CS 5450

Anonymity Networks

Vitaly Shmatikov

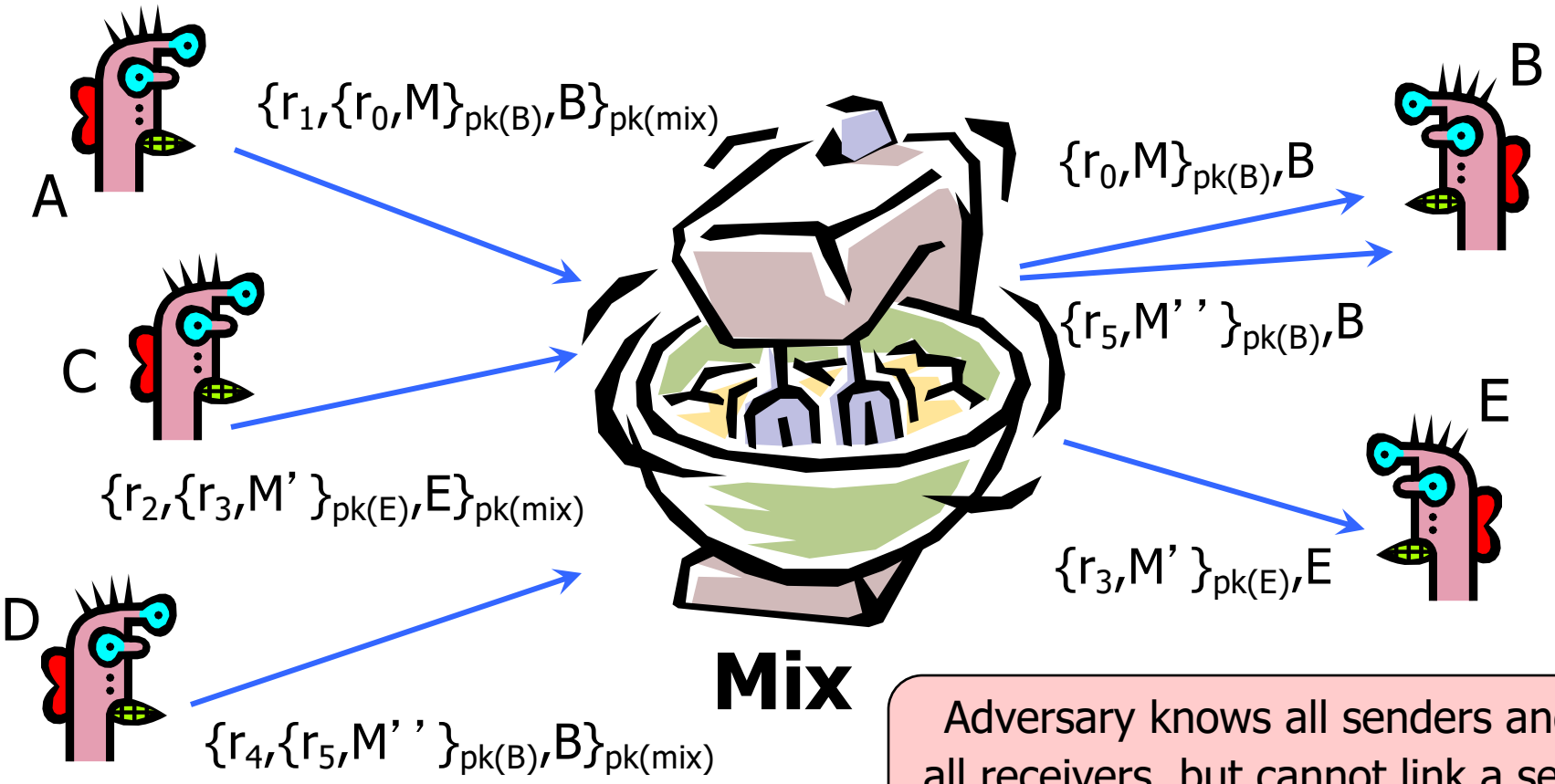
Privacy on Public Networks

- Internet is designed as a public network
- Routing information is public
  - IP packet headers identify source and destination
  - Even a passive observer can easily figure out who is talking to whom
- Encryption does not hide identities
  - Encryption hides payload, but not routing headers
  - Even IP-level encryption (VPNs, tunnel-mode IPsec) reveals IP addresses of gateways

Chaum's Mix

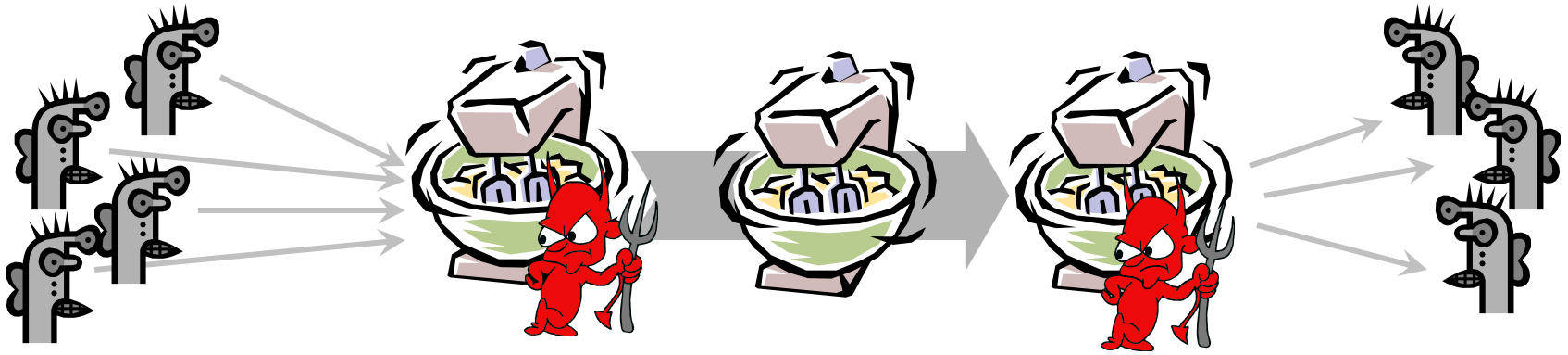
- Early proposal for anonymous email
  - David Chaum. "Untraceable electronic mail, return addresses, and digital pseudonyms". Communications of the ACM, February 1981.
- Public-key crypto + trusted re-mailer (Mix)
  - Untrusted communication medium
  - Public keys used as persistent pseudonyms
- Modern anonymity systems use Mix as the basic building block

Basic Mix Design



Adversary knows all senders and all receivers, but cannot link a sent message with a received message

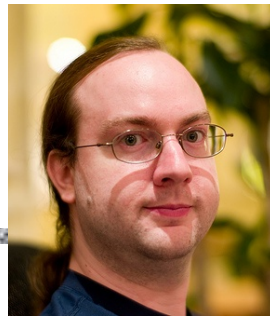
Mix Cascades and Mixnets



- Messages are sent through a sequence of mixes
  - Can also form an arbitrary network of mixes ("mixnet")
- Some of the mixes may be controlled by attacker, but even a single good mix ensures anonymity
- Pad and buffer traffic to foil correlation attacks

From Mixnets to Onion Routing

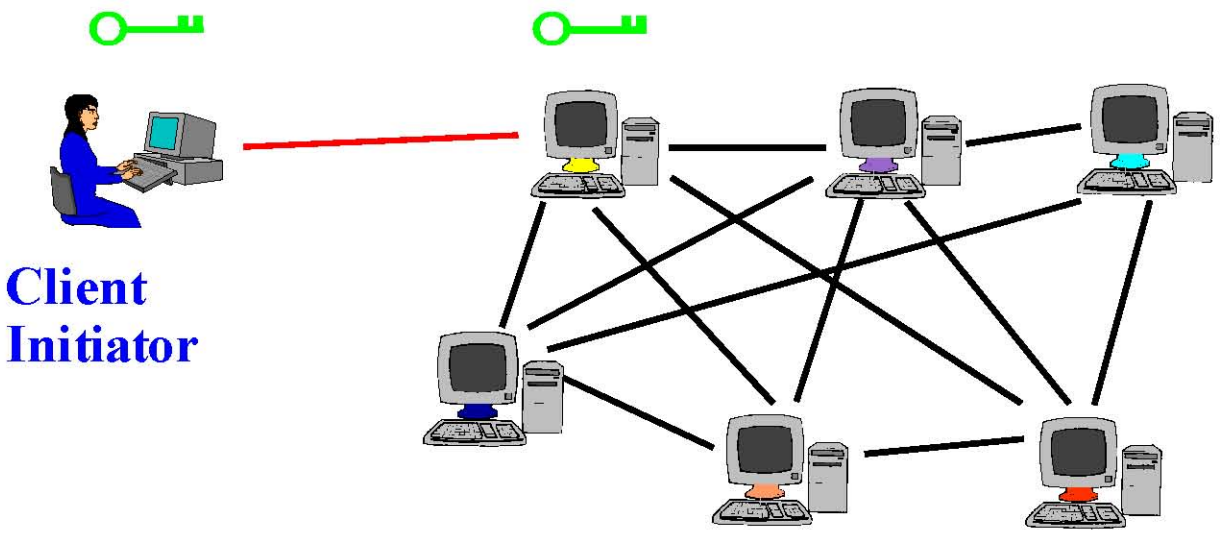
- Public-key encryption and decryption at each mix are computationally expensive
- Basic mixnets have high latency
  - Ok for email, but not for Web browsing
- Challenge: low-latency anonymity network
  - Use public-key crypto to establish a "circuit" with pairwise symmetric keys between hops
  - Then use symmetric decryption and re-encryption to move data along the established circuits



- Second-generation onion routing network
  - http://tor.eff.org
  - Specifically designed for low-latency anonymous Internet communications (e.g., Web browsing)
  - Running since October 2003
- Hundreds of nodes on all continents
- Over 2,500,000 users
- “Easy-to-use” client
  - Freely available, can use it for anonymous browsing

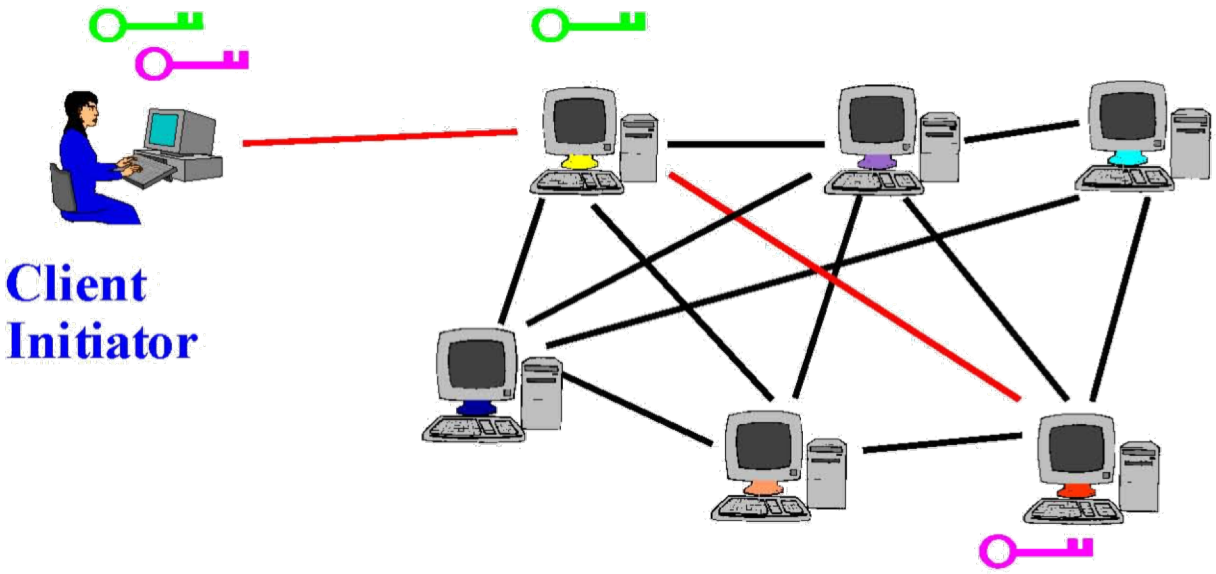
Tor Circuit Setup (1)

- Client proxy establishes a symmetric session key and circuit with Onion Router #1



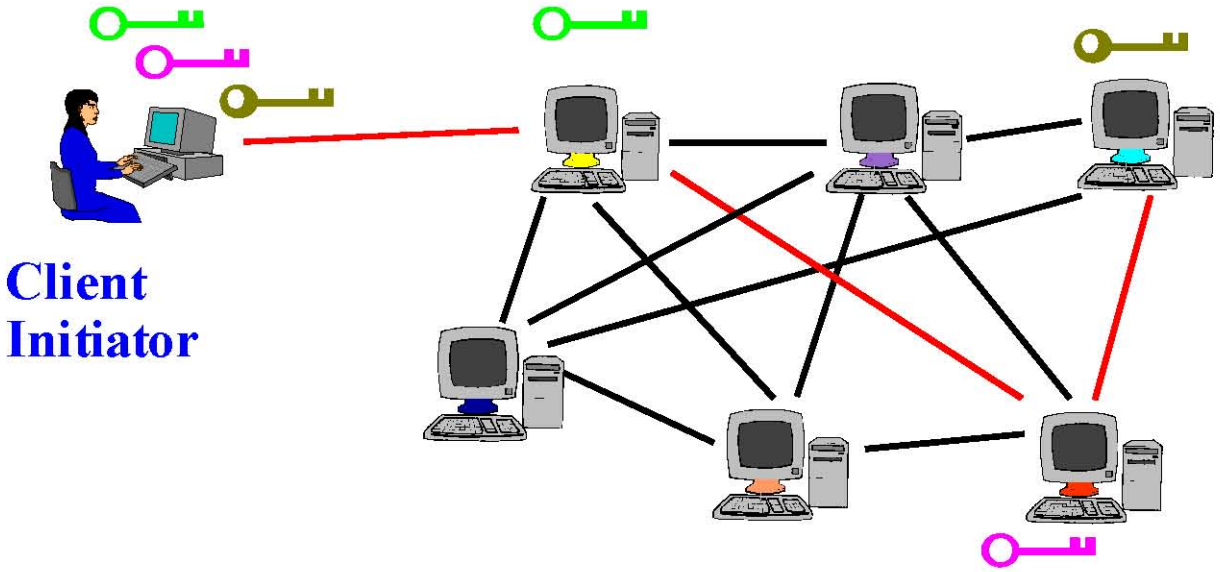
Tor Circuit Setup (2)

- Client proxy extends the circuit by establishing a symmetric session key with Onion Router #2
  - Tunnel through Onion Router #1



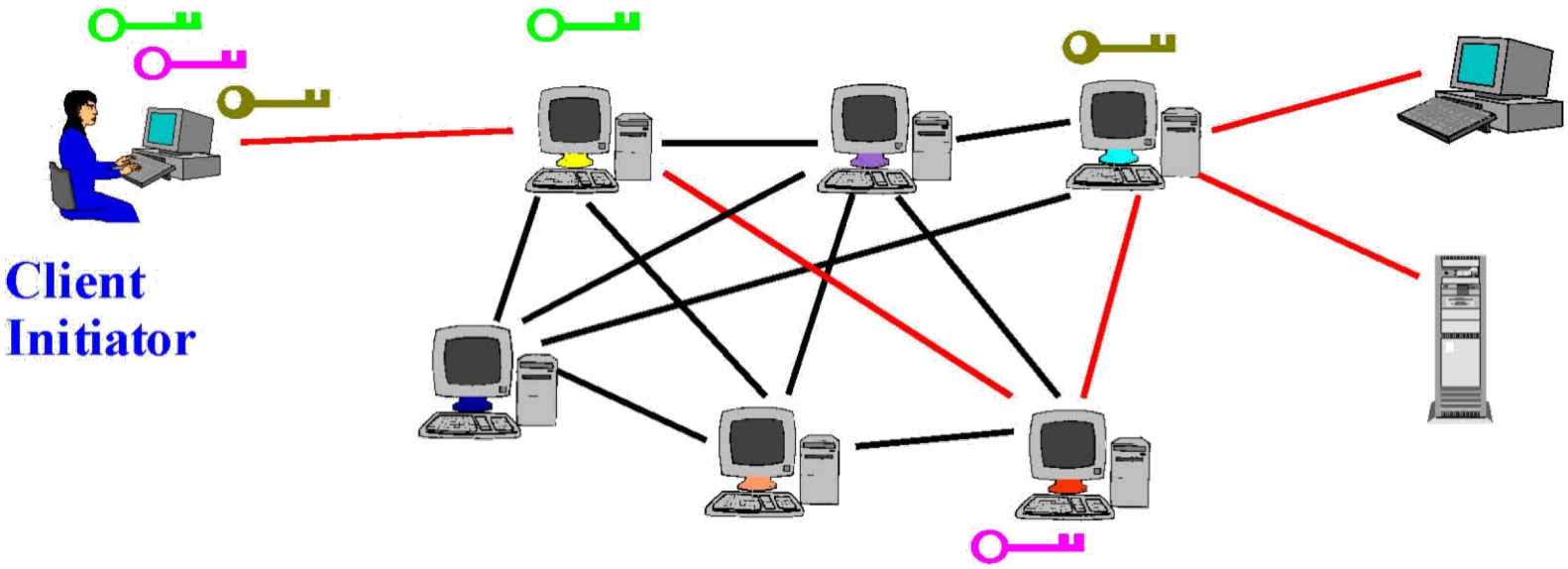
Tor Circuit Setup (3)

- Client proxy extends the circuit by establishing a symmetric session key with Onion Router #3
  - Tunnel through Onion Routers #1 and #2



Using a Tor Circuit

- Client applications connect and communicate over the established Tor circuit
  - Datagrams decrypted and re-encrypted at each link



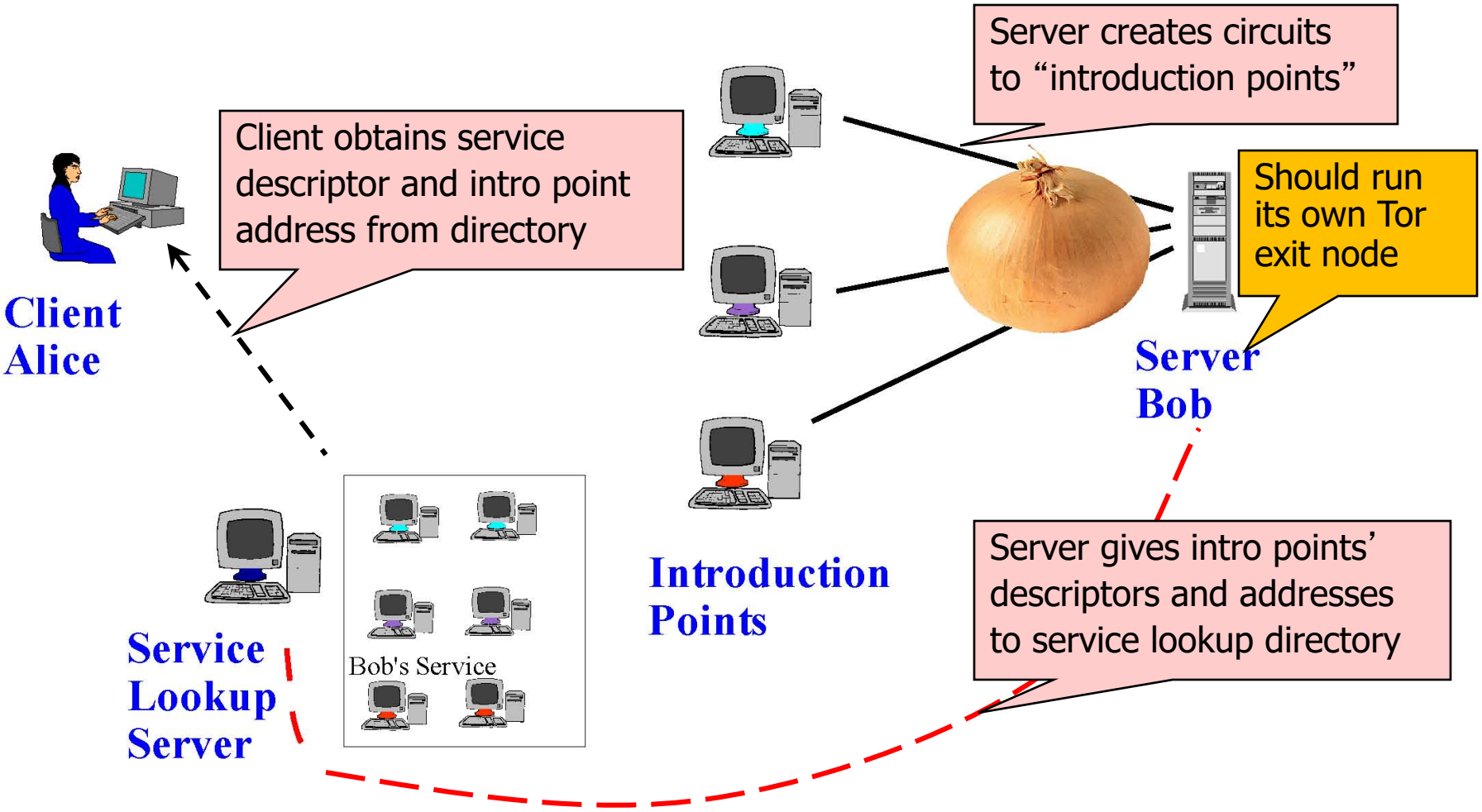
Tor Management Issues

- Many TCP connections can be "multiplexed" over one anonymous circuit
- Directory servers
  - Lists of active onion routers, their locations, current public keys, etc.
  - Control how new routers join the network
    - "Sybil attack": attacker creates a large number of routers
  - Directory servers' keys ship with Tor code

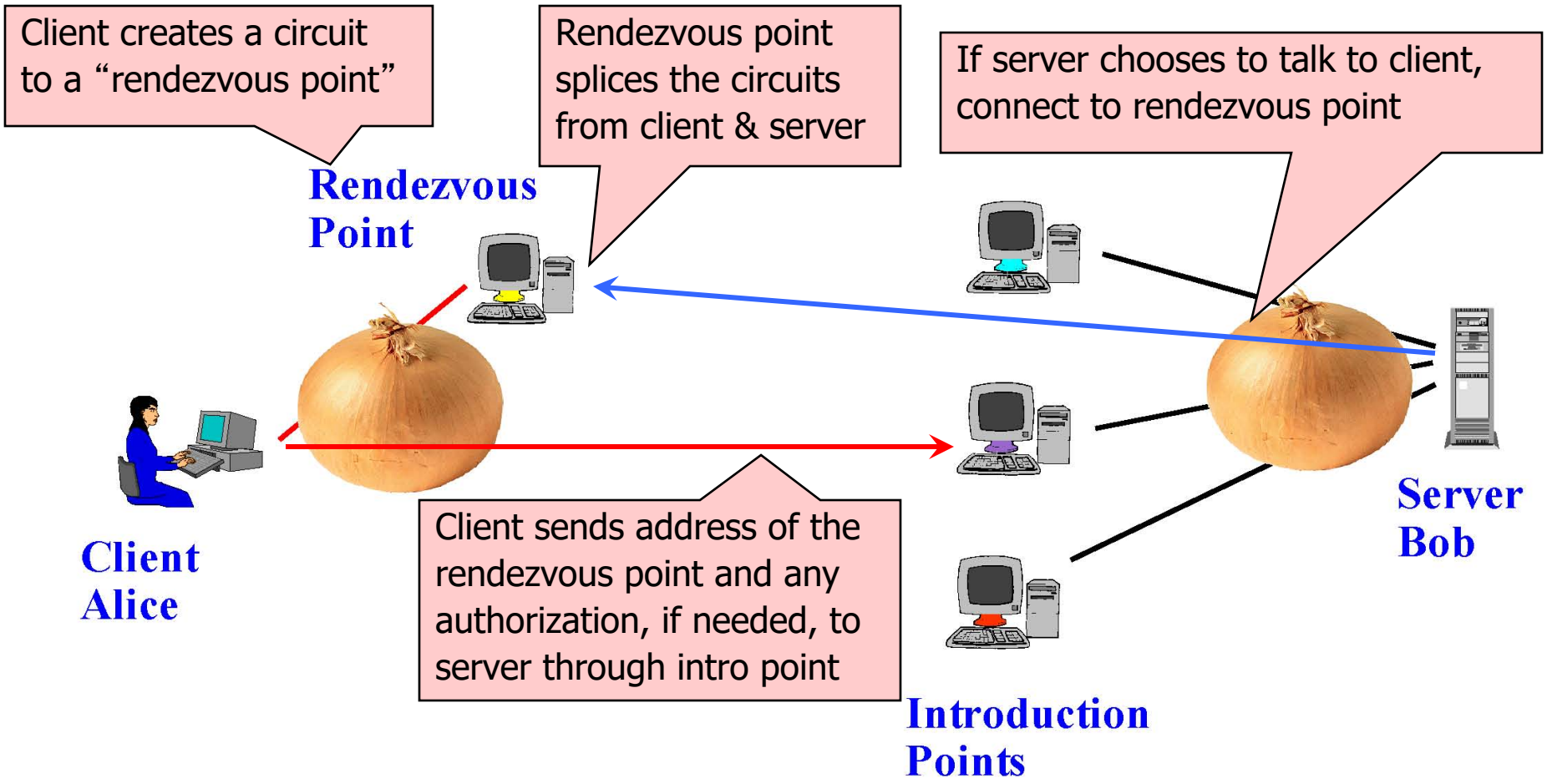
Location Hidden Services

- Goal: deploy a server on the Internet that anyone can connect to without knowing where it is or who runs it
- Accessible from anywhere
- Resistant to censorship
- Can survive a full-blown DoS attack
- Resistant to physical attack
  - Can’t find the physical server!

Deploying a Hidden Service



Using a Hidden Service



Silk Road

anonymous marketplace

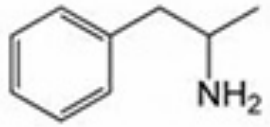
Wel
messages(0) | orders(0) | account(฿0.00)

Shop by category:

- Drugs(1582)
  - Cannabis(271)
  - Dissociatives(33)
  - Ecstasy(217)
  - Opioids(106)
  - Other(65)
  - Prescription(274)
  - Psychedelics(306)
  - Stimulants(190)
- Apparel(37)
- Art(1)
- Books(300)
- Computer equipment(9)
- Digital goods(218)
- Drug paraphernalia(33)
- Electronics(13)

10 Grams high grade MDMA 80+%

฿61.17



Amphetamines sulfate / Speed freebase...

฿28.59

2g Jack Frost (weed) *420 SALE****

฿8.54

5 Grams of pure MDMA crystals

฿42.04

100 red Y tablets 111mg (lab tested)...

฿97.77

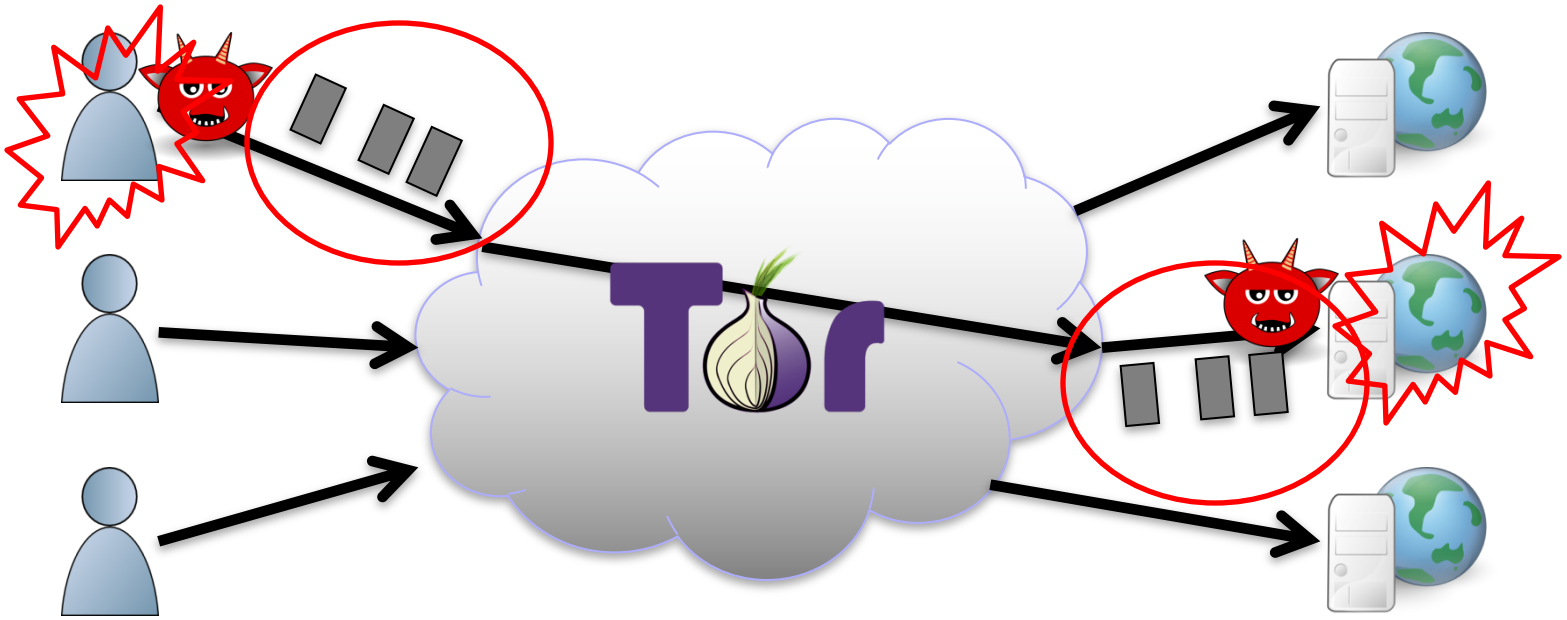
Michael Jackson Discography 1971-2009...

฿2.52

New

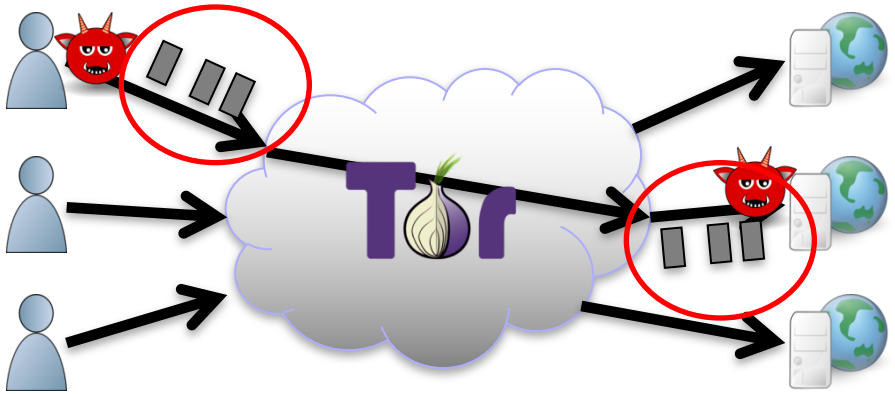
- Th or
- W fa
- Ac H
- A m A
- St A

Main (?) Tor Problem



Traffic correlation and confirmation

Traffic Confirmation Techniques

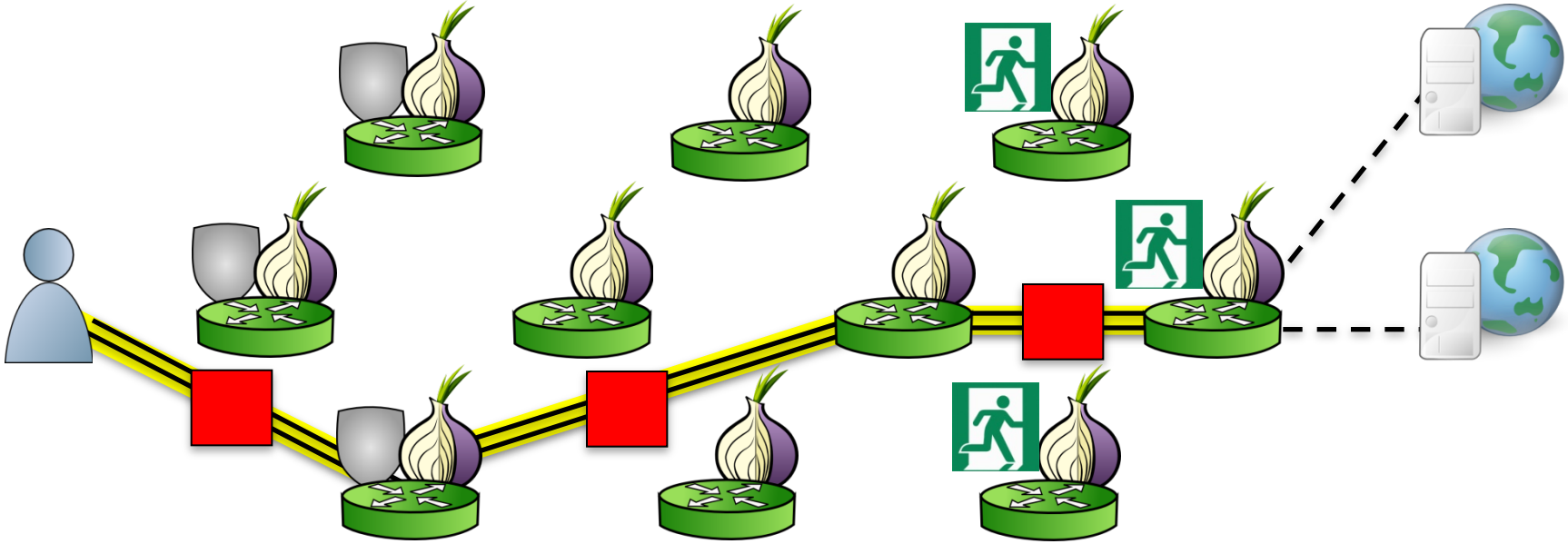


- Congestion and denial-of-service attacks
  - Attack a Tor relay, see if circuit slows down
- Throughput attacks
- Latency leaks
- Website fingerprinting

Not a Theoretical Threat!

- Sybil attack + traffic confirmation
- In 2014, two CMU CERT “researchers” added 115 fast relays to the Tor network
  - Accounted for about 6.4% of available guards
  - Because of Tor’s guard selection algorithm, these relays became entry guards for a significant chunk of users over their five months of operation
- The attackers then used these relays to stage a traffic confirmation attack

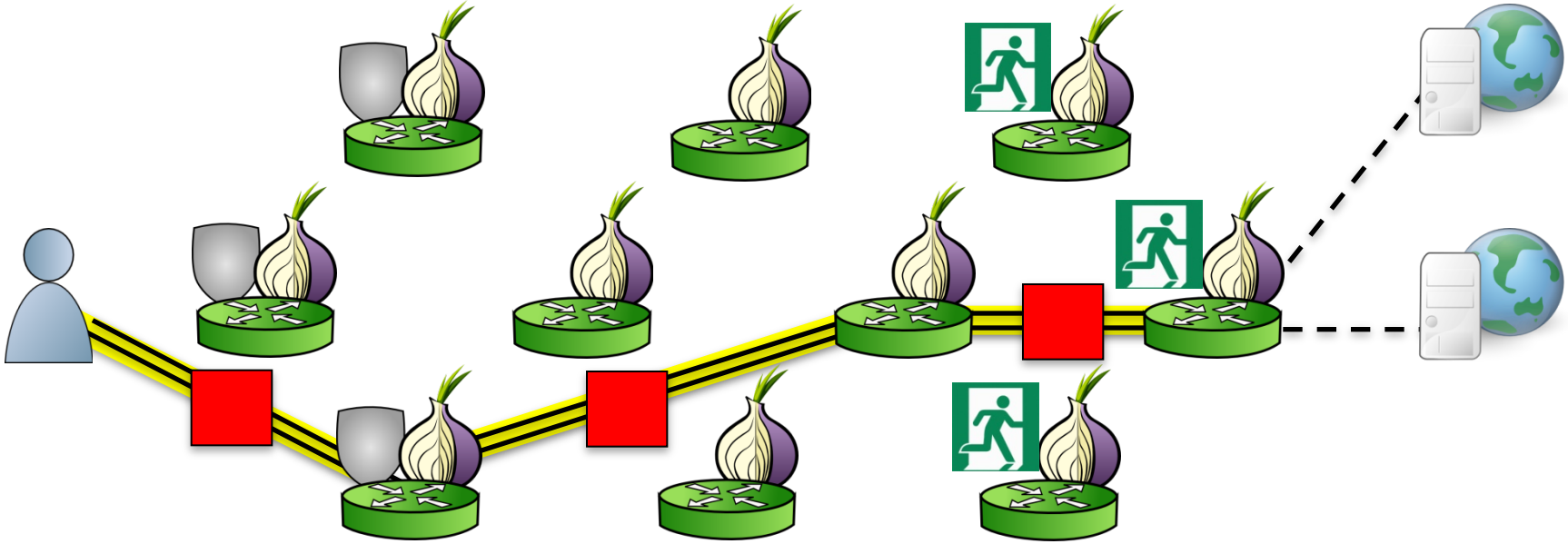
RELAY_EARLY Cell



Special control cell sent to the other end of the circuit (not just the next hop, like normal cell)

Used to prevent building very long Tor paths

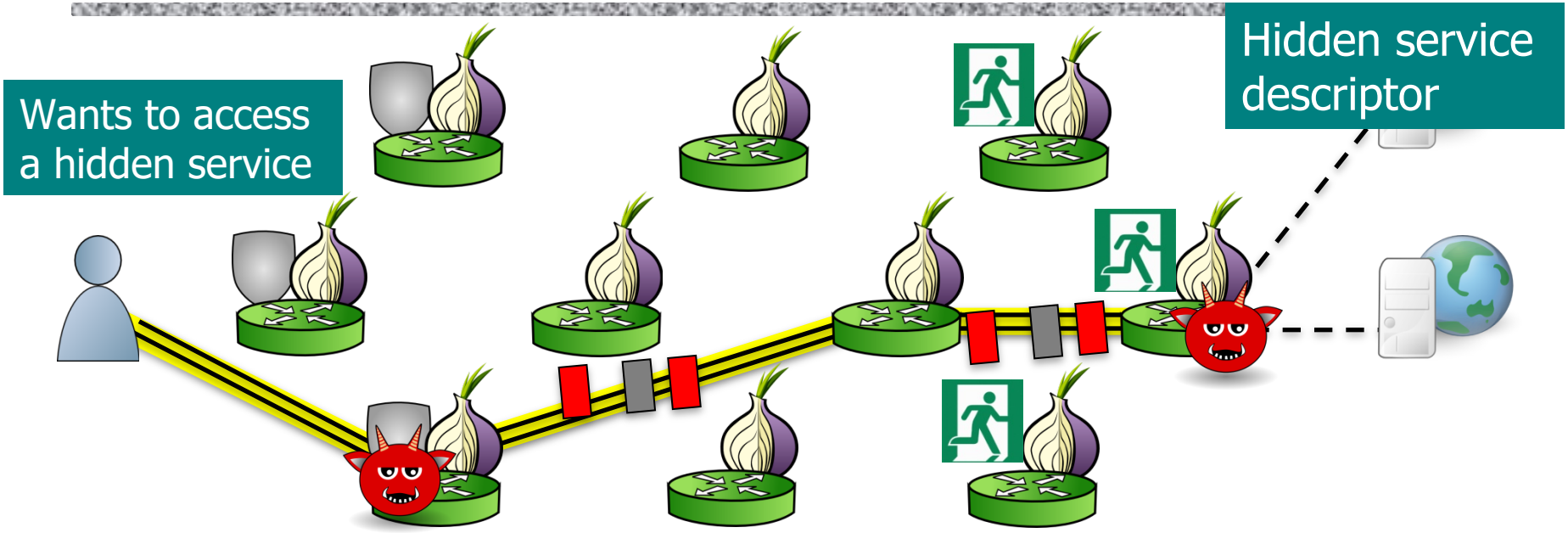
RELAY_EARLY Sent Backward



Any number of RELAY_EARLY cells can be sent backward along the circuit

No legitimate reason for this, just an oversight

Traffic Confirmation



Malicious exit node encodes the name of hidden service in the pattern of relay and padding cells

Malicious guard learns which hidden service the client is accessing