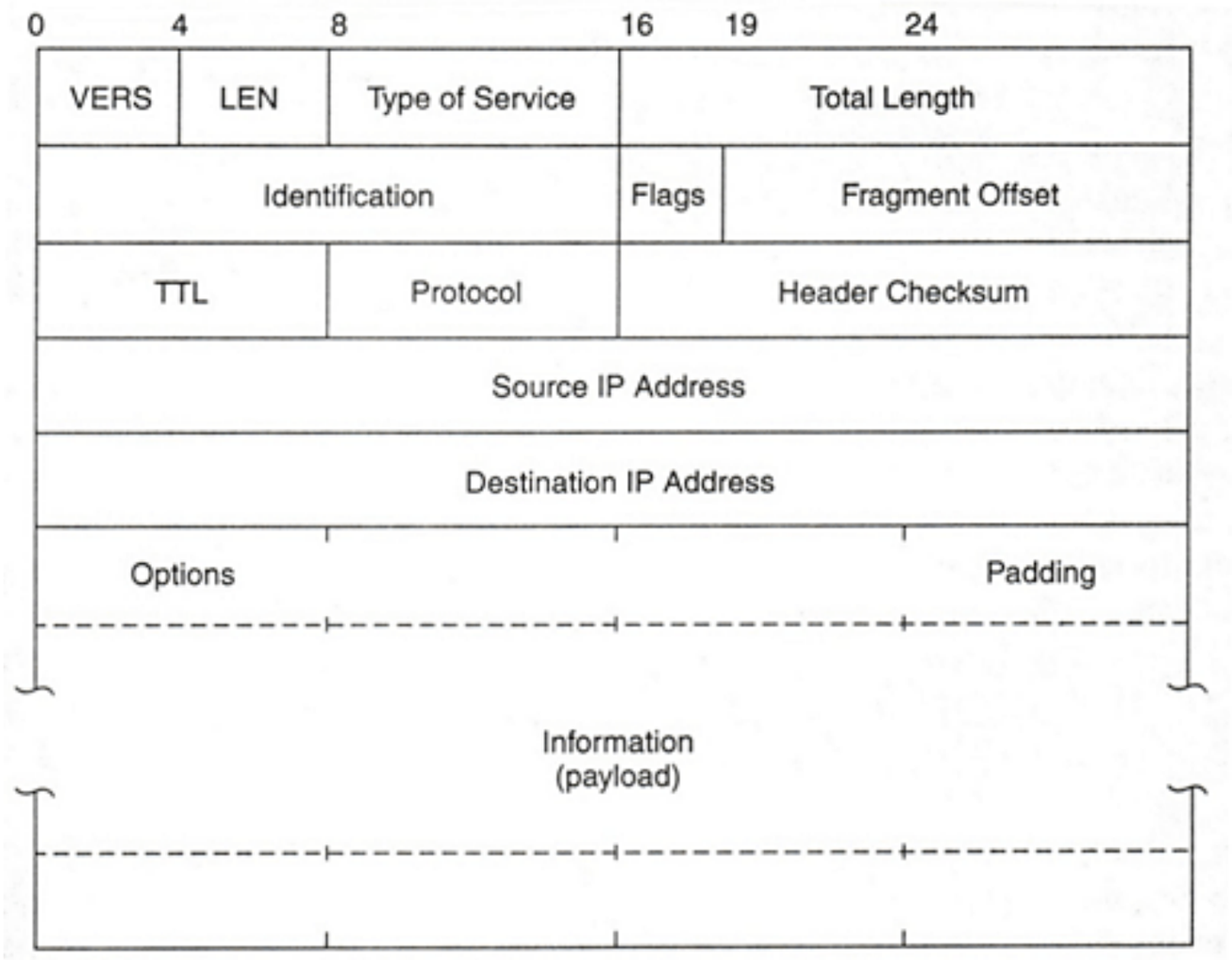


Solution:
?

Identity

- no clear mapping between IP and identity
  - early Internet: static IPs and routing tables
  - today's Internet: NAT, proxies, VPNs, dynamic IP, and mobile IP
  - IP addresses easily forged [Bellovin '89]
- simplifying assumption: IP == identity

Eavesdropping on the Internet



- **Internet routing incompatible with anonymity**
- To be deliverable, packets require accurate destination IP address
- Reliability requires accurate source IP address

Motivations for Internet anonymity

- Why do we want anonymity?

If you aren't doing anything wrong, so what if Big Brother knows you're communicating?

- Bad guy's motivation is obvious: do bad things (crimes) without getting caught
  - Terrorism (organize / e-attacks)
  - Platform to launch network attacks
  - Spam
  - Pornography (legal / illegal)
  - File sharing

Motivations for Internet anonymity

- What about the good guys?
  - circumvent censorship: anonymous access to otherwise restricted

Throttling Twitter: An Emerging Censorship Technique in Russia

Diwen Xue
University of Michigan

Reethika Ramesh
University of Michigan

ValdikSS
Independent

Leonid Evdokimov
Independent

Andrey Viktorov
Independent

Arham Jain
University of Michigan

Eric Wustrow
University of Colorado Boulder

Simone Basso
OONI

Roya Ensafi
University of Michigan

  - law enforcement tool
  - whistleblowing

HTTPS != Privacy

- Joe cares about confidentiality, so he visits only TLS-protected websites
- Yesterday, Joe visited:
  - Bank of America, ING Direct, AmericanExpress
  - Slashdot, Digg
  - NYTimes, Huffington Post
  - JustinBeiber.com
  - WebMD
  - Tufts Webmail
  - Monster.com
  - Match.com
- Even if we don't know *what* Joe communicated, knowing with *whom* he communicated leaks a lot of information

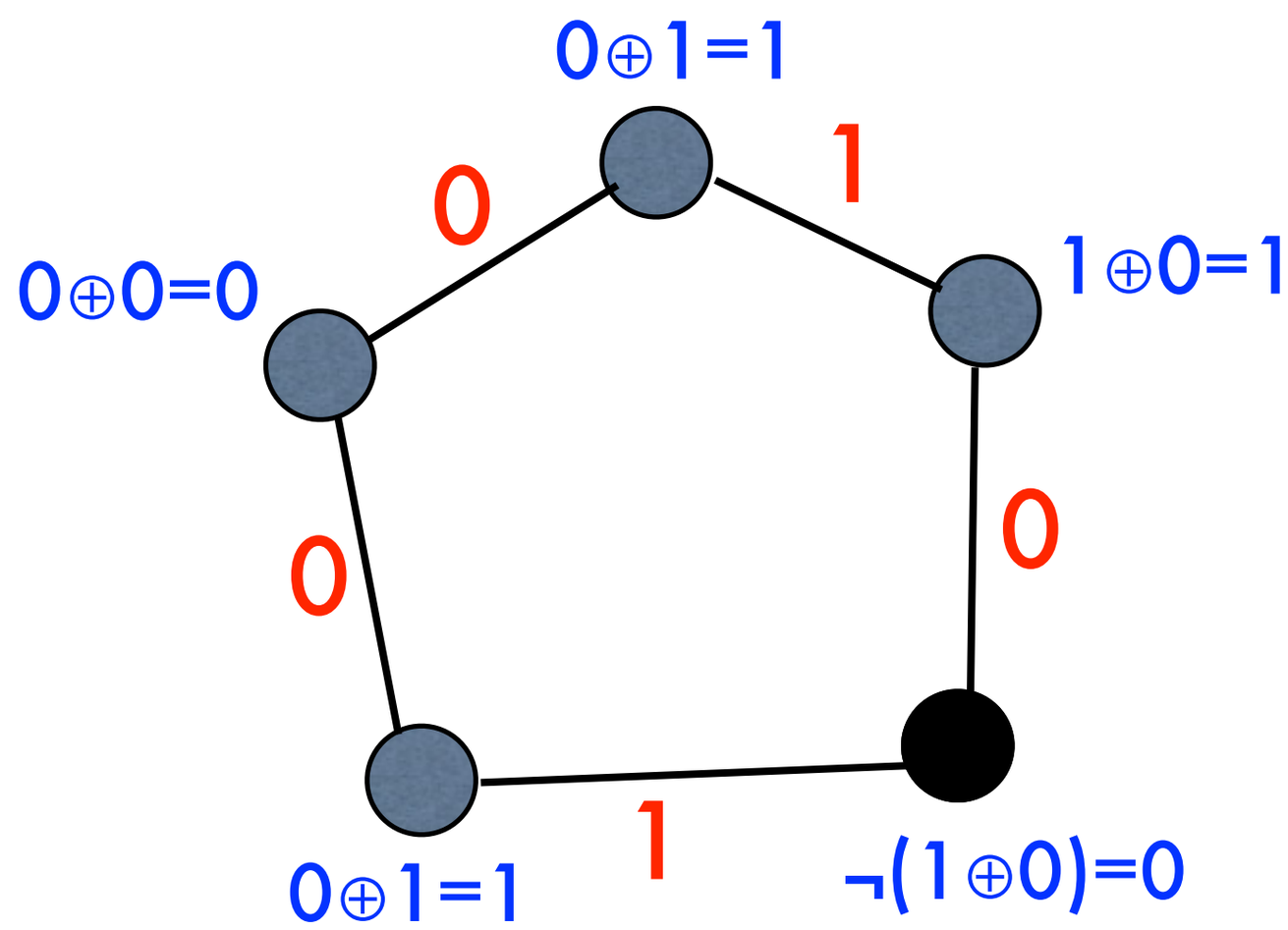
Secure, Anonymous Multi-Party Computation

Dining Cryptographers Problem

- N cryptographers are having dinner
- Waiter says meal has either been paid by a cryptographer, or by the NSA
- The diners want to figure out whether one of them paid (but not which one!) or whether the NSA paid

DC-Net

- Phase I: Each diner exchanges secret coin flip with neighbor
- Phase II:
  - If diner didn't pay, announces xor of local coin flips
  - If diner did pay, announces inverse of xor
- If xor of the announced xors is 0, then no one inverted and NSA paid; otherwise, a diner paid.



$$0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 = 1$$

DC-Nets

- Achieves information-theoretic anonymity (under certain conditions)
- Limitations:
  - Subject to collisions (what if two diners pay?)
  - Requires pairwise secret keys
  - Last diner who announces message gets to choose the result

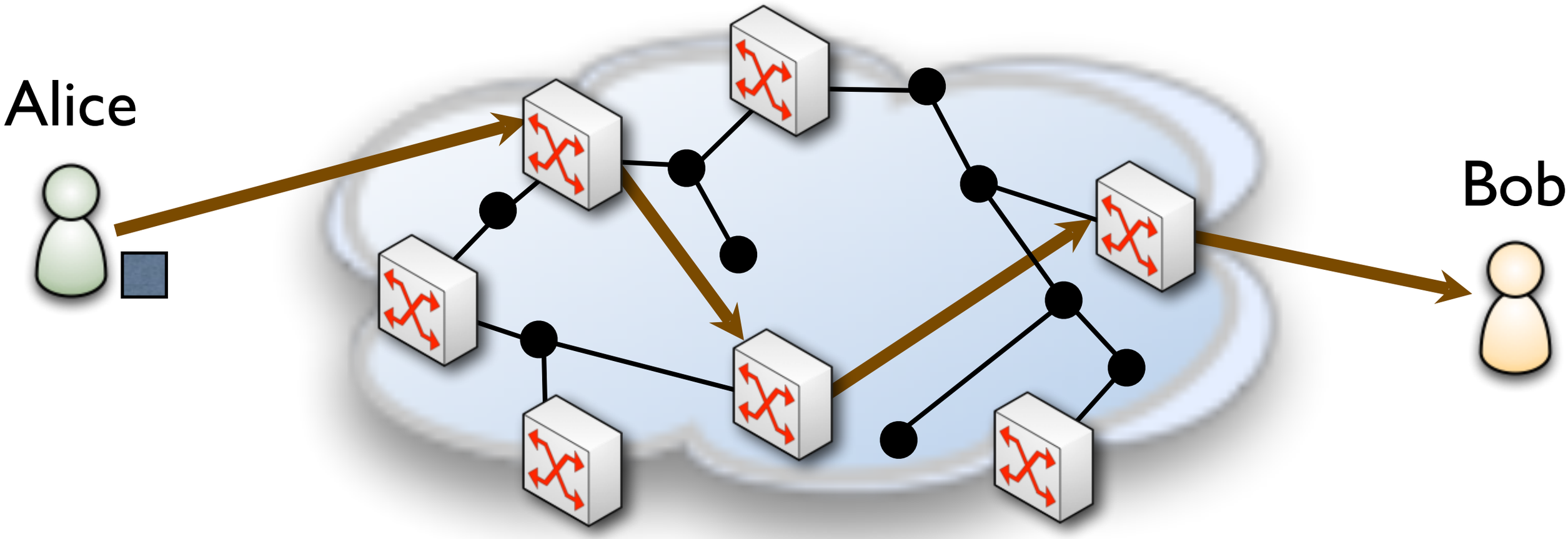
Plan for today

- Administrivia
- VPN Review
- Anonymous Communication
  - Overview
  - Network Overlays
    - Anonymizing Proxies
    - Crowds
    - Tor

Internet Anonymity 101: 10,000ft view

- Forward anonymous traffic at the application-layer via **network overlay**
  - Permits application-layer routing protocols
  - Overlay nodes act as intermediaries between sender and receiver
  - Packets transmitted using existing Internet infrastructure (no AS/ISP cooperation necessary)
- Use cryptography to prevent eavesdroppers from learning IDs of sender and/or receiver

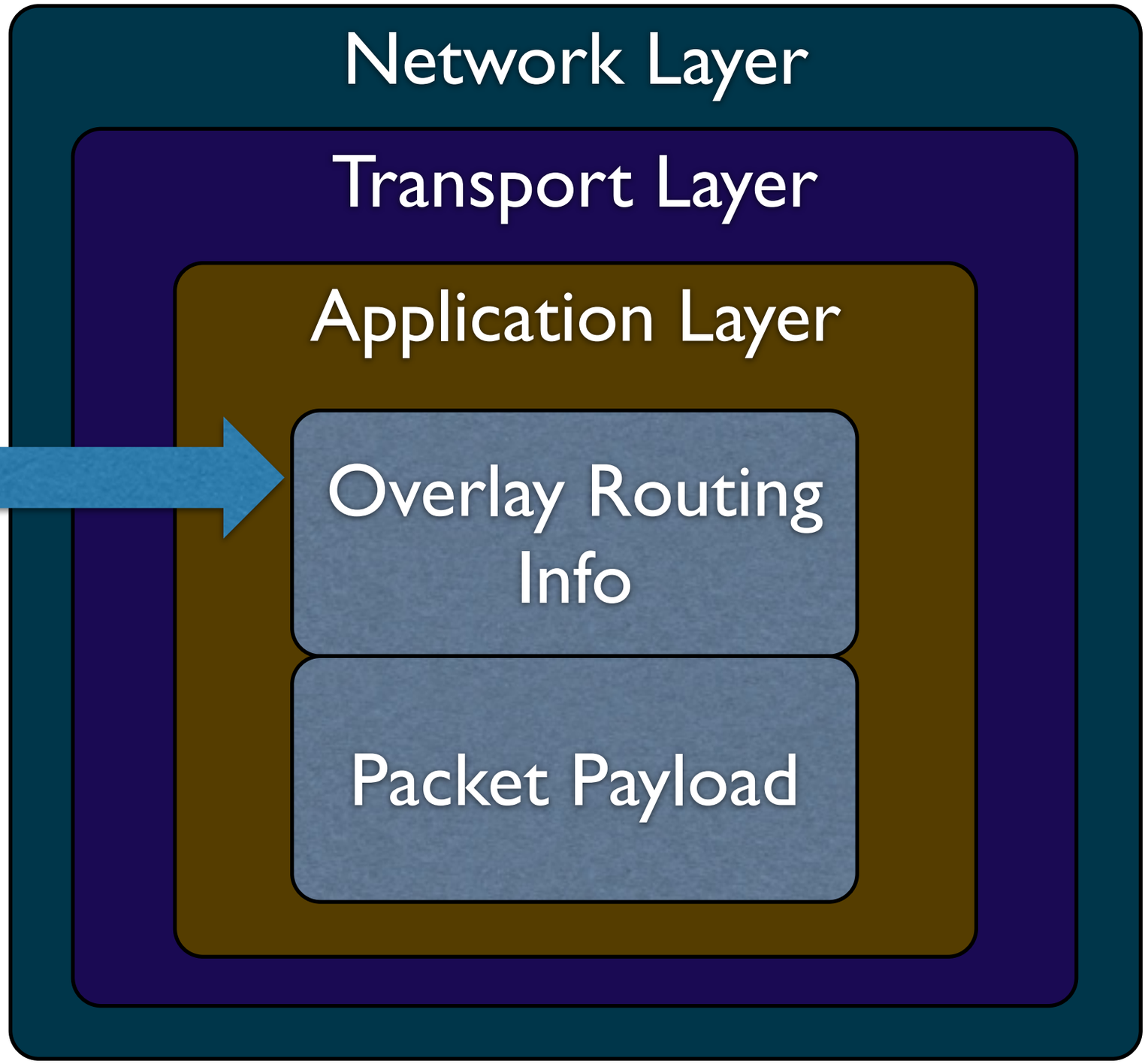
Overlay Networks



- Overlay Networks handle routing at the application-layer
- Basic concept: tunnel messages inside of other messages

Overlay Communication

Contains sufficient info for overlay node to deliver message to next hop on the overlay.

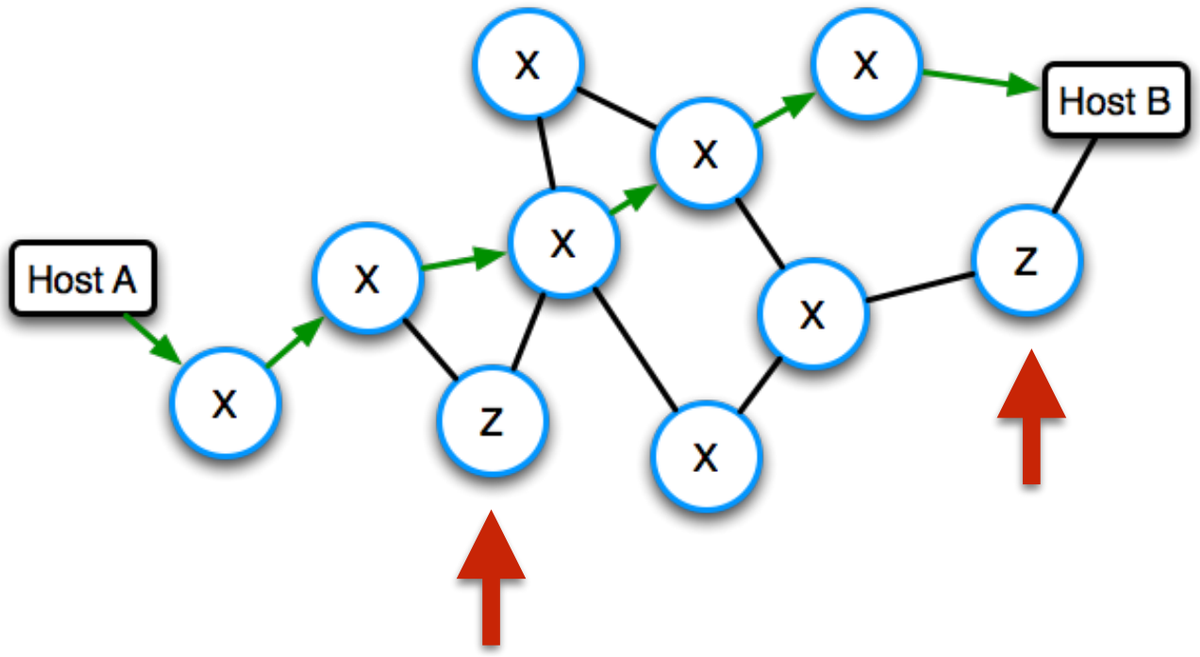


Overlay routing header can be encrypted!
--WHY?

Threat Model

- We often model the adversary as an insider Byzantine attacker who has a limited view of the network.
- Adversary might have tight control over a network, but unlikely to observe the entire Internet.
- a.k.a. “non-global adversary”

Standard Threat Model



For example, the adversary may control the "Z" ASes

Not Usually Considered

Global adversaries are viewed as unrealistic (requires too much international cooperation)

Measuring anonymity?

- What actually matters is a probability distribution over the likelihood that your behavior on the network will lead to de-anonymization
  - This requires understanding:
    - The network topology
    - The anonymity network protocols
    - The capabilities of the adversary
    - The behavior of the user and the destination
    - The traffic characteristics of the (anonymized) communication
    - Etc.

Let's look at some anonymity services...

First up:

Anonymizing Proxies

Anonymizing Proxies

PROXIFY

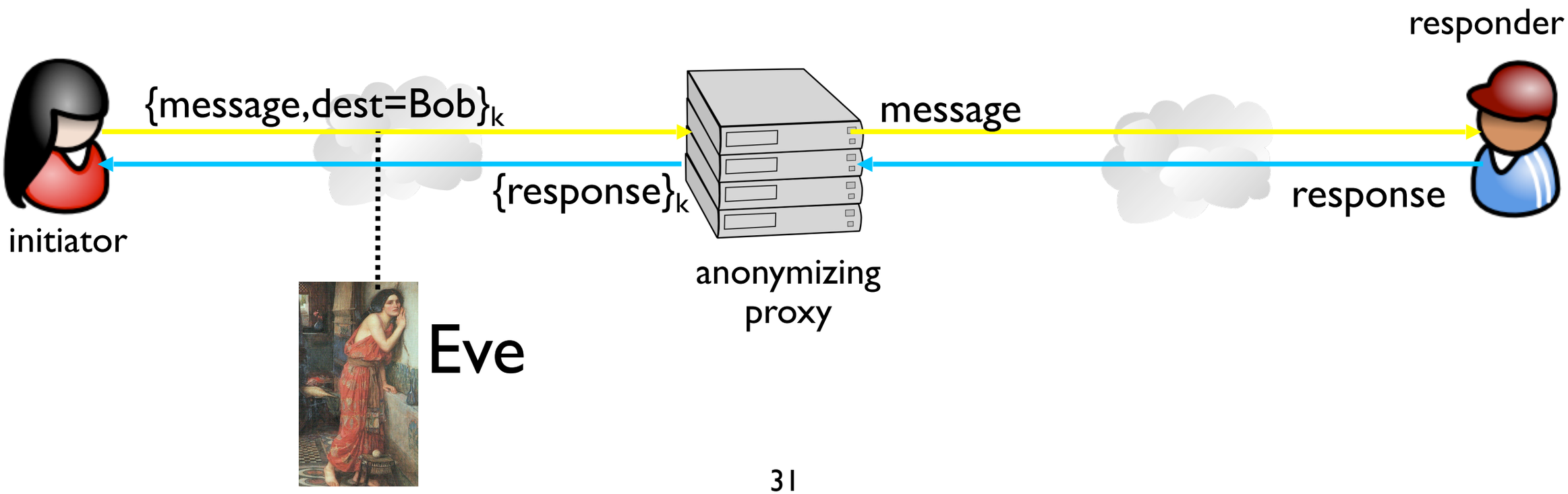
Anonymouse.org

FREEPROXY.CA
Anonymous, free and proudly Canadian.

Zend2.com
Freedom of Speech

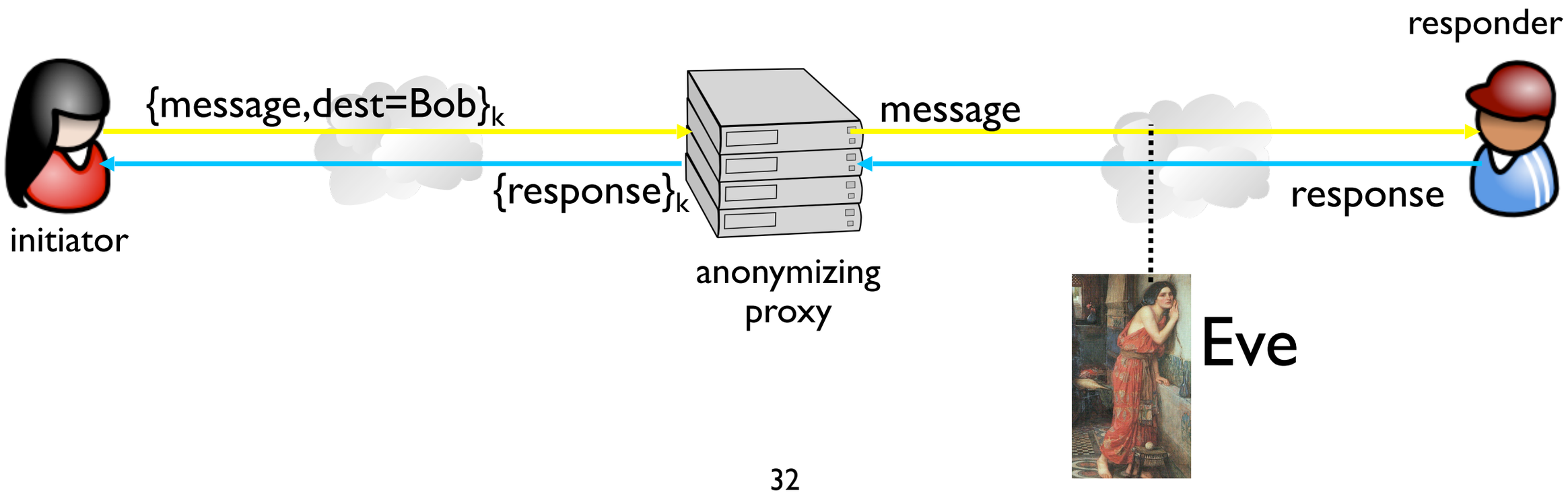
Anonymizing proxies

- Anonymizing proxy acts as intermediary between Alice and Bob
- Alice relays all traffic through the proxy, encrypting destination and payload
- Requires minimal configuration (SOCKS or SSL)
- Asymmetric technique – receiver not involved (or informed of) anonymity
- If Eve is located between Alice and the anonymizing proxy, then sender is exposed



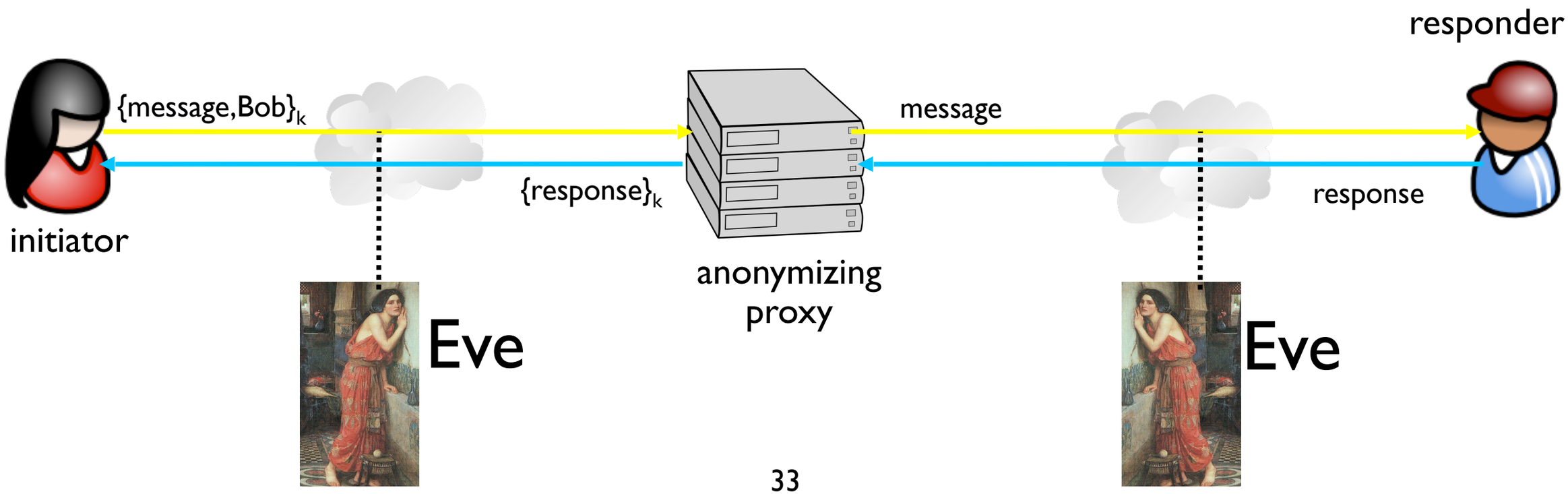
Anonymizing proxies

- Anonymizing proxy acts as intermediary between Alice and Bob
- Alice relays all traffic through the proxy, encrypting destination and payload
- Requires minimal configuration (SOCKS or SSL)
- Asymmetric technique – receiver not involved (or informed of) anonymity
- If Eve is located between the anonymizing proxy and Bob, then the receiver is exposed



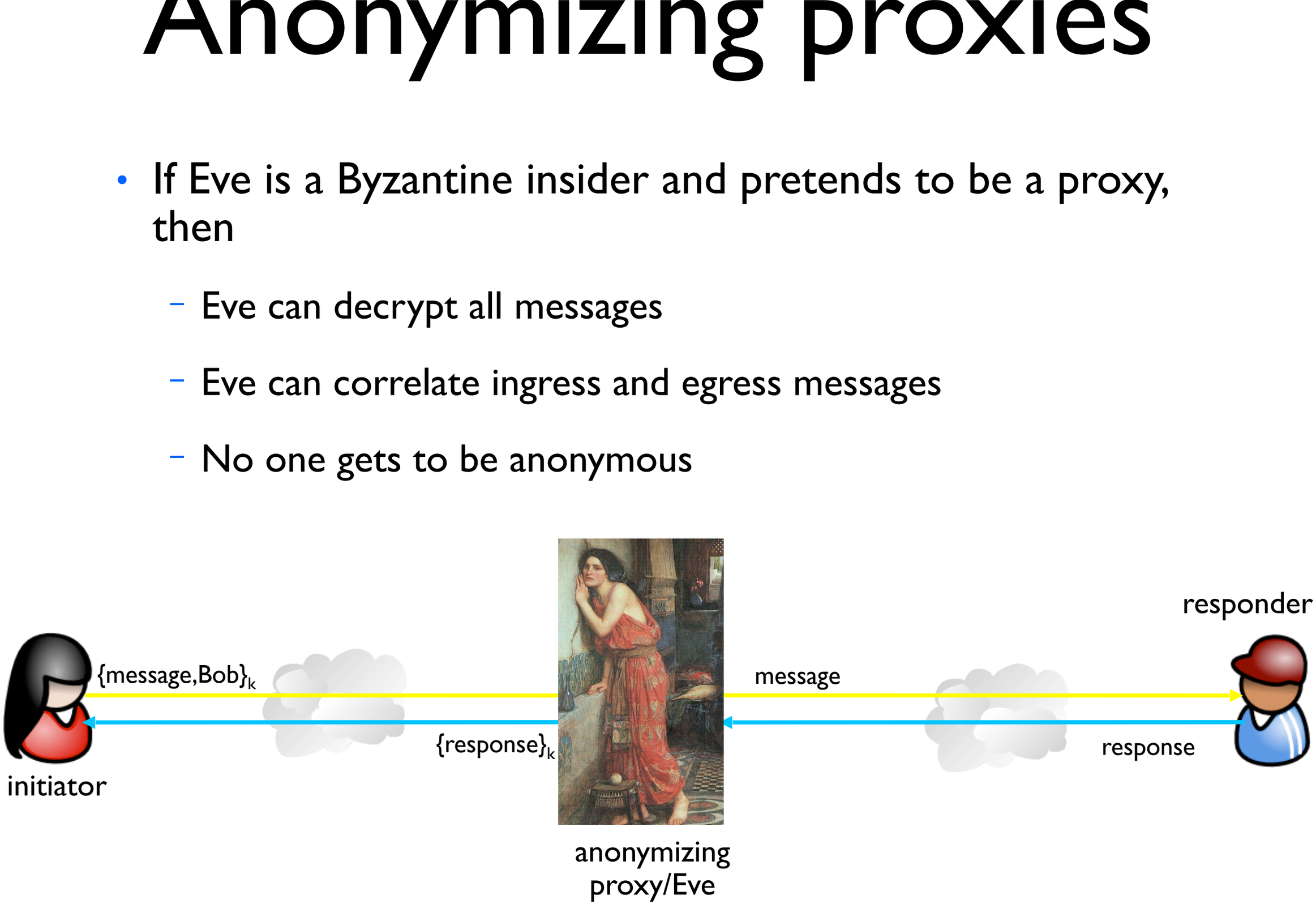
Anonymizing proxies

If eavesdroppers collude, Eve can correlate ingress and egress proxy traffic to identify Alice and Bob



Anonymizing proxies

- If Eve is a Byzantine insider and pretends to be a proxy, then
  - Eve can decrypt all messages
  - Eve can correlate ingress and egress messages
  - No one gets to be anonymous



Anonymizing proxies

- Advantages:
  - Easy to configure -- most browsers support SOCKS proxies
  - Does not require receiver's active participation -- receiver need not be aware of anonymity service
  - In plentiful supply on the Internet

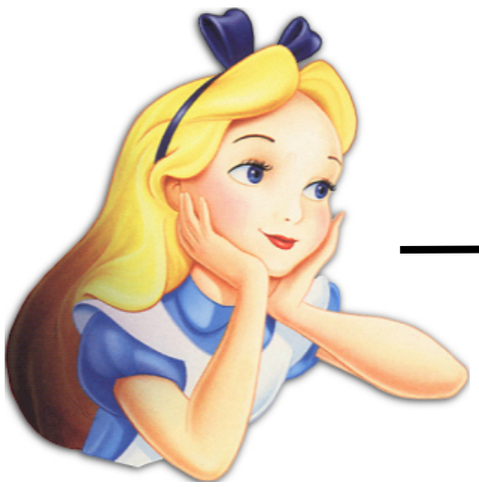
Anonymizing proxies

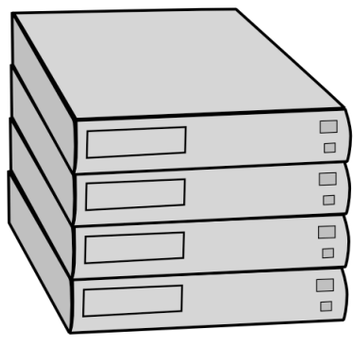
- Disadvantages:
  - Require trust in 3rd party
    - proxy may release its logs
    - or sell them
    - or blackmail Alice!
- Anonymity largely depends on the (unknown) location of Eve

Q:

When should anonymizing proxies be used?

A: When the position of the eavesdropper is known





Anonymizing
Proxy

Google

Prevents Google from learning
who is communicating with it.
(I.e., the receiver is the “Eavesdropper”.)

Crowds

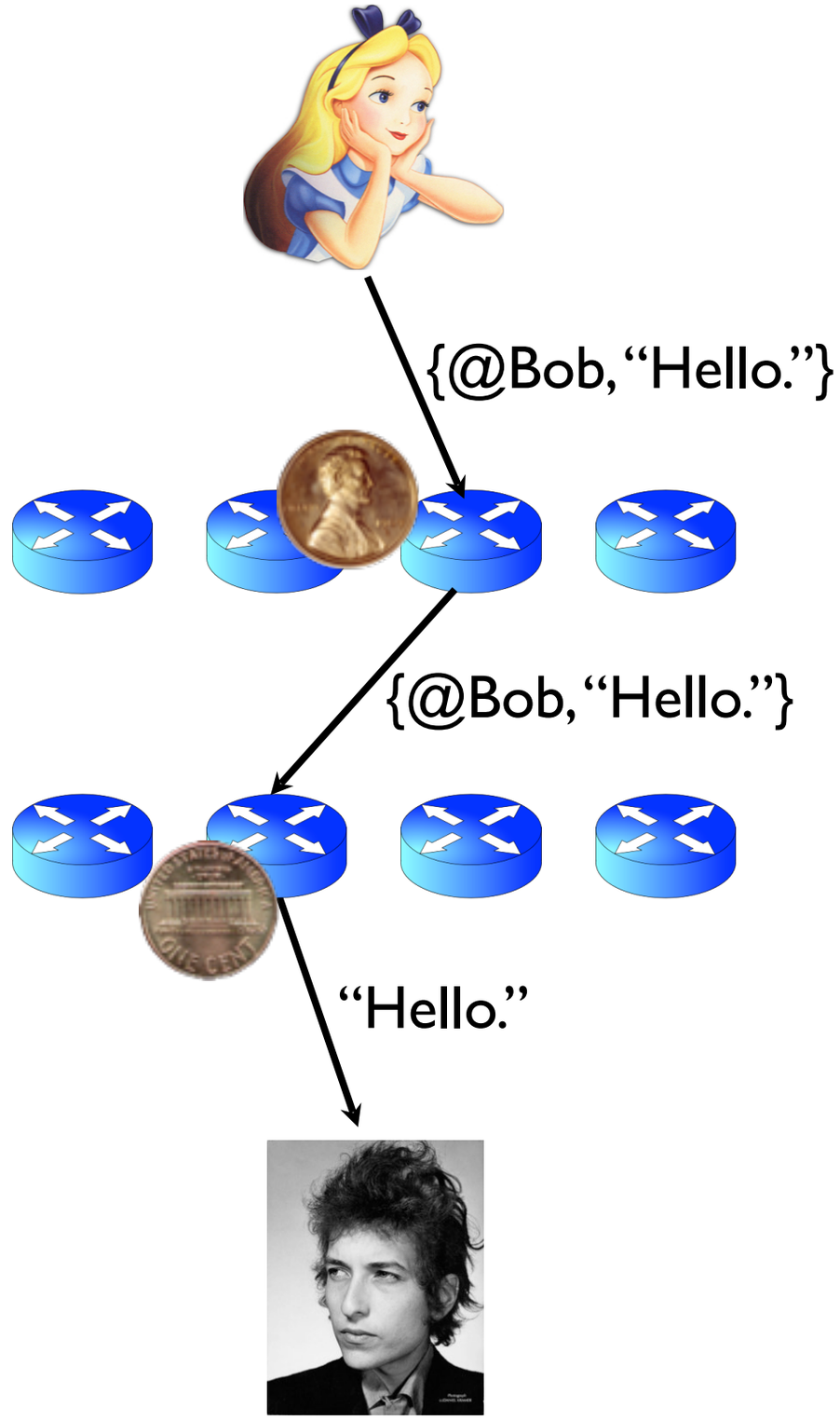
Crowds

[Reiter and Rubin, 1998]

- Basic Idea: Get lost in a "crowd"
- Jump from one member to another
- Members of a crowd called *Jondos* *(i.e., John Doe)*

Crowds

- Algorithm:
  - Relay message to random jondo
  - With probability p, jondo forwards message to another jondo
  - With probability 1-p, jondo delivers message to its intended destination



Crowds

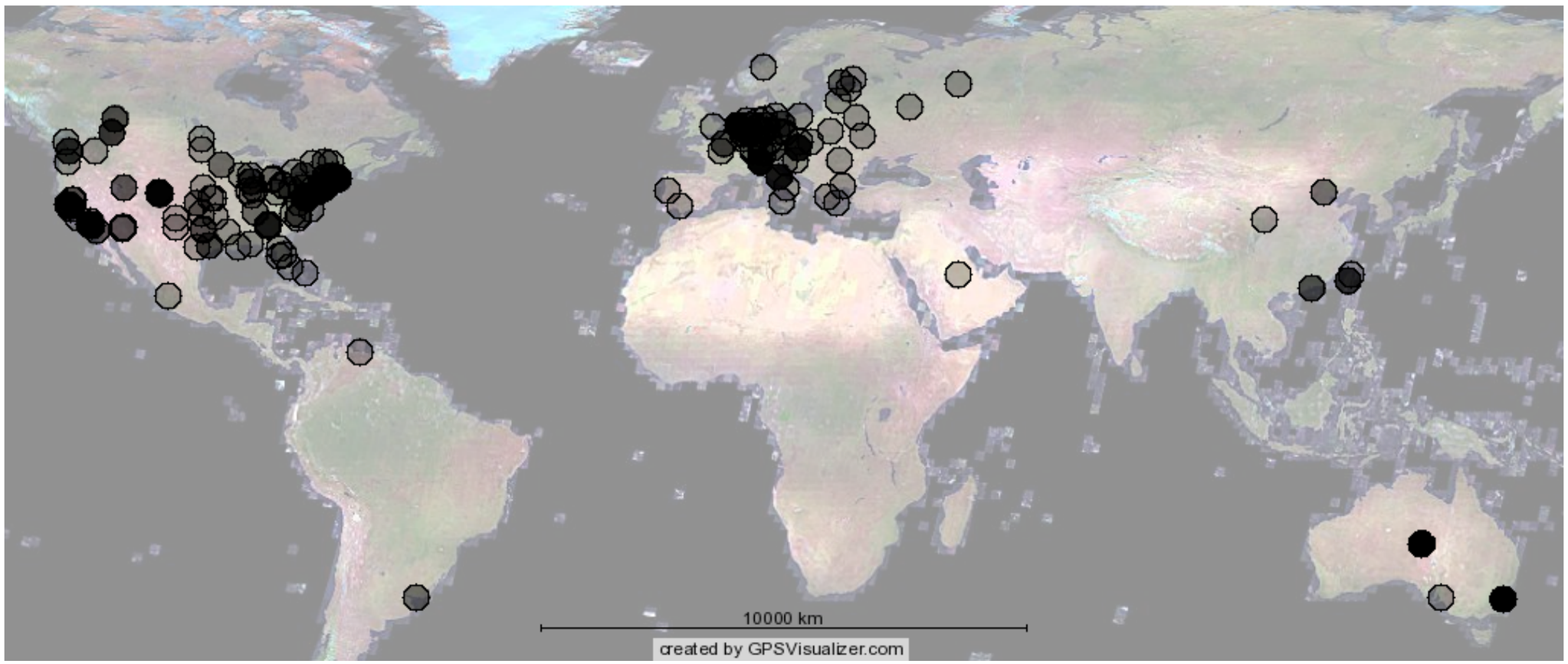
- Significant weaknesses:
  - **must trust network to provide anonymity!**
    - Q: what happens if a jondo is corrupt?
- If any message is intercepted, the receiver is trivially exposed
- Initiator has *probable innocence* against c malicious nodes if $n \geq \frac{p_f}{p_f - \frac{1}{2}}(c+1)$

Can we do better?

Yes, with **source routing**!
(not supported by the Internet,
but easy to support using network overlays)

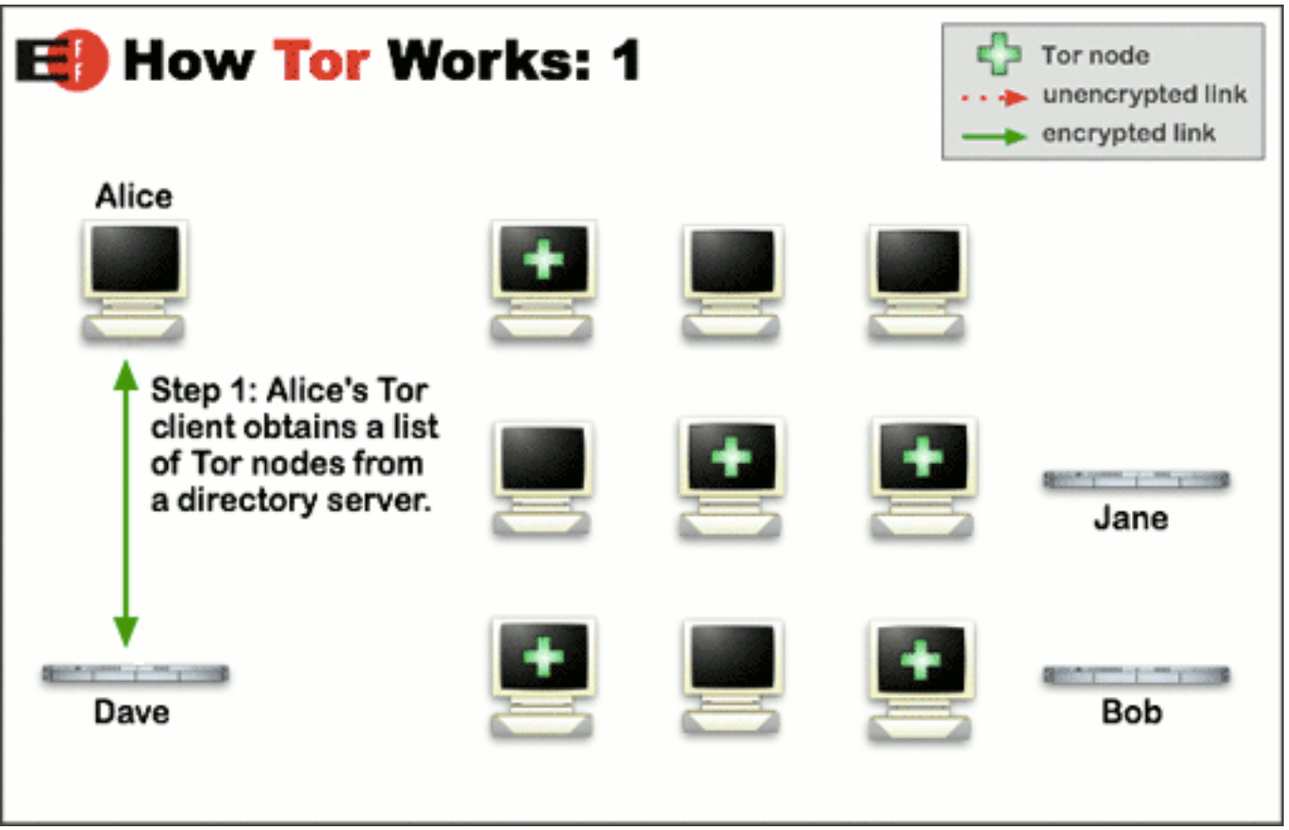
Tor (The Onion Router)

- FOSS onion routing implementation
- Network of approximately 6,555 geographically distributed volunteer onion routers (in 71 different countries)
- Approximately 2,500,000 users (difficult to accurately estimate b/c of that whole "anonymity" thing)
- ~300 Gbits/s consumed across the network

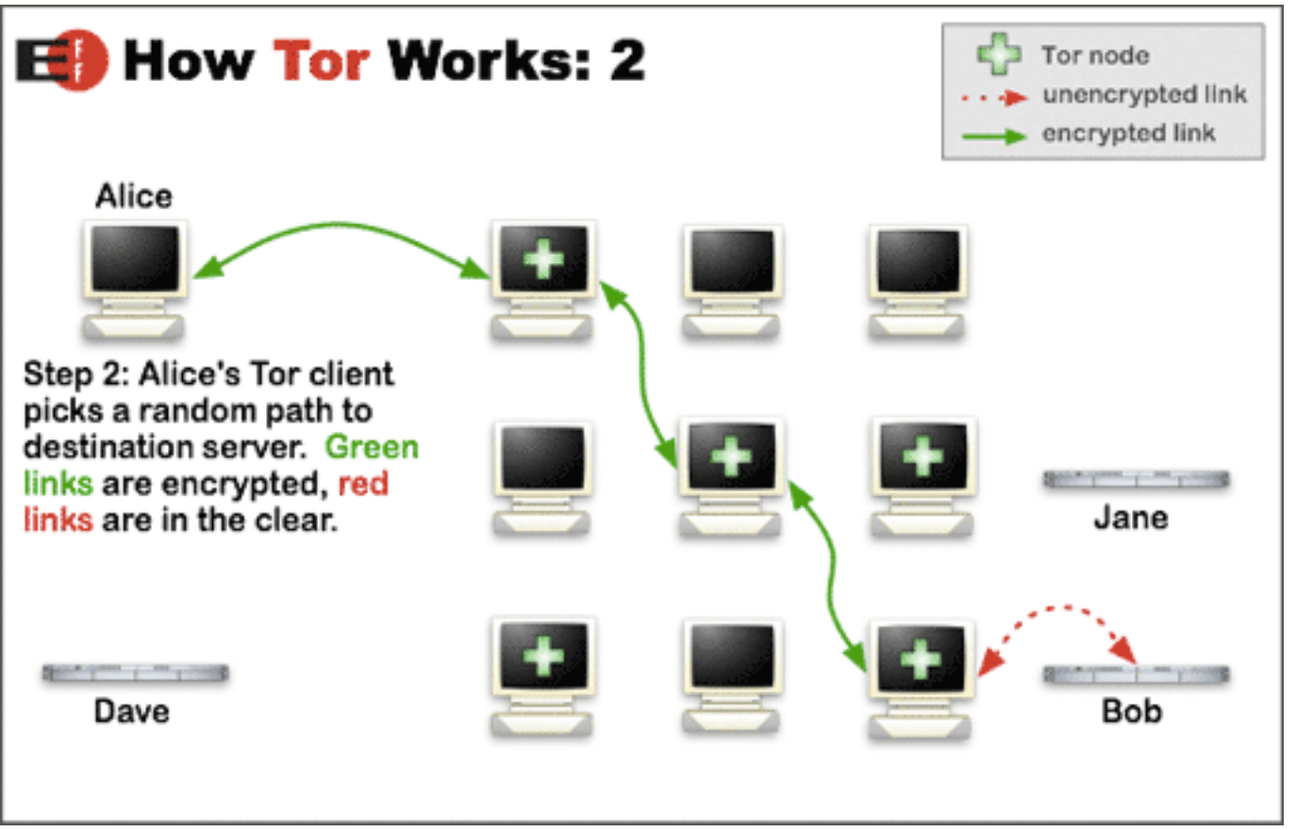


metrics.torproject.org

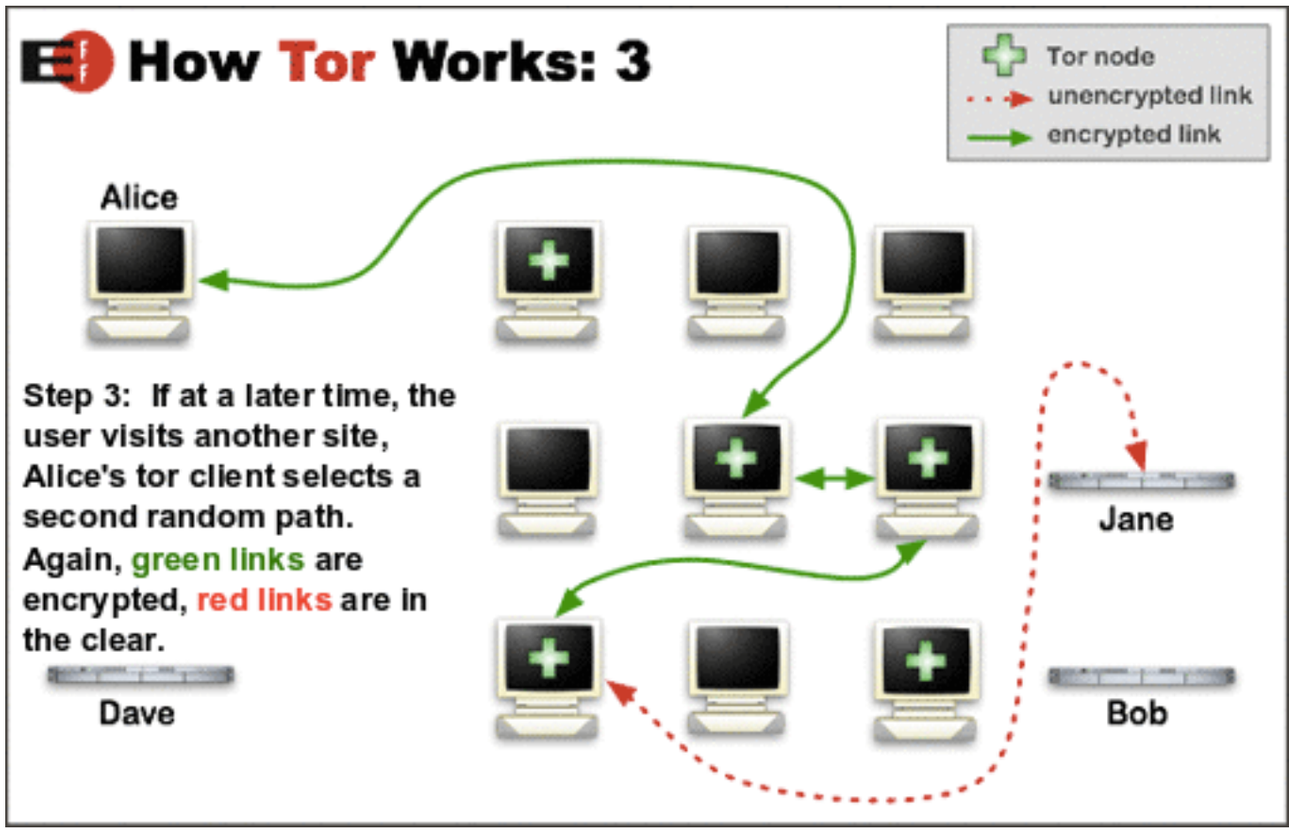
How Tor Works: 1



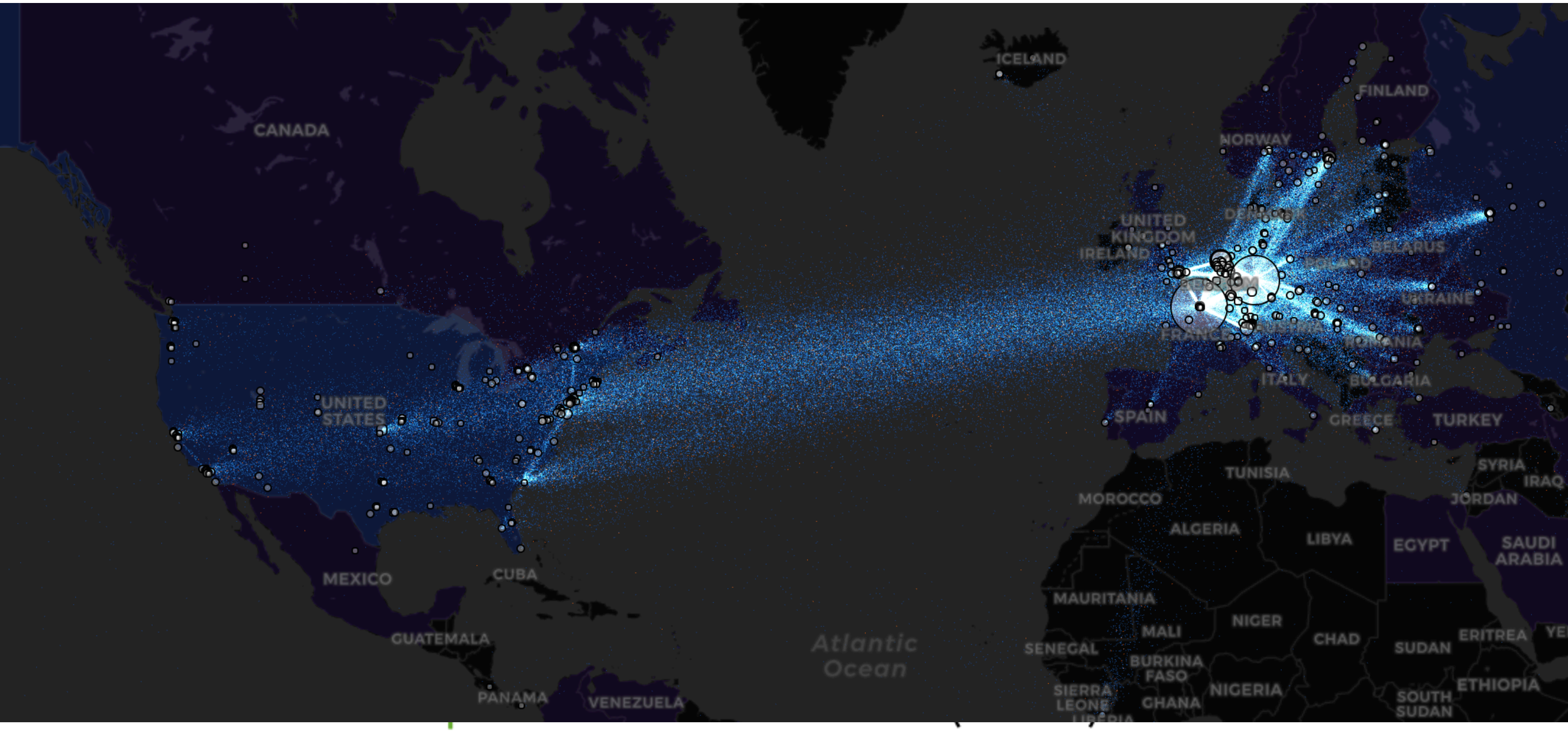
How Tor Works: 2



How Tor Works: 3



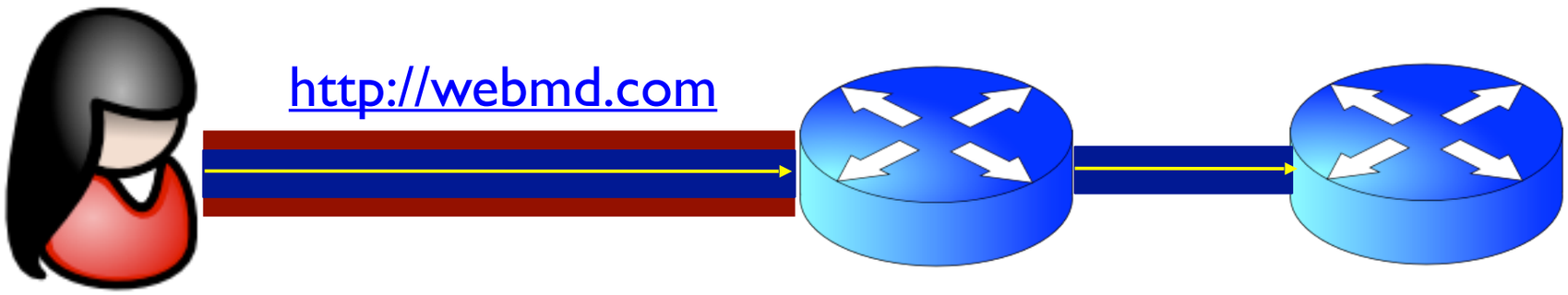
Who uses Tor?



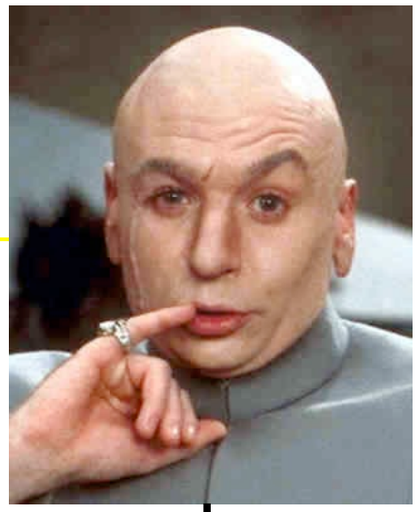
https://metrics.torproject.org/

Security issues with Tor

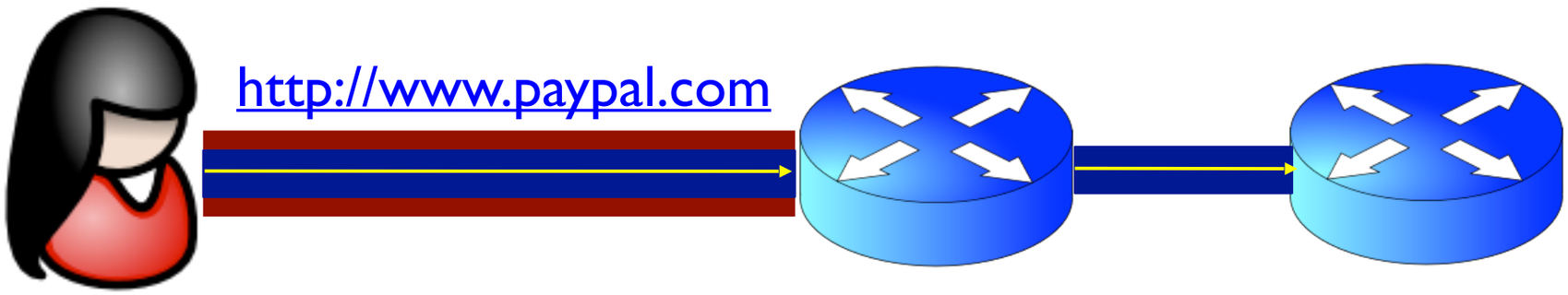
Anonymity Systems Lower the Bar for Eavesdropping



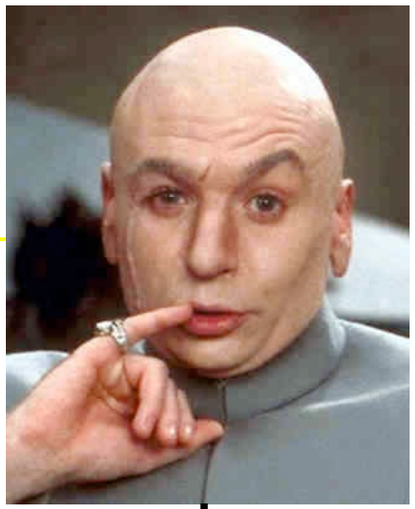
Malicious Relay

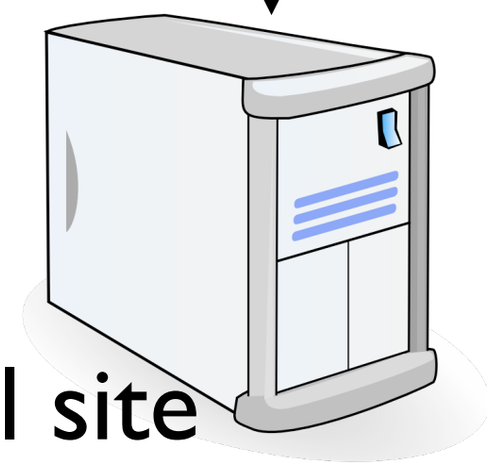


Anonymity Systems Lower the Bar for Routing Attacks



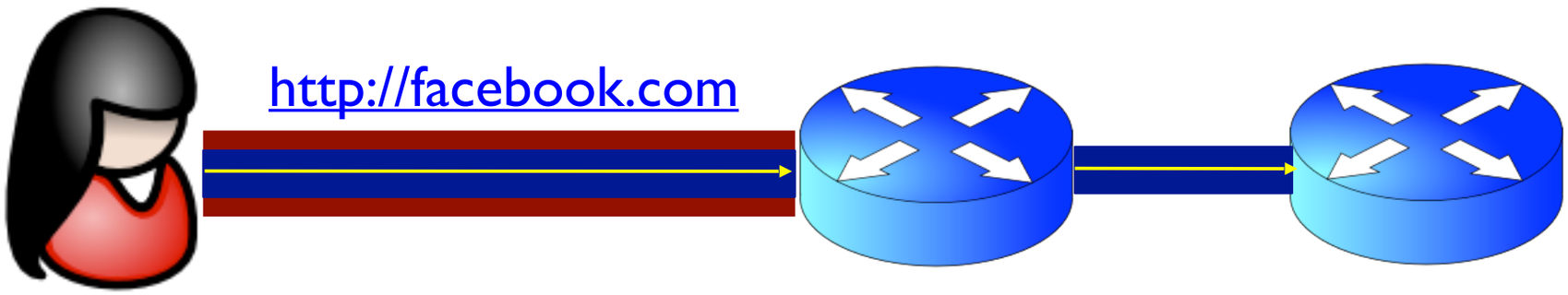
Malicious Relay



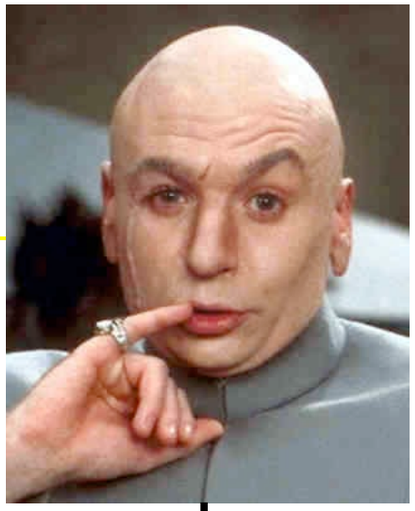


Fake Paypal site

Anonymity Systems Lower the Bar for MitM Attacks



Malicious Relay



Takeaways

- Use anonymity services with caution
  - Use HTTPS/SSL/TLS whenever possible
    - Don't ignore browser certificate warning messages
- The design and attack of Internet anonymity systems is a hot research area