



Secure Web Access: Onion Routing and Self-Authentication

Paul Syverson
U.S. Naval Research Laboratory

Technion Summer School on
Cyber and Computer Security
Haifa (via Cyberspace)
September 7 02020

Some main take-aways

- Tor and onion services are primarily just ways to access ordinary internet sites more securely.
- They are today where web encryption (https) was around 02001.
- There are no stupid questions: please ask.

Motivational Use Case Example

- U.S. Navy Commander Alice going on travel overseas
 1. Before traveling she must get DoD anti-terror training



AT Themes

 ANON		Be Anonymous
 PLAN		Plan Ahead
 AWARE		Be Aware
 ACCESS		Control Access
 UNPRED		Be Unpredictable
 TEAM		Be a Team Player

Blend in, don't be an easily identified target

Think ahead and choose safer options

Look for suspicious persons/activities

Prevent crime, maintain security

Change routines, routes, times, and speeds

Cooperate with unit security measures



ANTI-TERRORISM

AT FUNDAMENTALS

Surveillance Detection

Government Facility

Active Shooter

Residential

Off-Duty Activities

Air Travel

Don't be a Target



Items that display your DOD affiliation may also help identify you as a potential target.

Not all threats are predictable. As a result, you should consider your surroundings for attack.

Reduce your exposure by being inconspicuous in your surroundings.

- Do not wear clothing or accessories that draw criminal attention
- Remain low key and do not display DOD affiliation
- Avoid places of high criminal activity

In addition to blending in, you can reduce your exposure:

- Select places with security measures to reduce local threat
- Be unpredictable and vary your routes
- Travel with a friend or family member
- Use automobiles and residences with security features

You can greatly increase your safety by remaining anonymous and inconspicuous.

Select Next to continue.



Anticipate



Be Vigilant



Don't be a Target



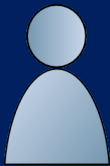
Respond & Report

Be inconspicuous when out & about

Motivational Use Case Example

- U.S. Navy Commander Alice going on travel overseas
 1. Before traveling she must get DoD anti-terror training
 2. She follows her training when traveling or working on site
 3. Safe back in her hotel room, she needs to connect to her home worksite at the U.S. Naval Research Lab

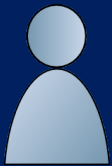
Connecting when overseas



Commander Alice
back in her hotel

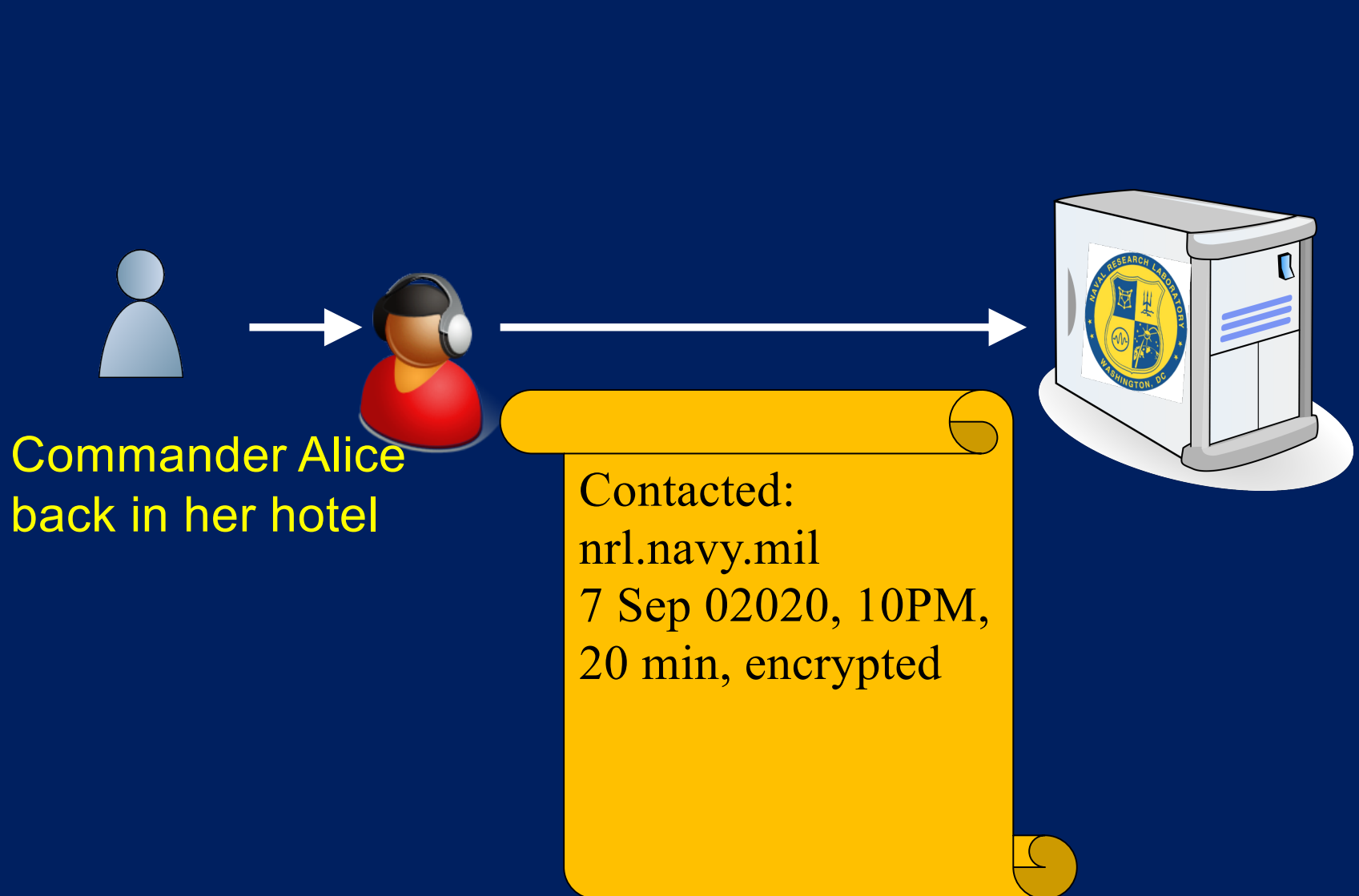
Connecting when overseas

What does she need to do to secure her connection?



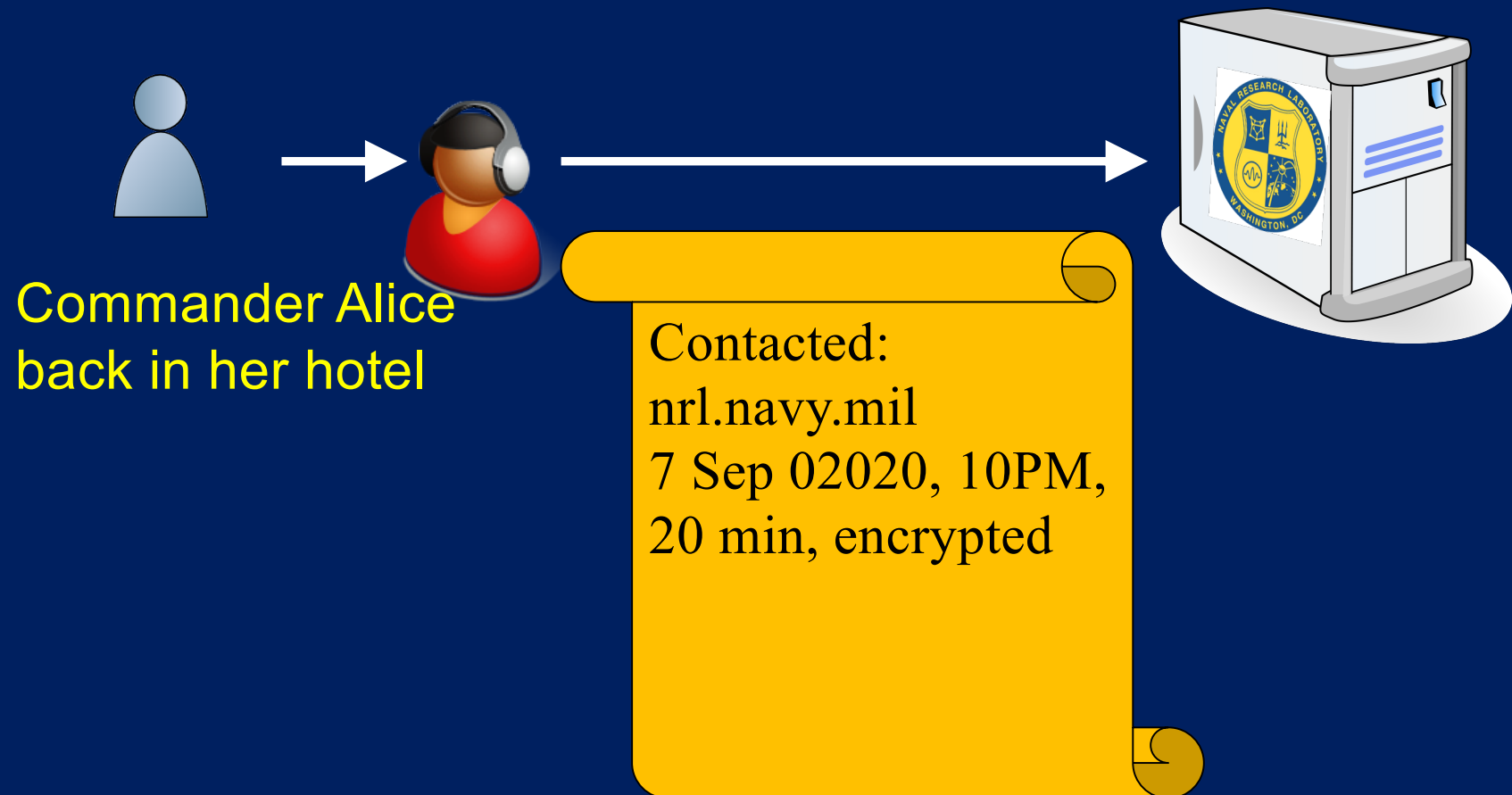
Commander Alice
back in her hotel

Encryption is not adequate

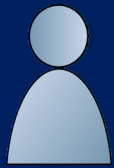


Encryption is not adequate for OPSEC or counter-intelligence

Identified as likely U.S. Navy, anywhere else she connects now under scrutiny



Encryption is not adequate for personnel protection



Commander Alice
back in her hotel

Contacted:
nrl.navy.mil
7 Sep 02020, 10PM,
20 min, encrypted
Rm: 416
Ckout on:
11 Sep 02020

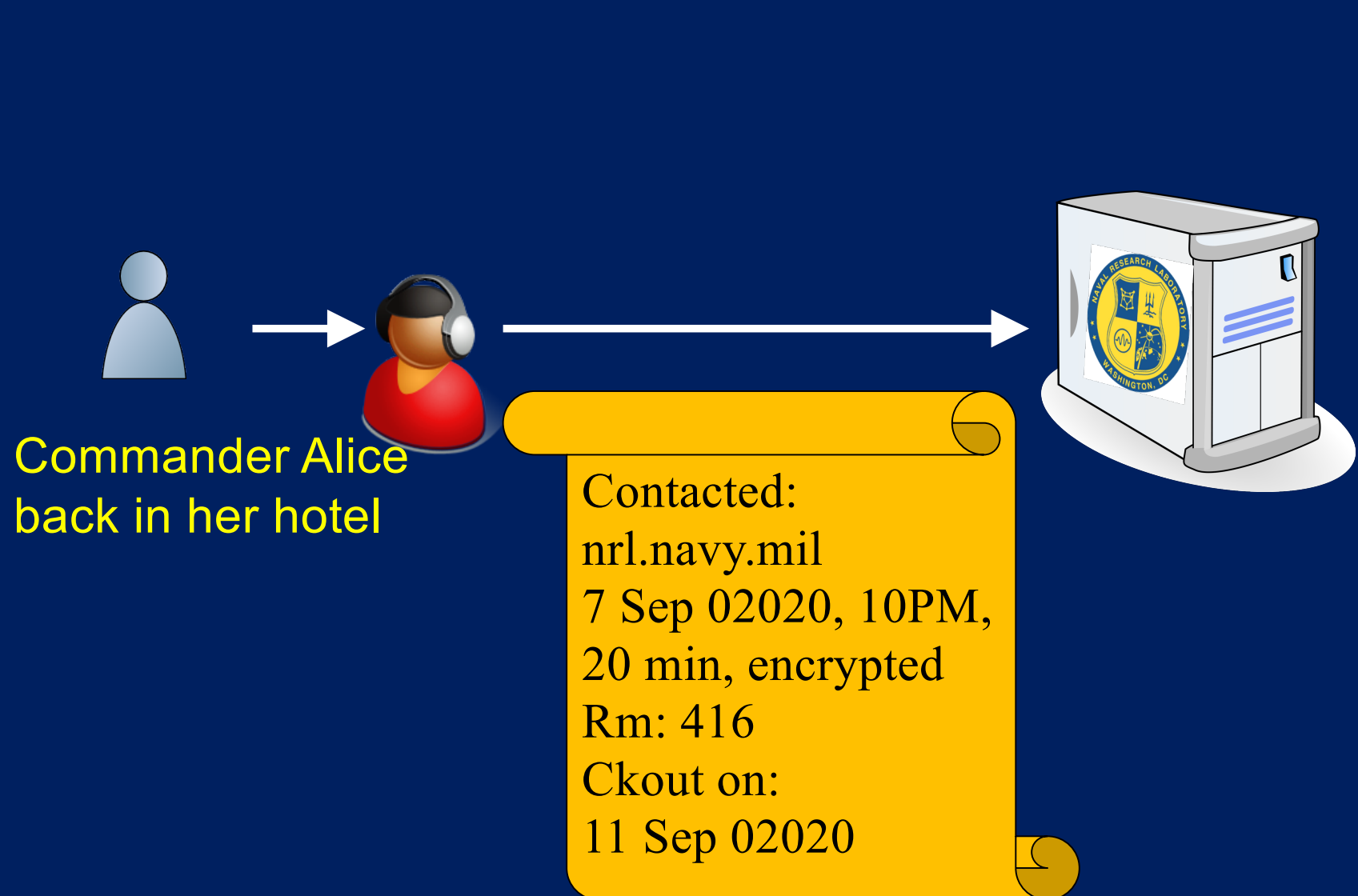
Some additional government uses

- Open source intelligence gathering
 - Patent examiners investigating related work
- Interactions with criminals
 - Visit gang website without telegraphing law enforcement affiliation
- Encouraging open communications with citizens
 - Sensitive information & sensitive services: public health, tax or immigration info, amnesty info for crimes, gun/drug surrender, ...
- Protecting the public infrastructure
 - Interacting with network sensors
 - Hiding access points for SCADA and critical systems
 - Secure system administration from remote locations

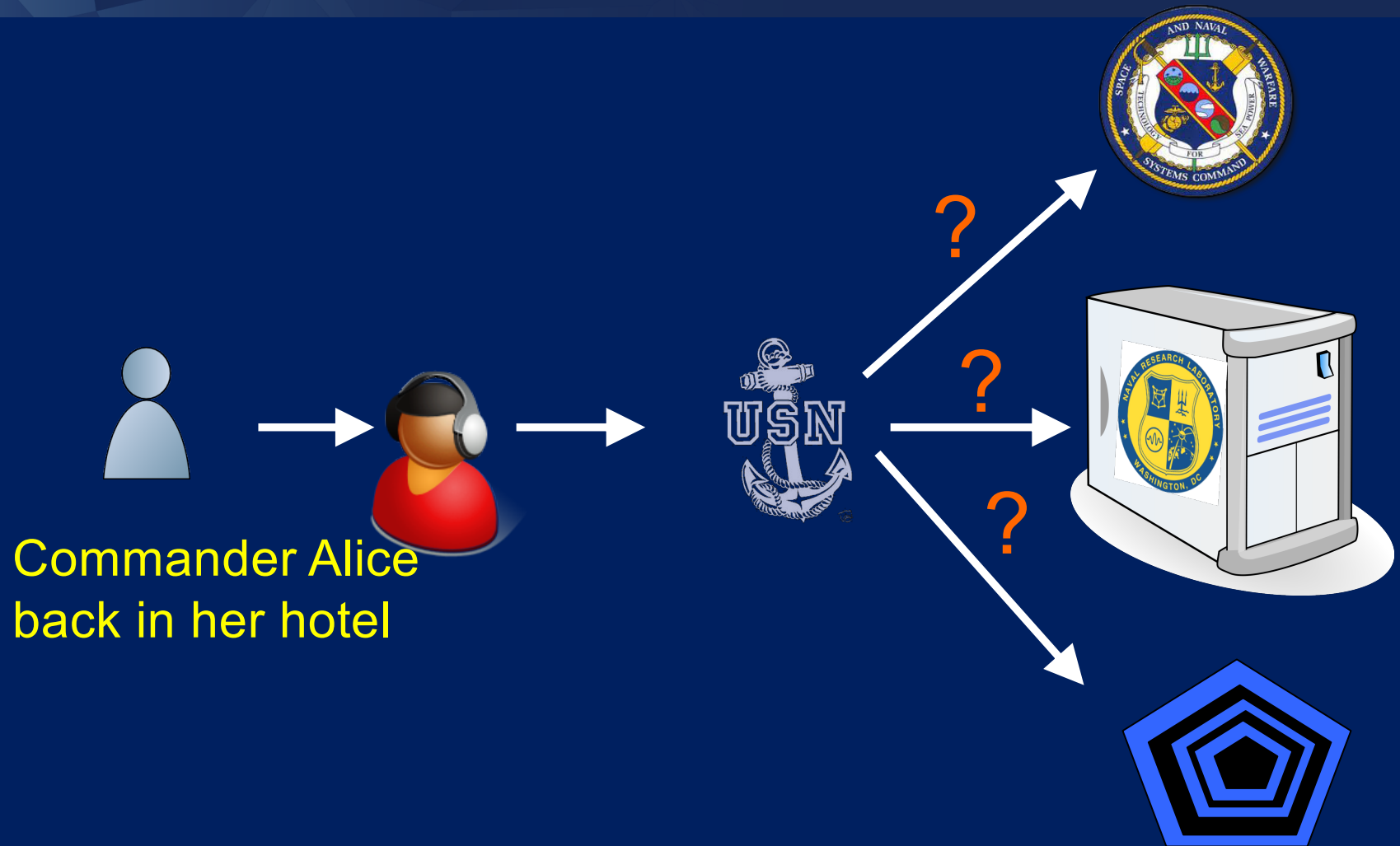
What would a solution look like for securing these government activities?

- Open source intelligence gathering
 - Patent examiners investigating related work
- Interactions with criminals
 - Visit gang website without telegraphing law enforcement affiliation
- Encouraging open communications with citizens
 - Sensitive information & sensitive services: public health, tax or immigration info, amnesty info for crimes, gun/drug surrender, ...
- Protecting the public infrastructure
 - Interacting with network sensors
 - Hiding access points for SCADA and critical systems
 - Secure system administration from remote locations

What would a solution look like for securing these government activities?

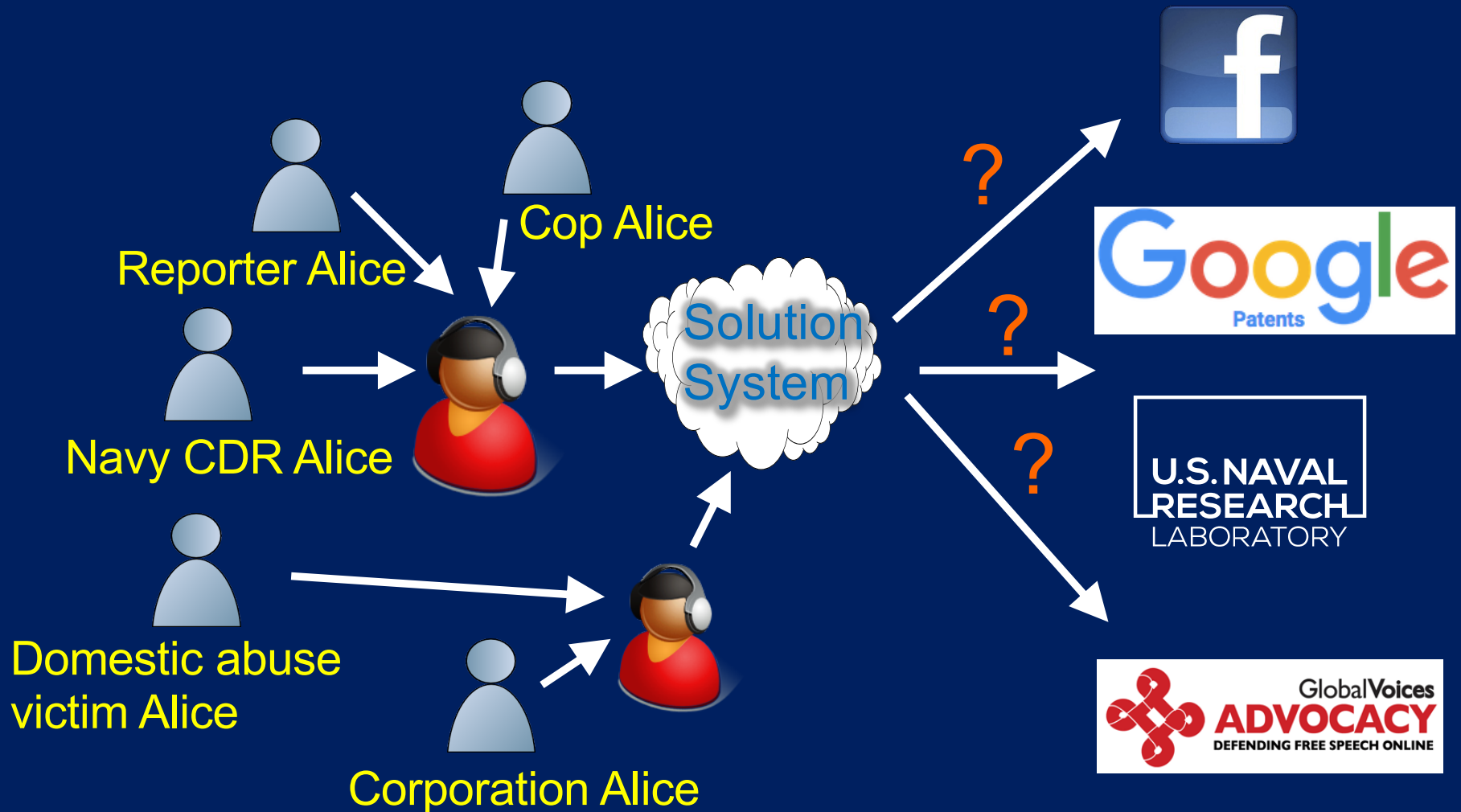


VPNs of limited help



Commander Alice
back in her hotel

Carry traffic for diverse users with diverse goals and adversaries

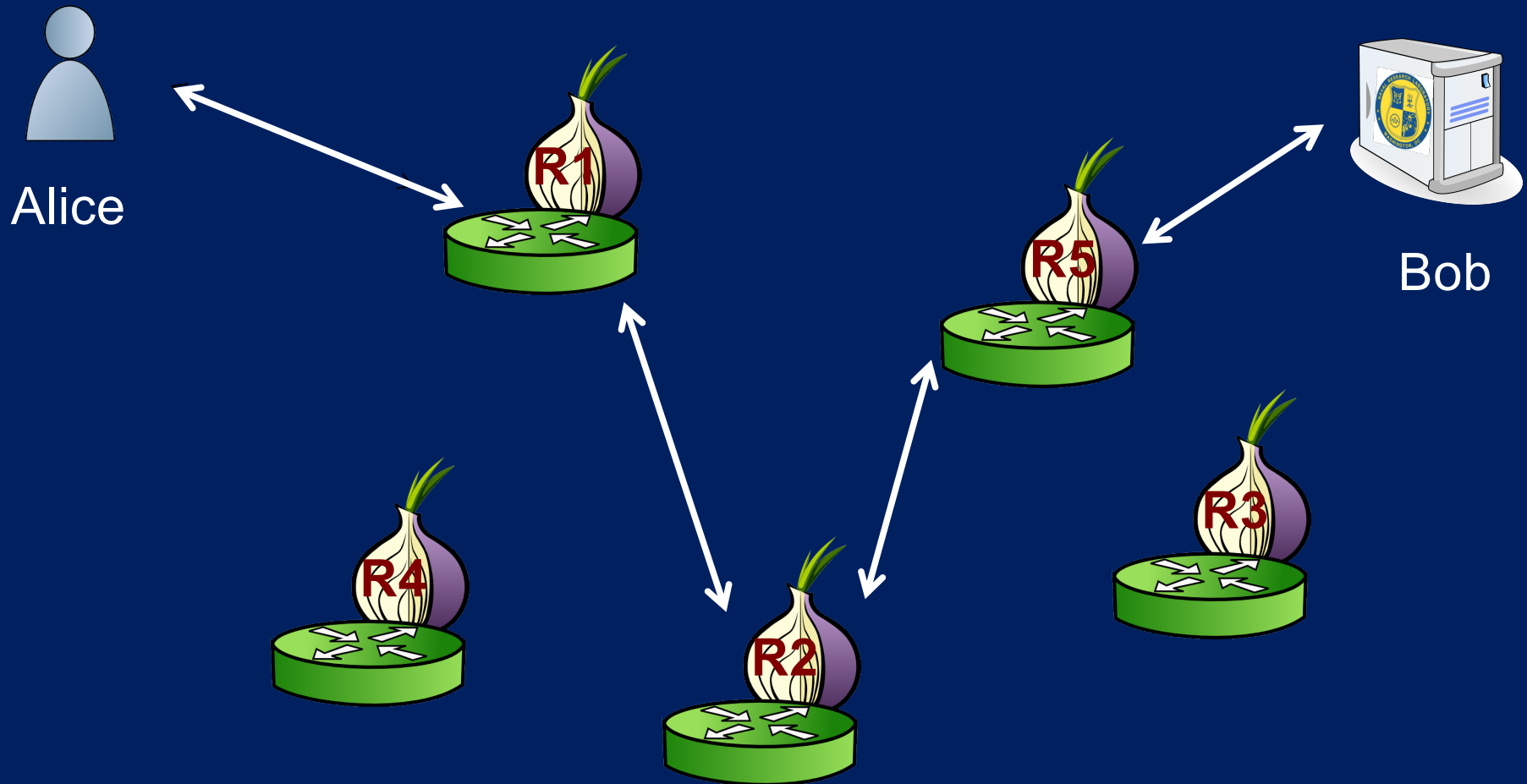




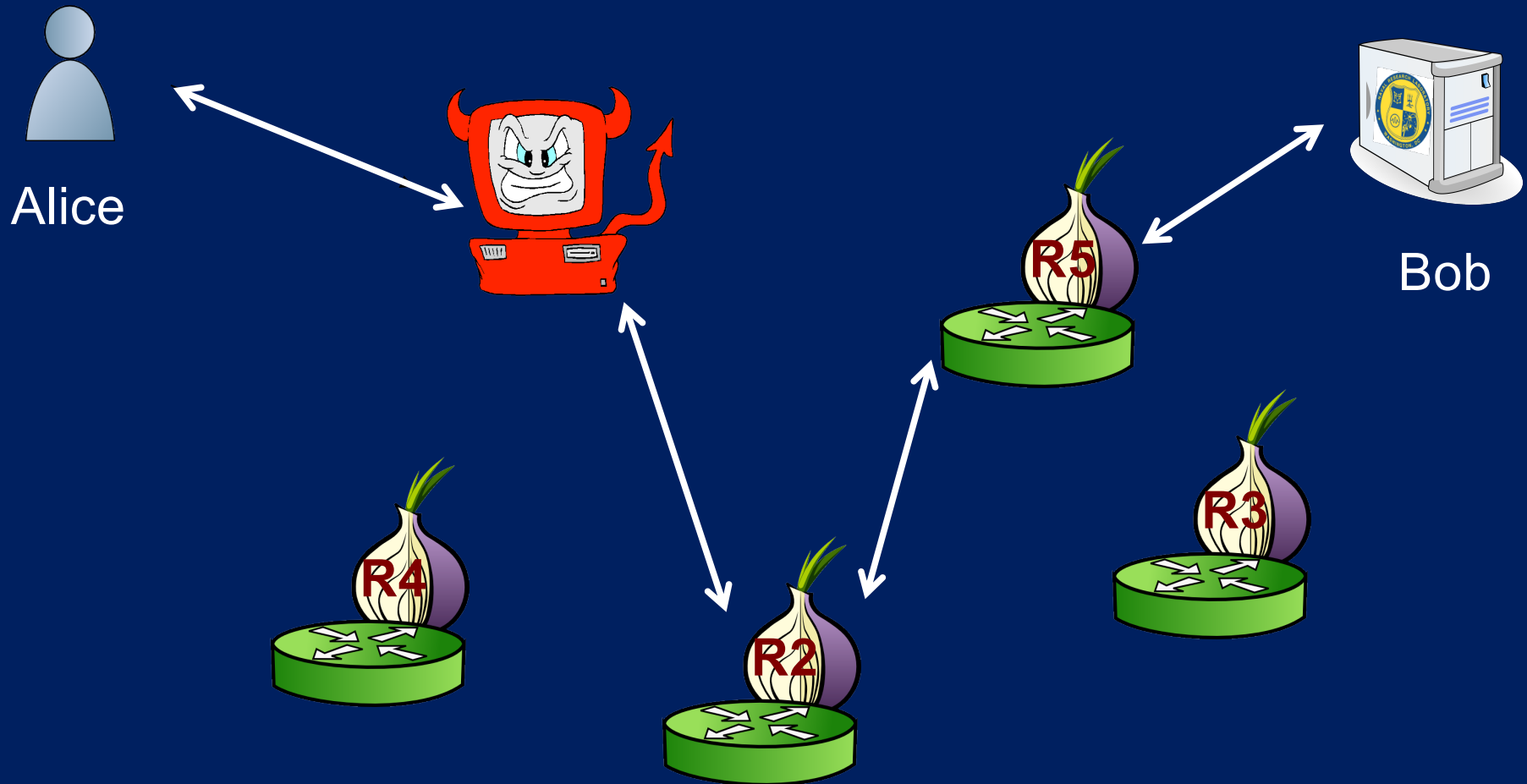
Solution must

- Carry traffic bidirectionally with low latency
- Carry traffic for a diverse user population
 - not just Navy or U.S. govt.
 - cannot have single point of failure/trust for any type of user
 - Diversely managed infrastructure
 - Open source

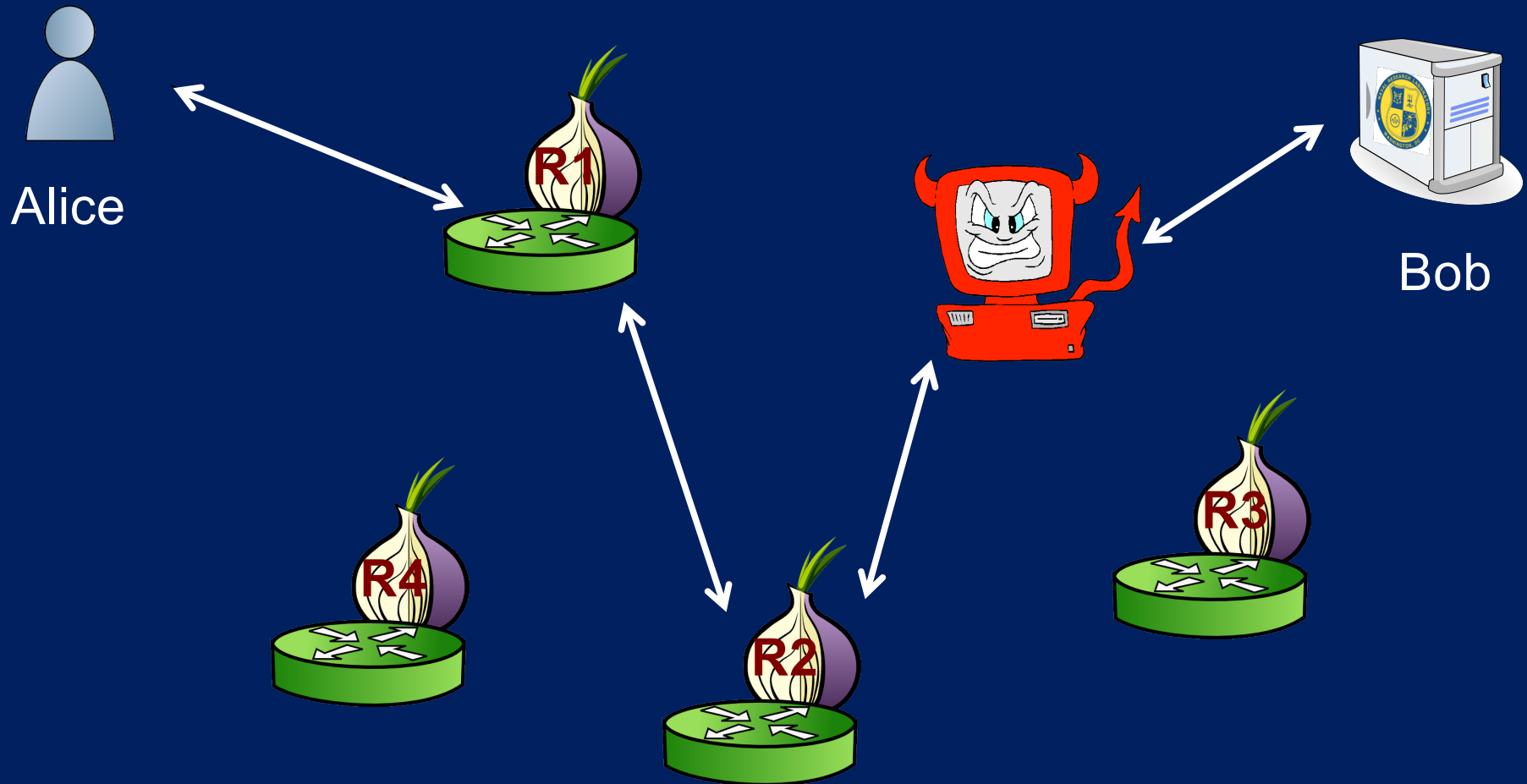
Idea: network of diversely managed relays so that no single one can betray Alice



A corrupt first hop can tell that Alice is talking, but not to whom

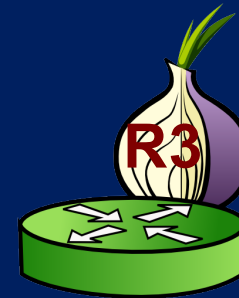
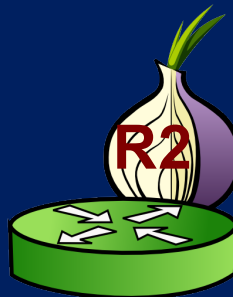
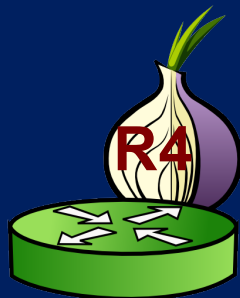
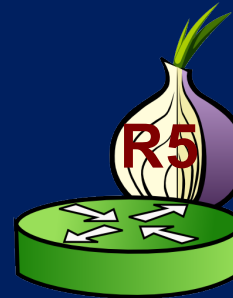
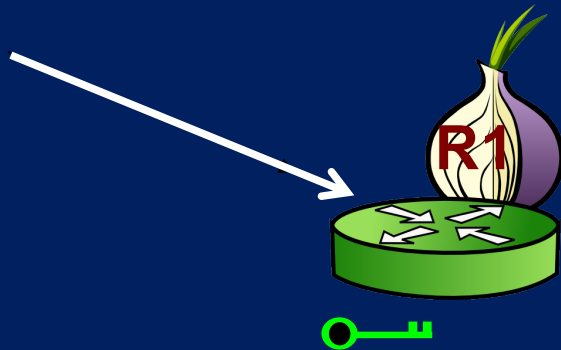


A corrupt last hop can tell someone is talking to Bob, but not who

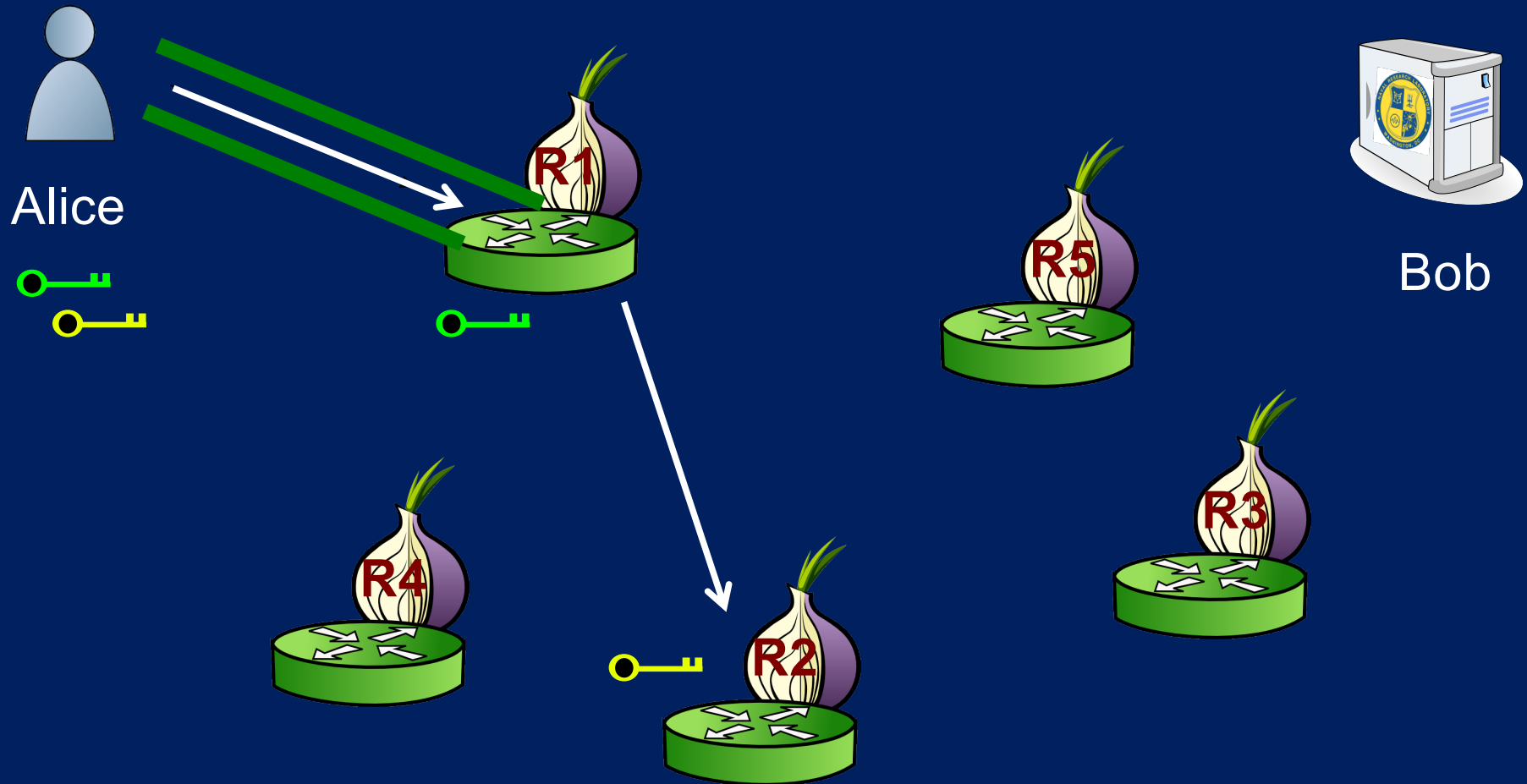


- **“Our motivation here is not to provide anonymous communication, but to separate identification from routing.”**
- “Proxies for anonymous routing”. Reed, Syverson, and Goldschlag. ACSAC 01996

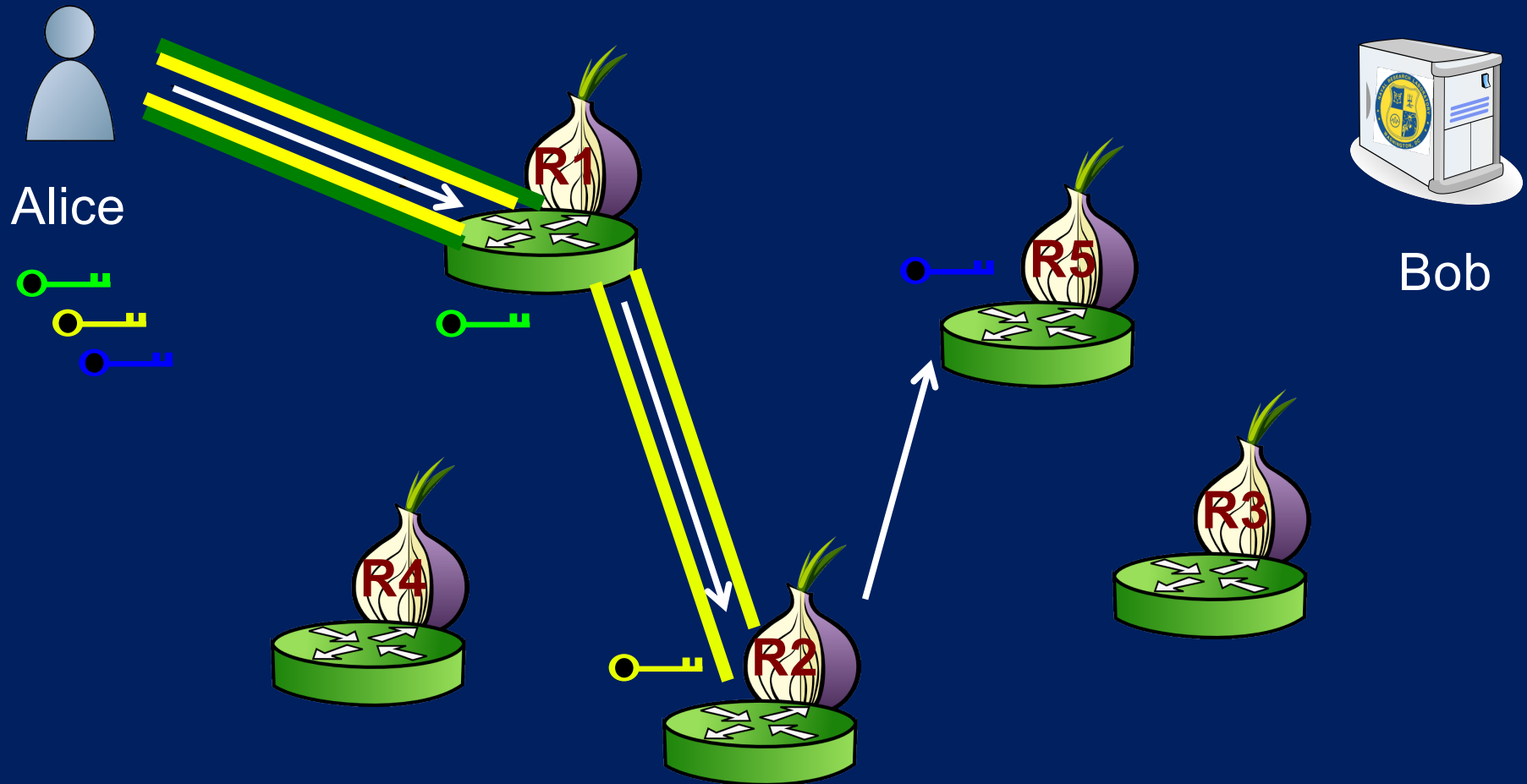
Onion Routing: Circuit construction



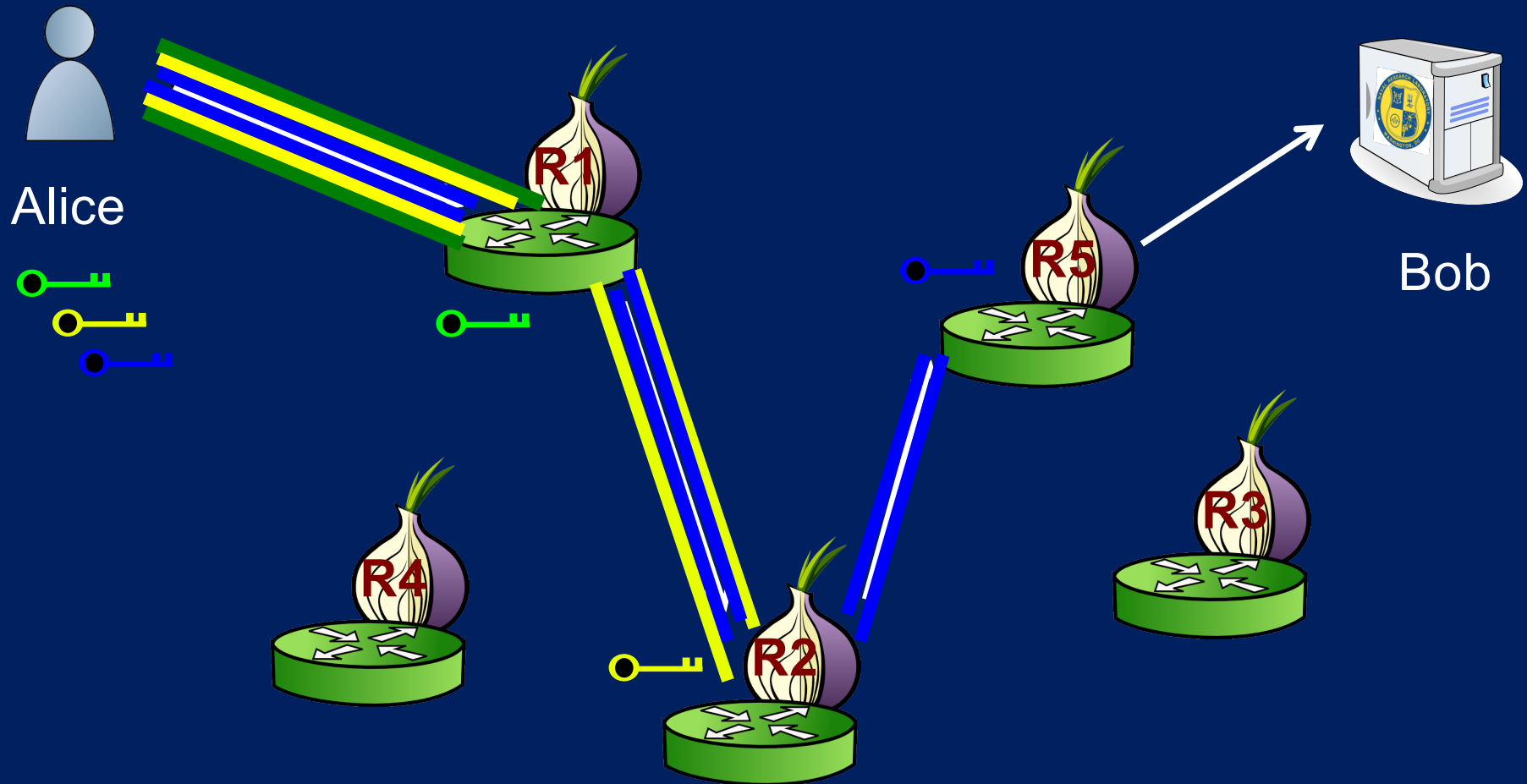
Onion Routing: Circuit construction



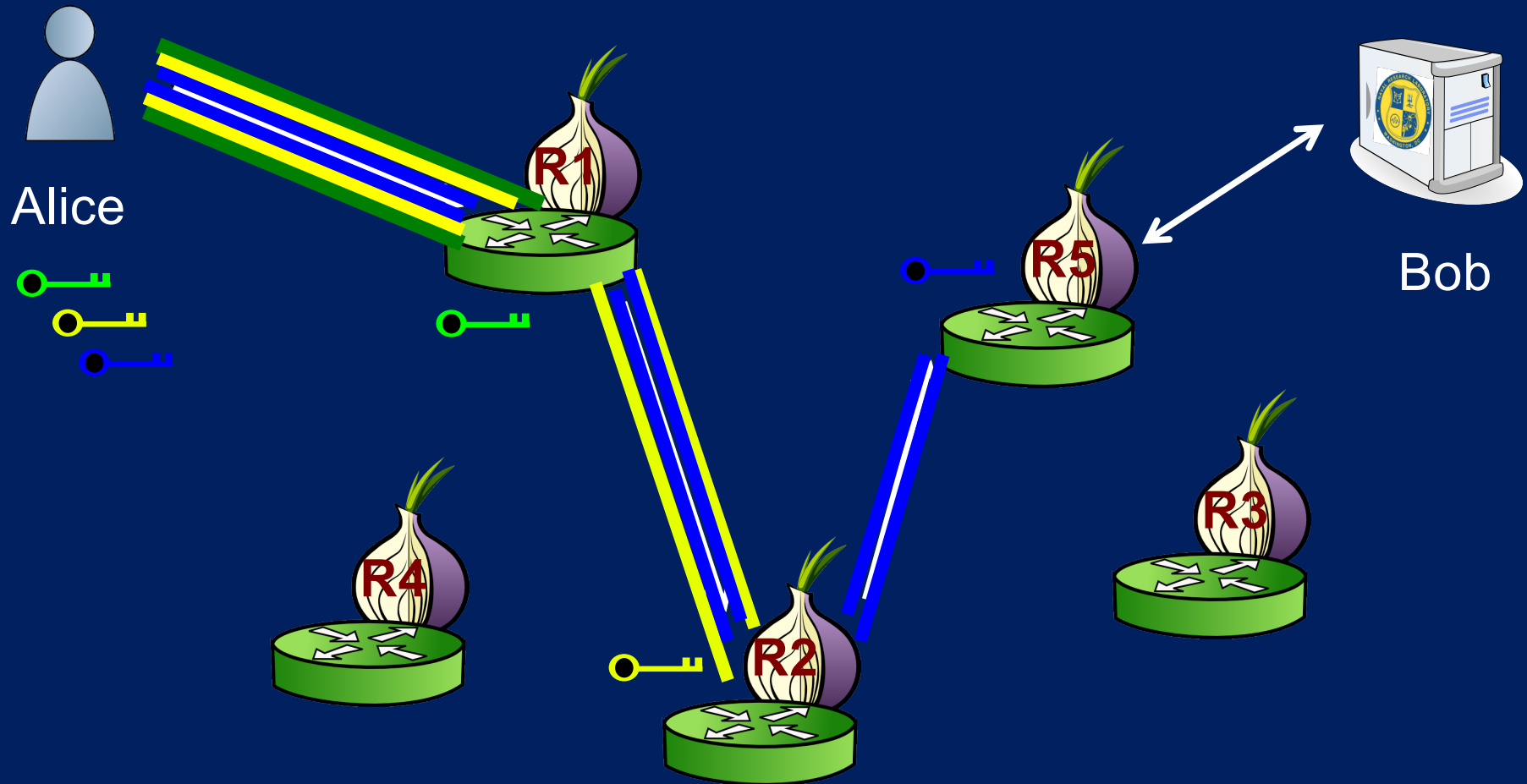
Onion Routing: Circuit construction



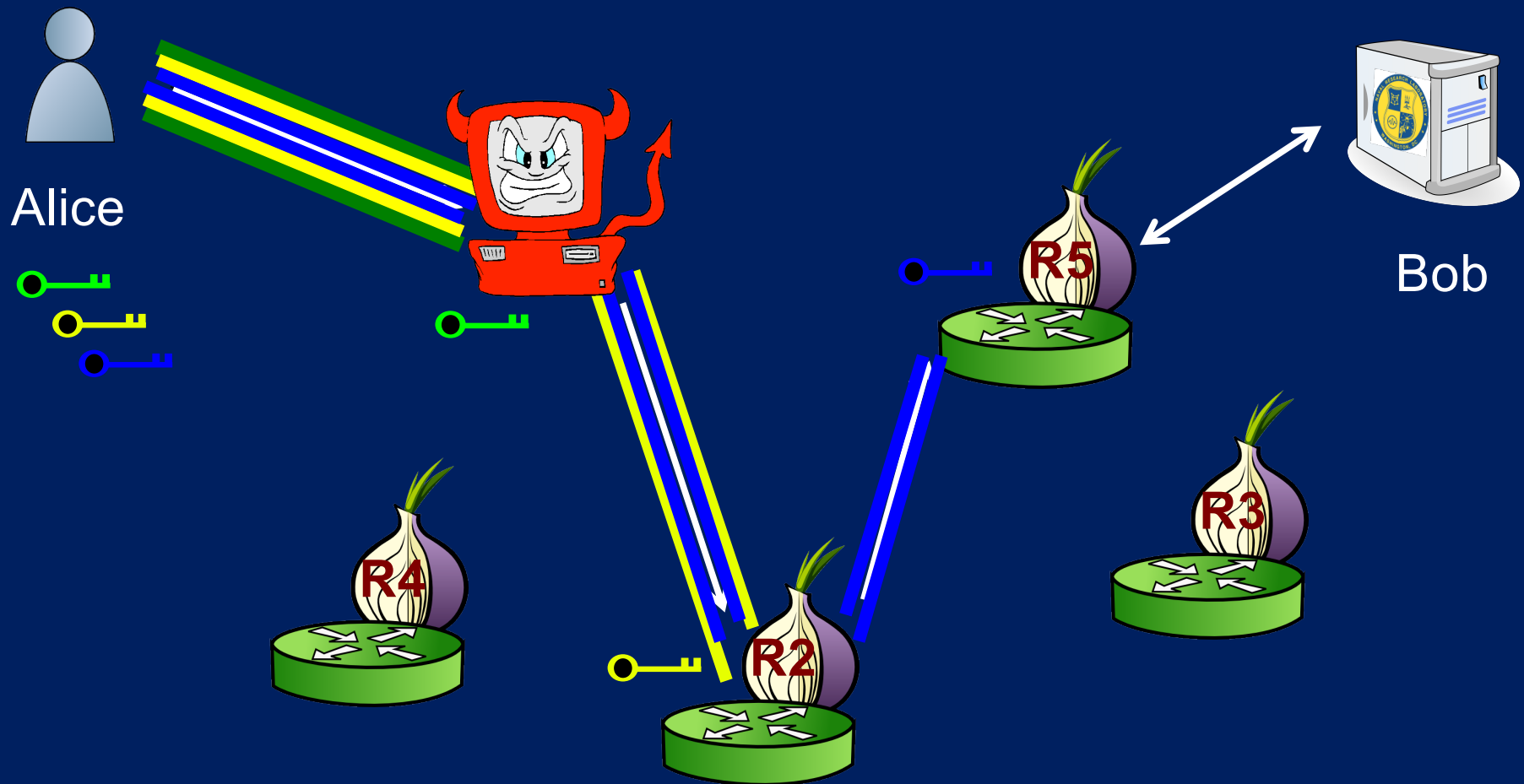
Onion Routing: Connection creation



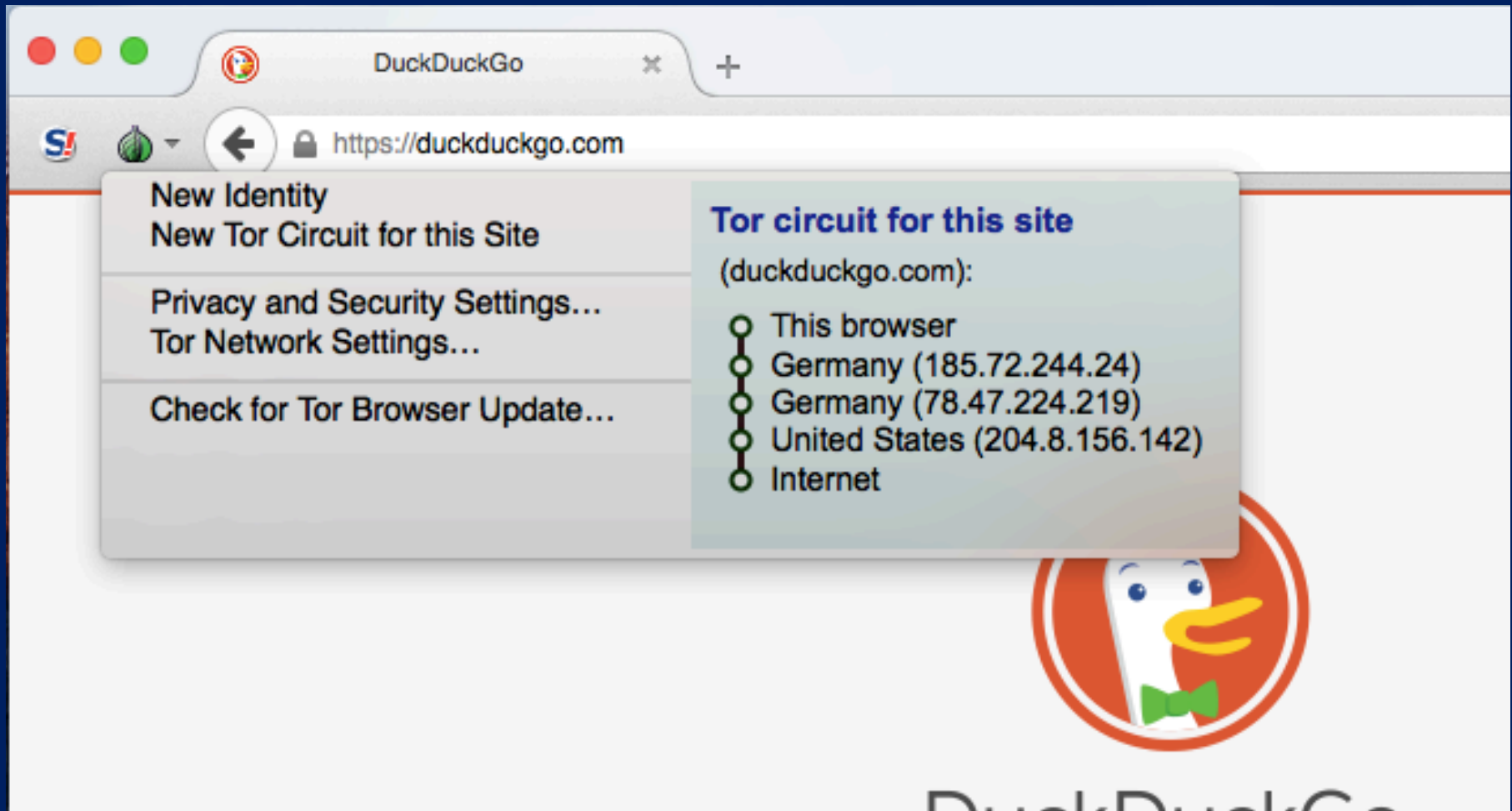
Onion Routing: Data Exchange



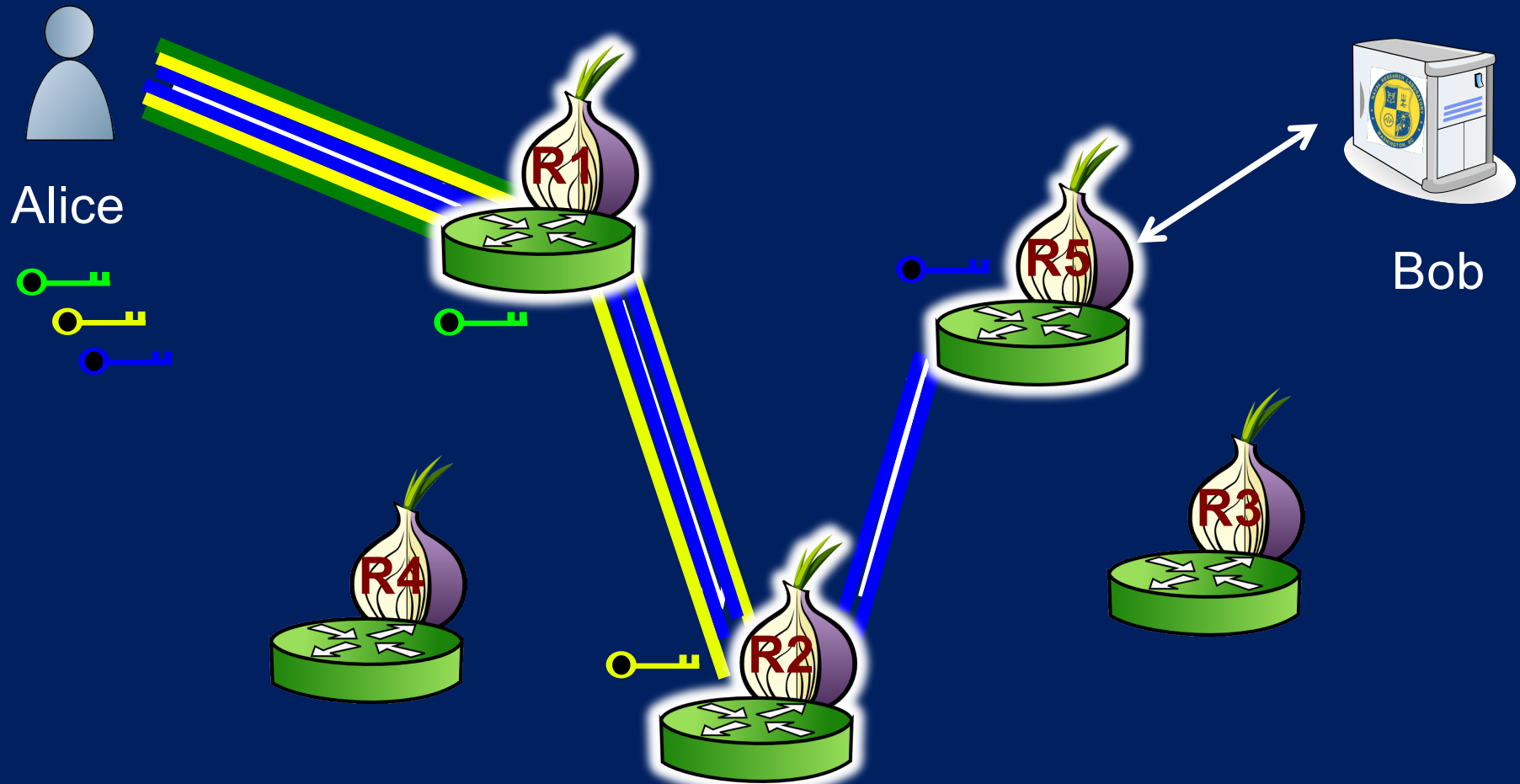
Route authentication: Not only about confidentiality of metadata



The Alluminated Net



Onion routing illuminates connection paths otherwise dark and vulnerable for users

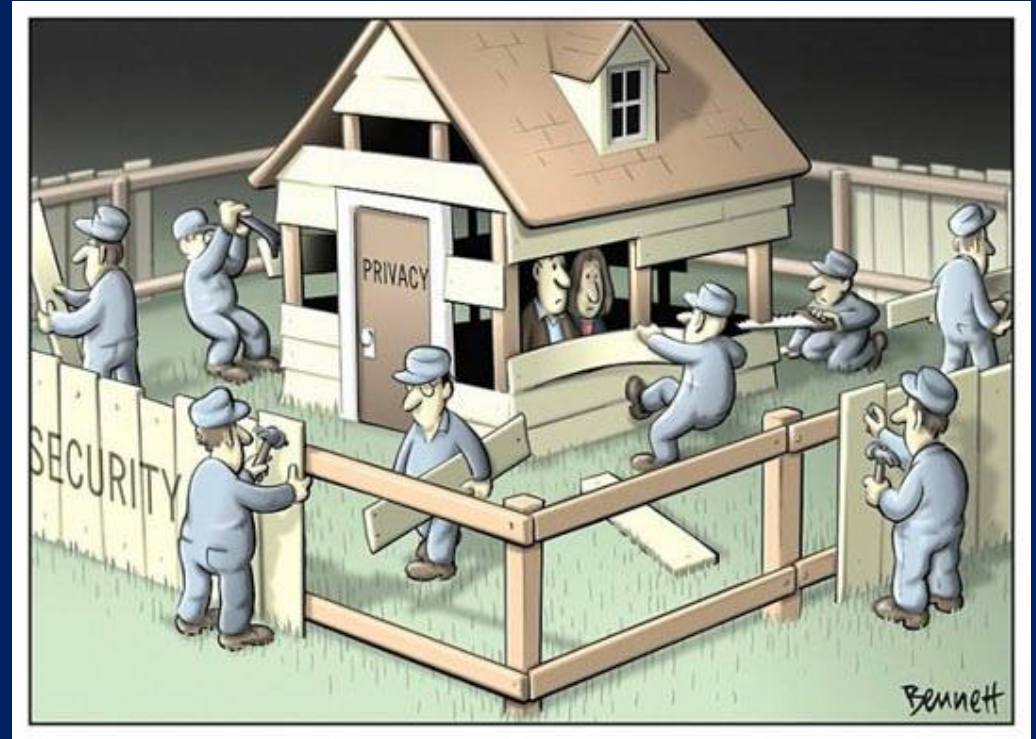


That's onion routing in a nutshell

What is 'Tor'?

- Tor: A (class of) onion routing design created at NRL starting c. 2001-2
- Tor: A U.S. 501(c)3 nonprofit organization formed 2006
- Tor: A client software program that connects your computer to the Tor network
- Tor: A volunteer network comprised of c. 7,000 nodes serving over 200 gigabits/s data for millions of daily users (see metrics.torproject.org)
- Tor: A community of researchers, developers, operators, trainers, advocates
- Any amorphous combination of the above

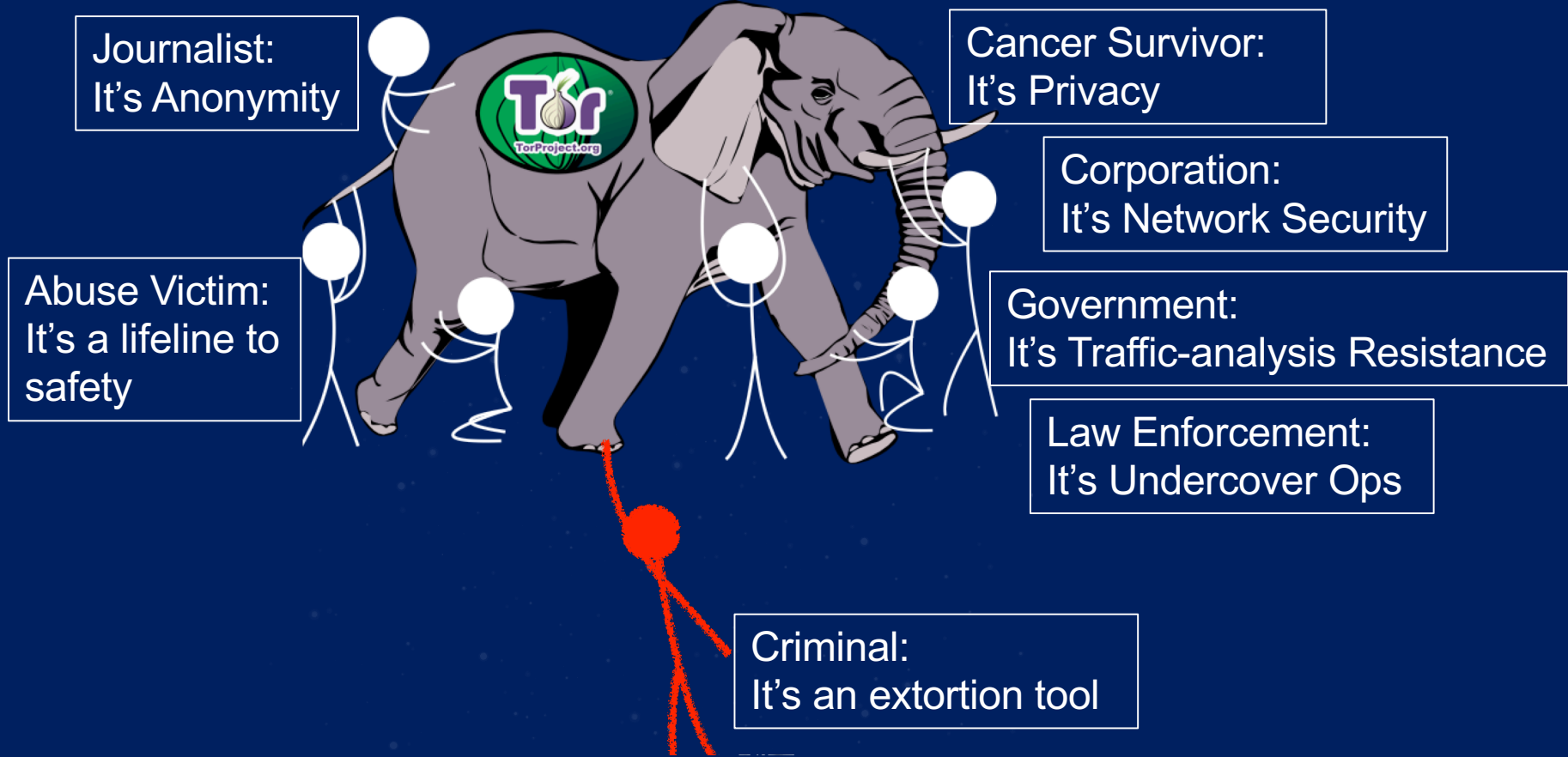
Is Tor a security or privacy technology?



From Clay Bennett's 02002 Pulitzer Prize for Editorial Cartooning portfolio

Protecting Users and Systems Perspective: Security, and Privacy are The Same Thing





Journalist:
It's Anonymity

Cancer Survivor:
It's Privacy

Corporation:
It's Network Security

Abuse Victim:
It's a lifeline to
safety

Government:
It's Traffic-analysis Resistance

Law Enforcement:
It's Undercover Ops

Trojans, Viruses,
Exploits

Criminal:
It's an extortion tool

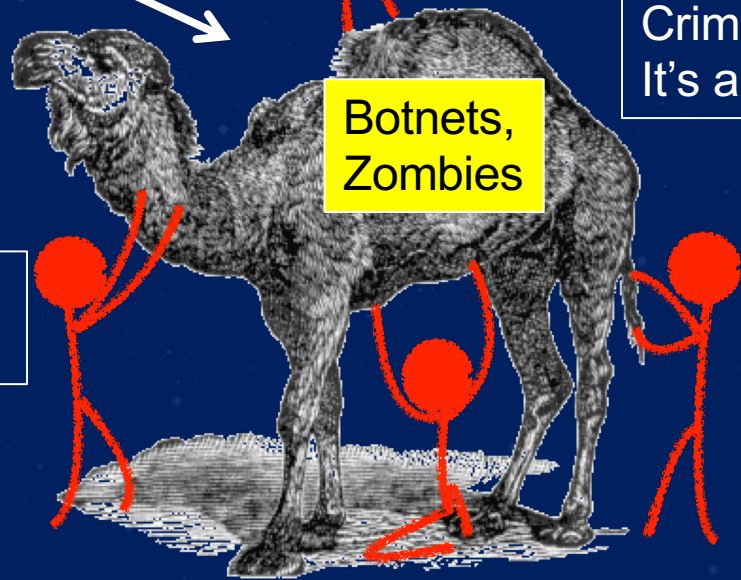
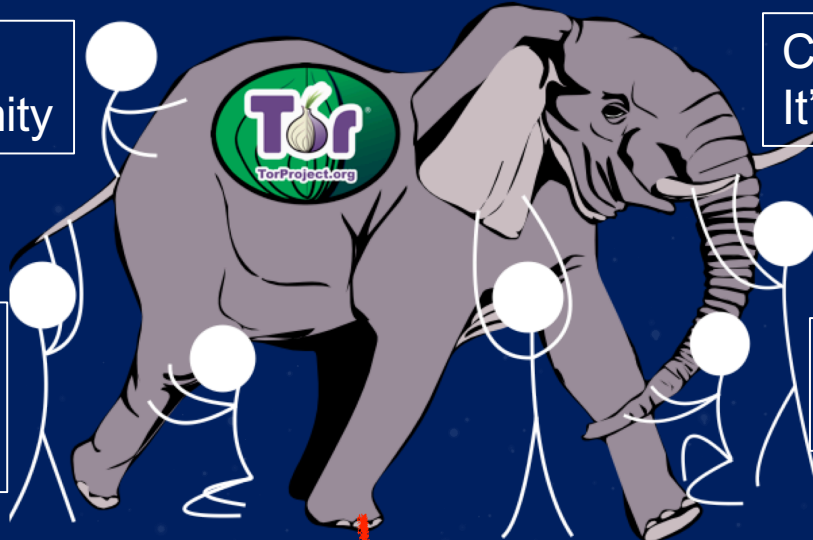
Criminal:
It's a DDoS engine

Criminal:
It's a phishing tool

Criminal:
It's a Spam tool

Botnets,
Zombies

Criminal:
It's an espionage tool



Journalist:
Can't get story



Cancer Survivor:
I feel powerless

Abuse Victim:
Help!



Corporation:
What?

Government:
We're exposed

Law Enforcement:
Your cover is blown

Trojans, Viruses,
Exploits

Criminal:
It's an extortion tool

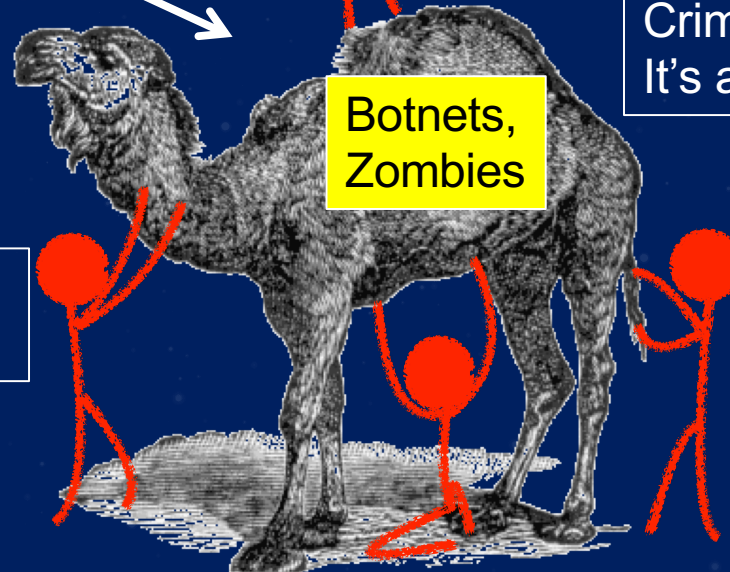
Criminal:
It's a DDoS engine

Criminal:
It's a phishing tool

Criminal:
It's a Spam tool

Botnets,
Zombies

Criminal:
It's an espionage tool

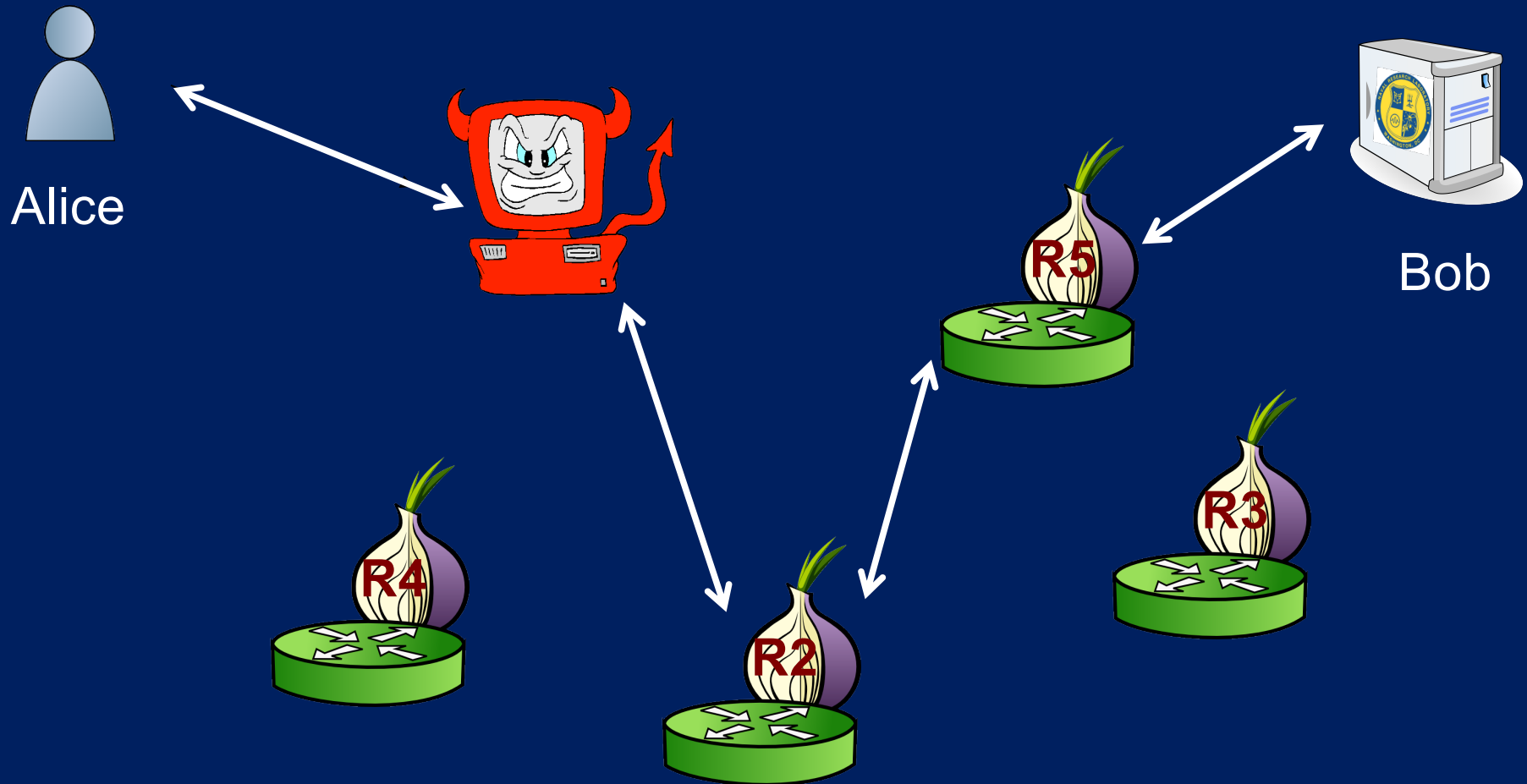


Protecting Users and Systems Perspective: Security, and Privacy are The Same Thing

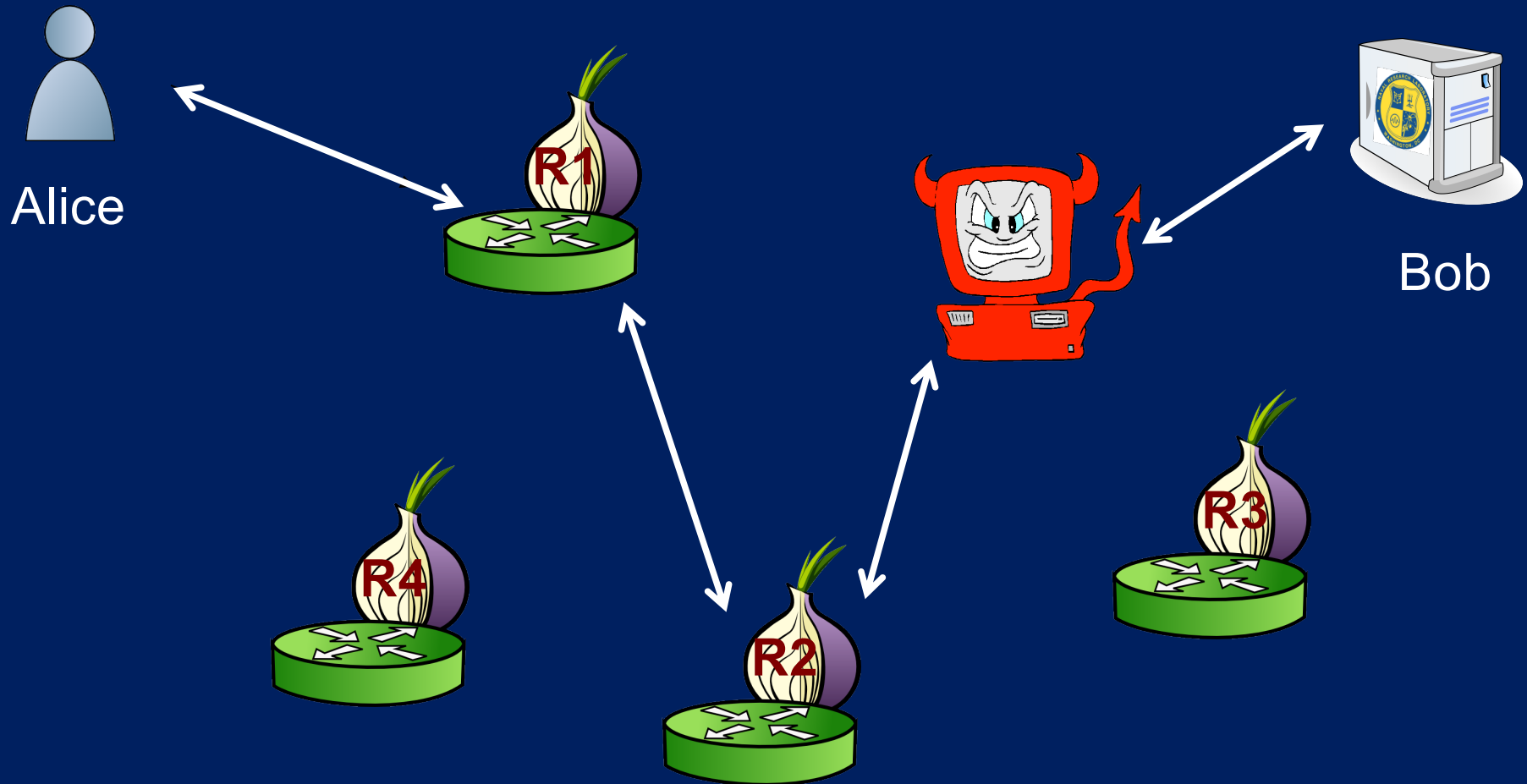


- Part 1: Onion Routing and Tor
 - Background, Motivation, Basic Concepts, Basic Design
- Part 2: How Secure Is It?
 - Network and Adversary Models, Metrics
- Part 3: Onion Services
 - Background, Motivation, Basic Concepts, Basic Design
- Part 4: Self-Authenticating Traditional Addresses (SATAs)
 - Background, Motivation, Basic Concepts, Basic Design

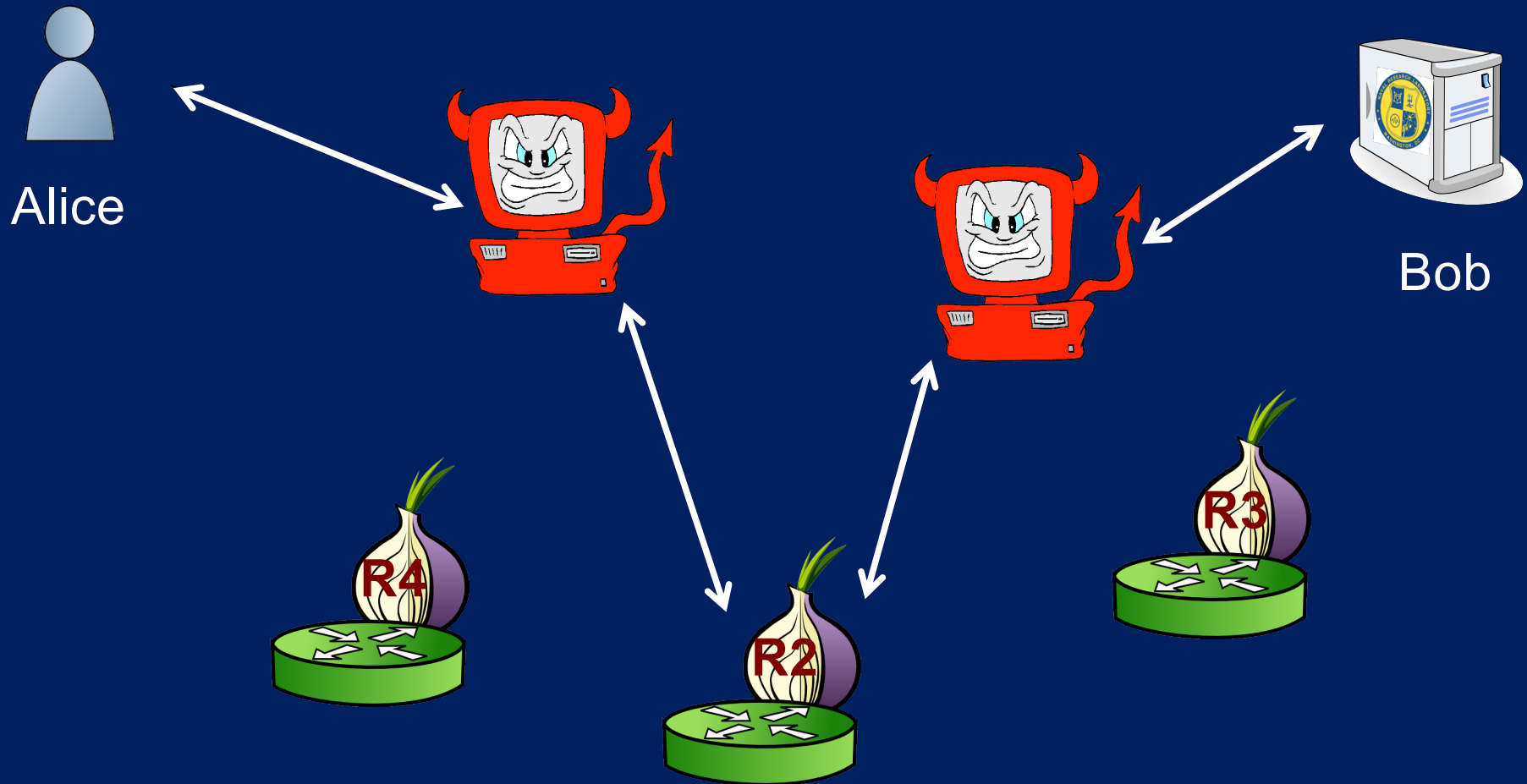
A corrupt first hop can tell that Alice is talking, but not to whom



A corrupt last hop can tell someone is talking to Bob, but not who

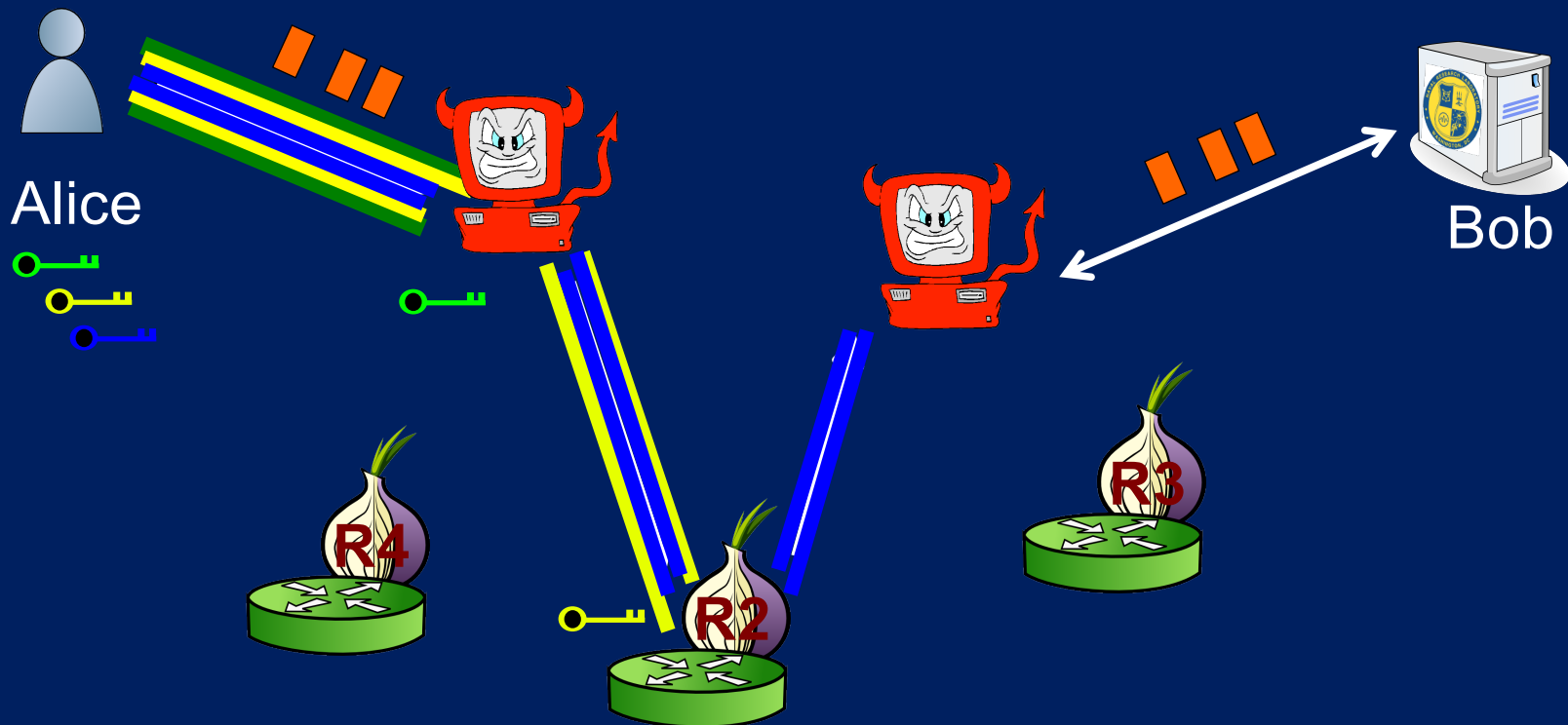


What if the adversary is on both ends?



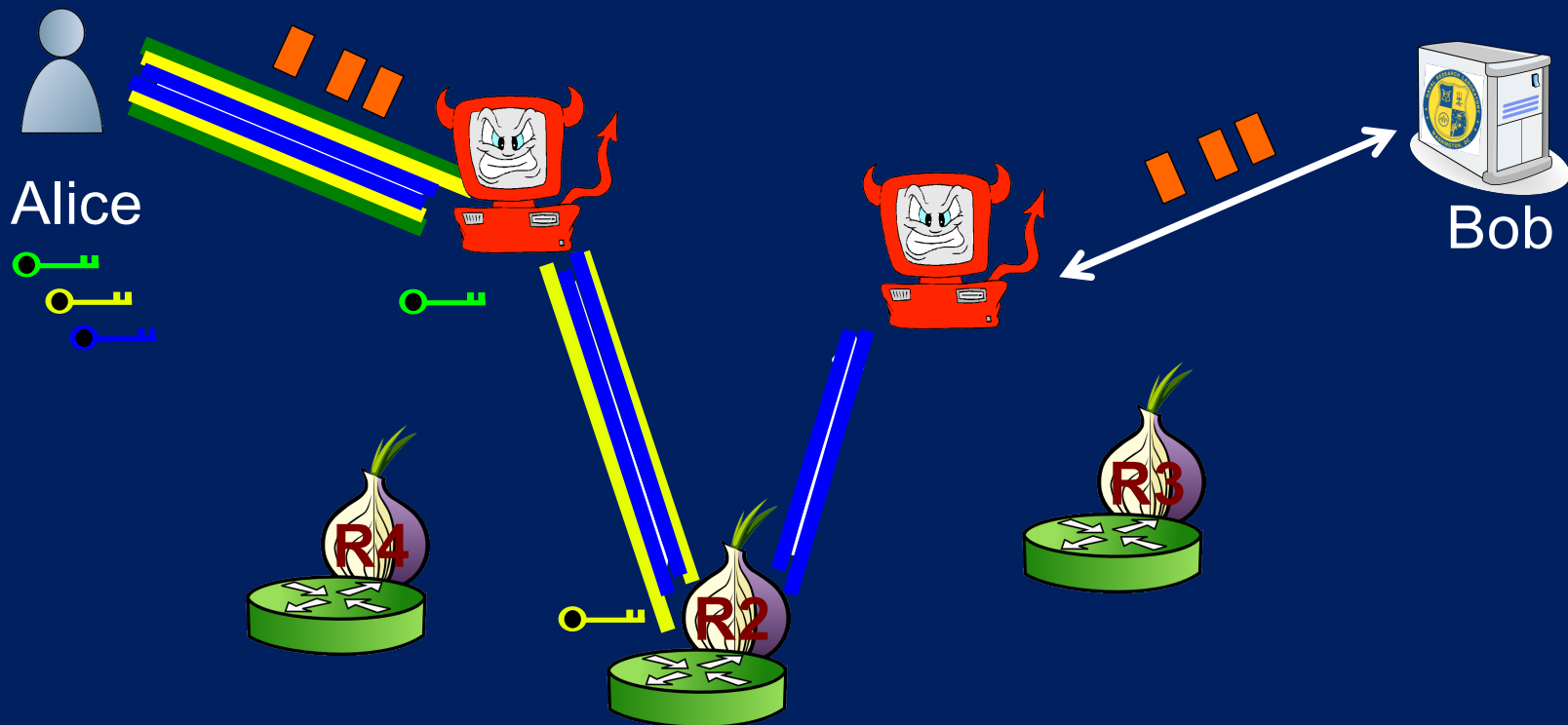
Basic adversary model: Observing traffic entering & leaving network breaks onion routing

- “Towards an Analysis of Onion Routing Security” Syverson et al. PETS 02000
- Presented and analyzed adversary model assumed in prior onion routing work
 - Network of n onion routers, c compromised onion routers
 - Security approx. c^2 / n^2



Basic adversary model: Observing traffic entering & leaving network breaks Tor

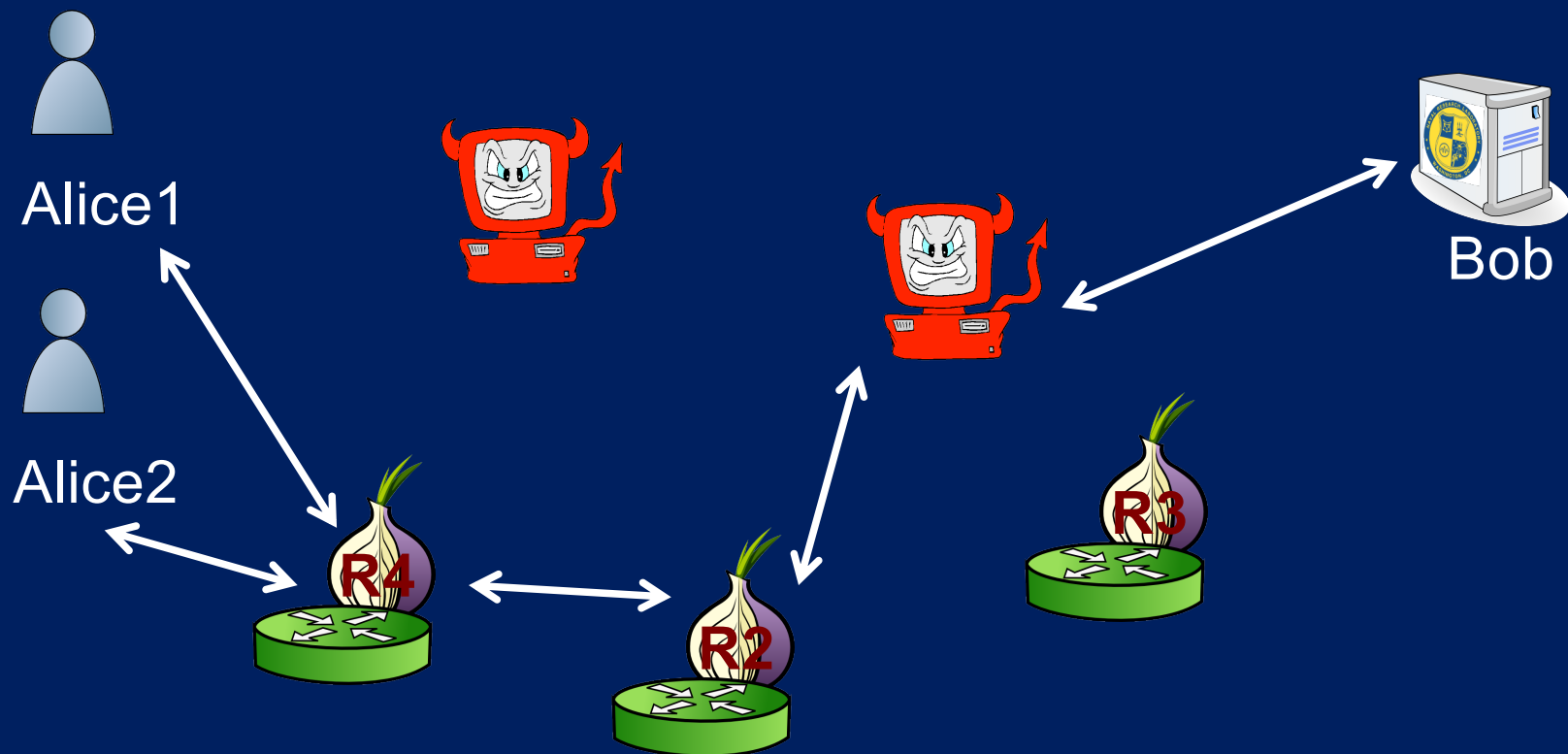
- It's a more complicated c^2 / n^2 for Tor
 - Relay selection is weighted by node capacity
 - Only some relays can exit the network
 - roughly 1/6 of relays have exit flag (1/4 volume) 1/2 have entry guard flag
- We ignore network discovery/route selection for simplicity



Observing traffic entering & leaving network breaks onion routing

How do we define security?

- Possibilistic: Somebody else might have sent a message.



Observing traffic entering & leaving network breaks onion routing

How do we define security?

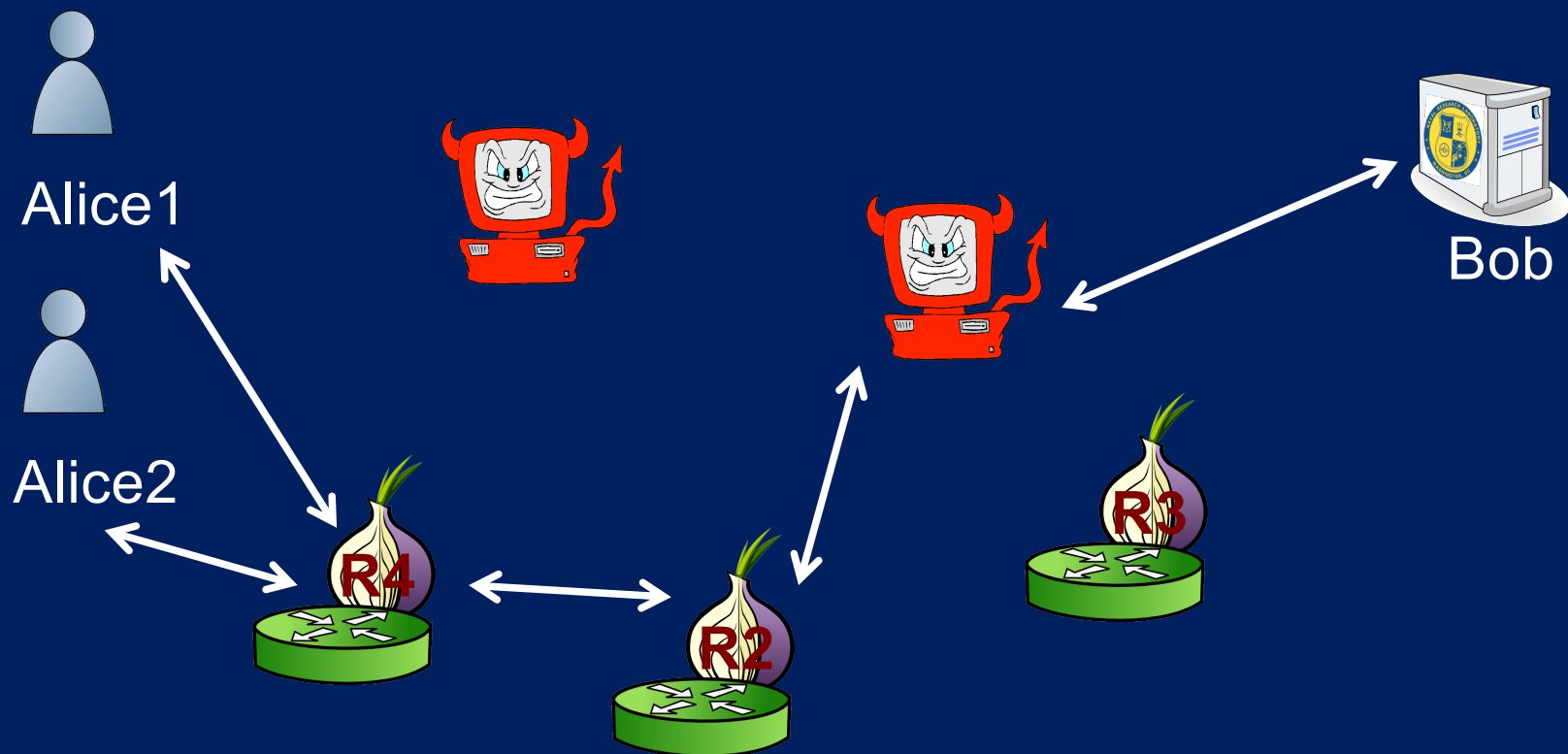
- Possibilistic: Somebody else might have sent a message.
- Probabilistic: Probability that Alice1 is sender.



Observing traffic entering & leaving network breaks onion routing

How do we define security?

- Possibilistic: Somebody else might have sent a message.
- Probabilistic: Probability that Alice1 is sender.



How do we define security in a world lousy with cryptologists?

How do those relate to standard cryptographic definitions?

- Possibilistic: Somebody else might have sent a message?
- Probabilistic: What probability that Alice is sender?

How do we define security in a world lousy with cryptologists?

How do those relate to standard cryptographic definitions?

- Onion Routing Ideal Functionality in Universally Composable Framework
- *“Probabilistic Analysis of Onion Routing in a Black-box Model”* Feigenbaum, Johnson and Syverson ACM TISSEC 02012

Upon receiving destination d from user U

$$x \leftarrow \begin{cases} u & \text{with probability } b \\ \emptyset & \text{with probability } 1-b \end{cases}$$

$$y \leftarrow \begin{cases} d & \text{with probability } b \\ \emptyset & \text{with probability } 1-b \end{cases}$$

Send (x,y) to the adversary.

\mathcal{F}_{OR}

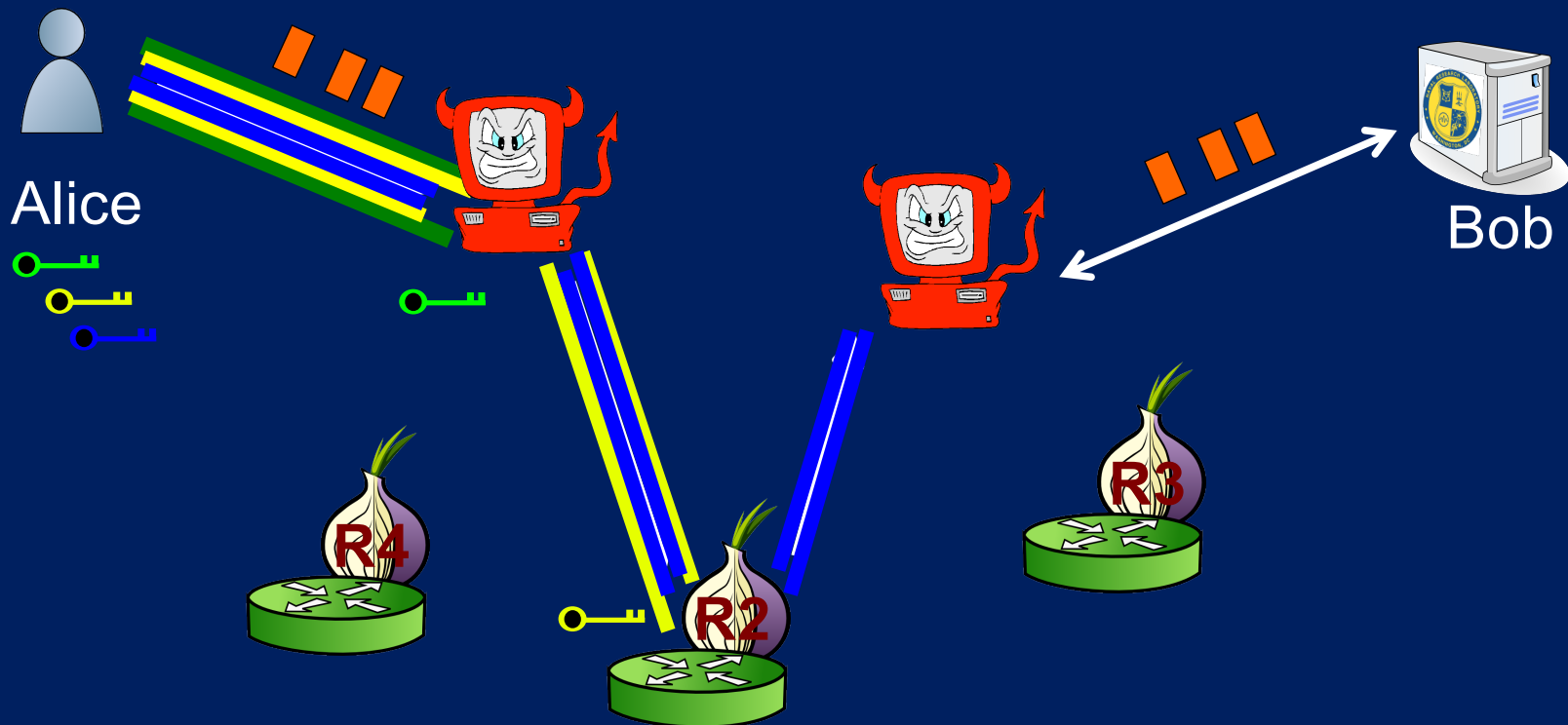
How do we define security in a world lousy with cryptologists?

Ideal Functionality modeling more of reality

- “Provably Secure and Practical Onion Routing” Backes, Goldberg, Kate, and Mohammadi, IEEE CSF 02012
- Functionality can actually send messages
- Also gave ideal functionality covering key exchange, circuit building
 - Needs wrapper to hide irrelevant circuit-building options
- Shown to UC-emulate \mathcal{F}_{OR}
- Further developments in AnoA Framework of Backes et al. and following

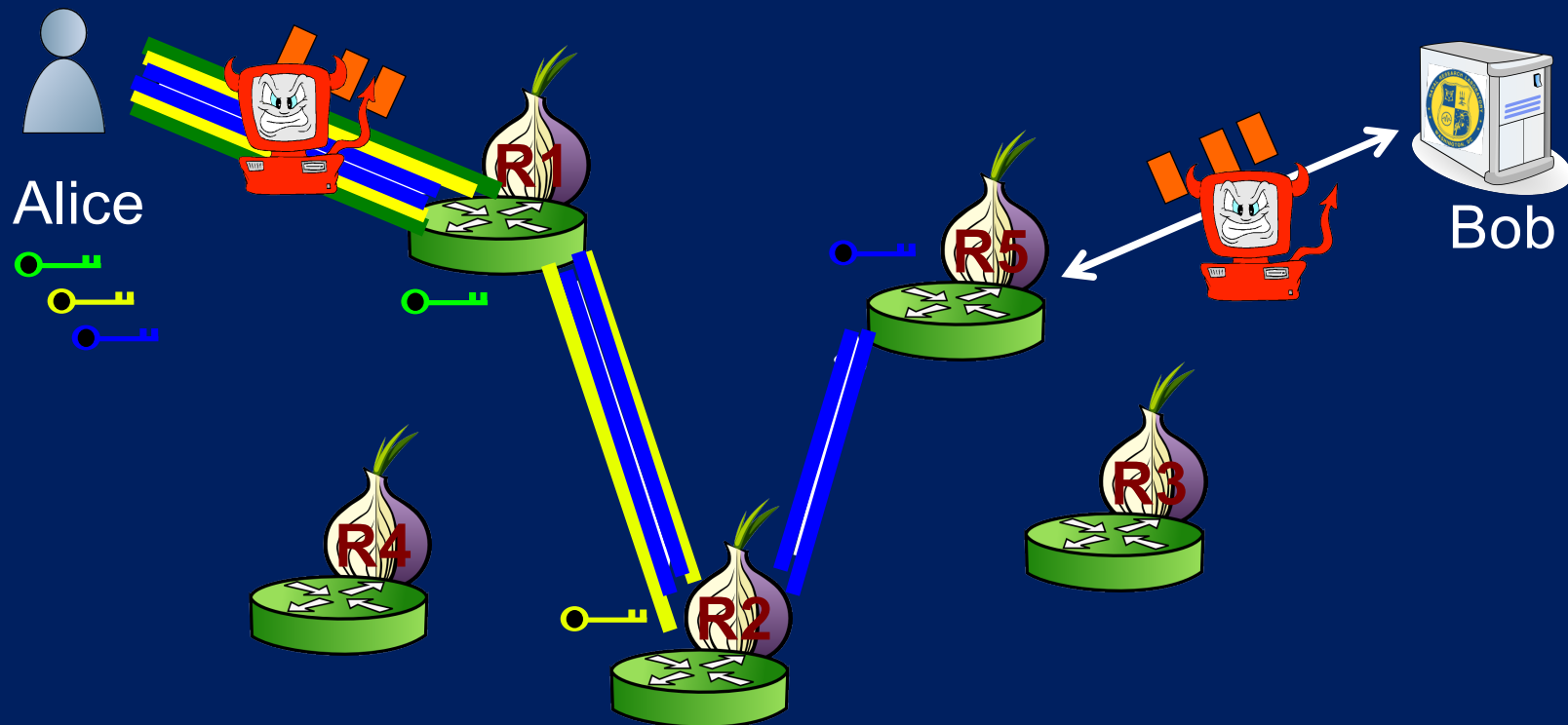
Basic adversary model: Observing traffic entering & leaving network breaks onion routing

Are we missing anything in the models developed so far?

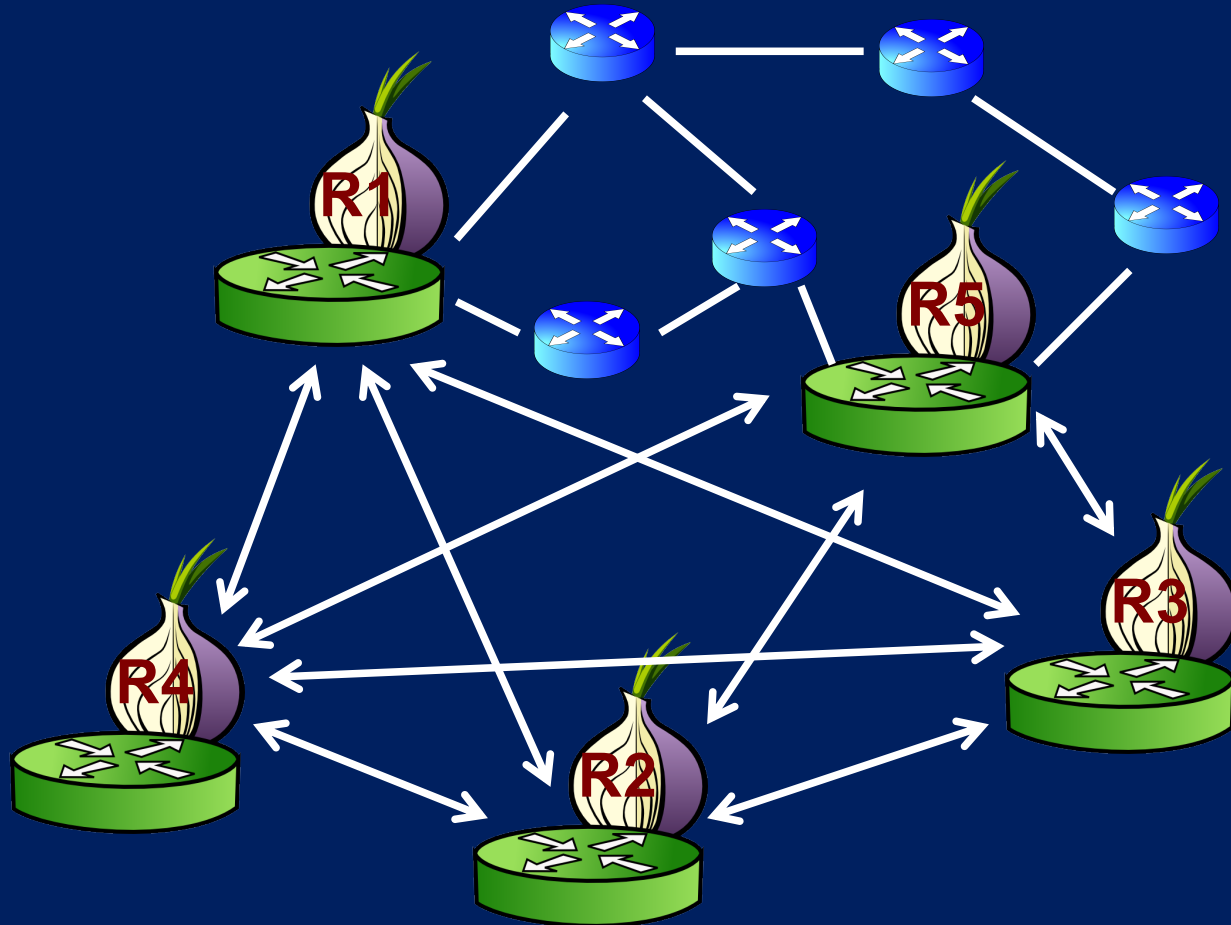


Basic adversary model: Observing traffic entering & leaving network breaks onion routing

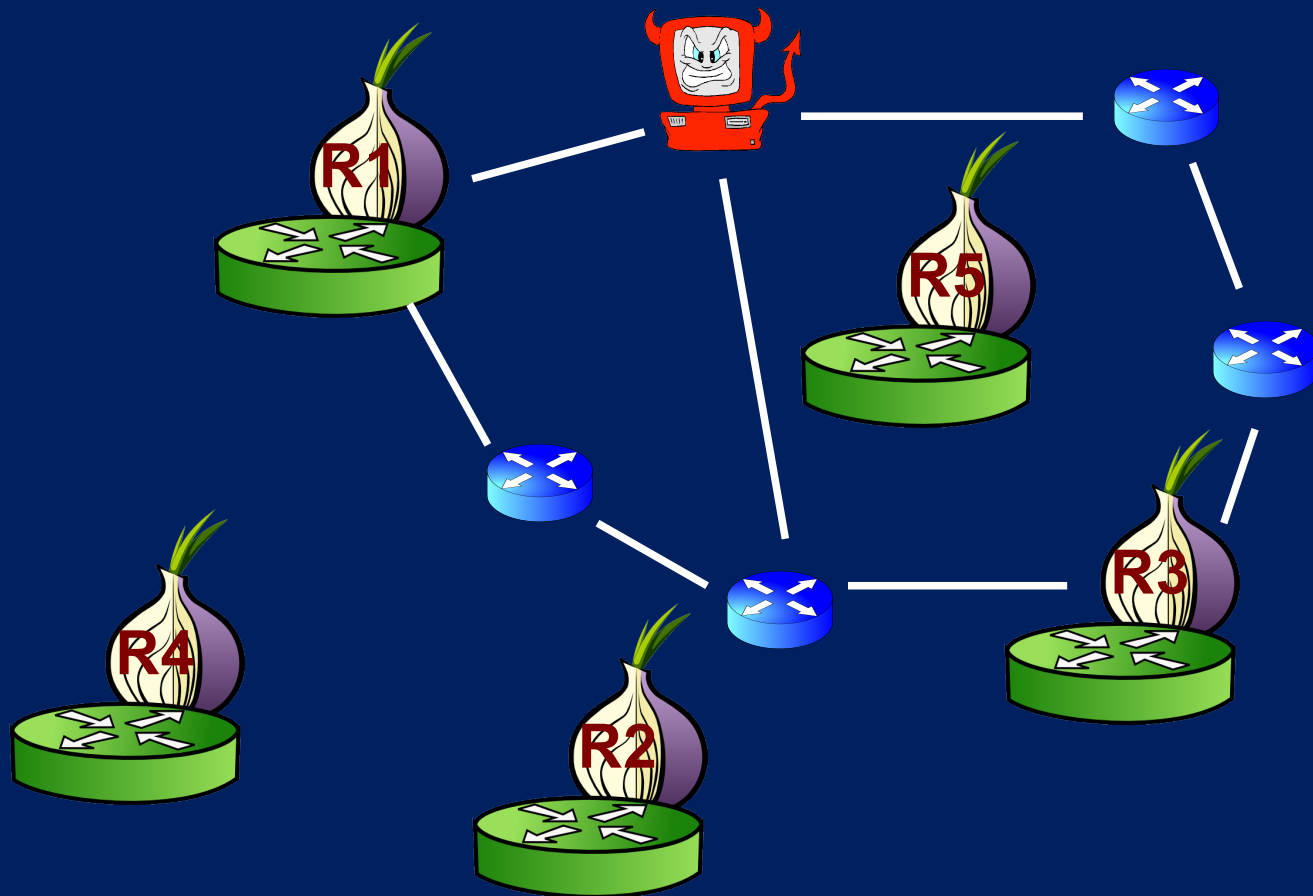
- “Location diversity in anonymity networks” Feamster-Dingledine. WPES 02004
- Adversaries live on network links as well as onion routers



Onion Routers (Tor Relays) overlay underlying Internet

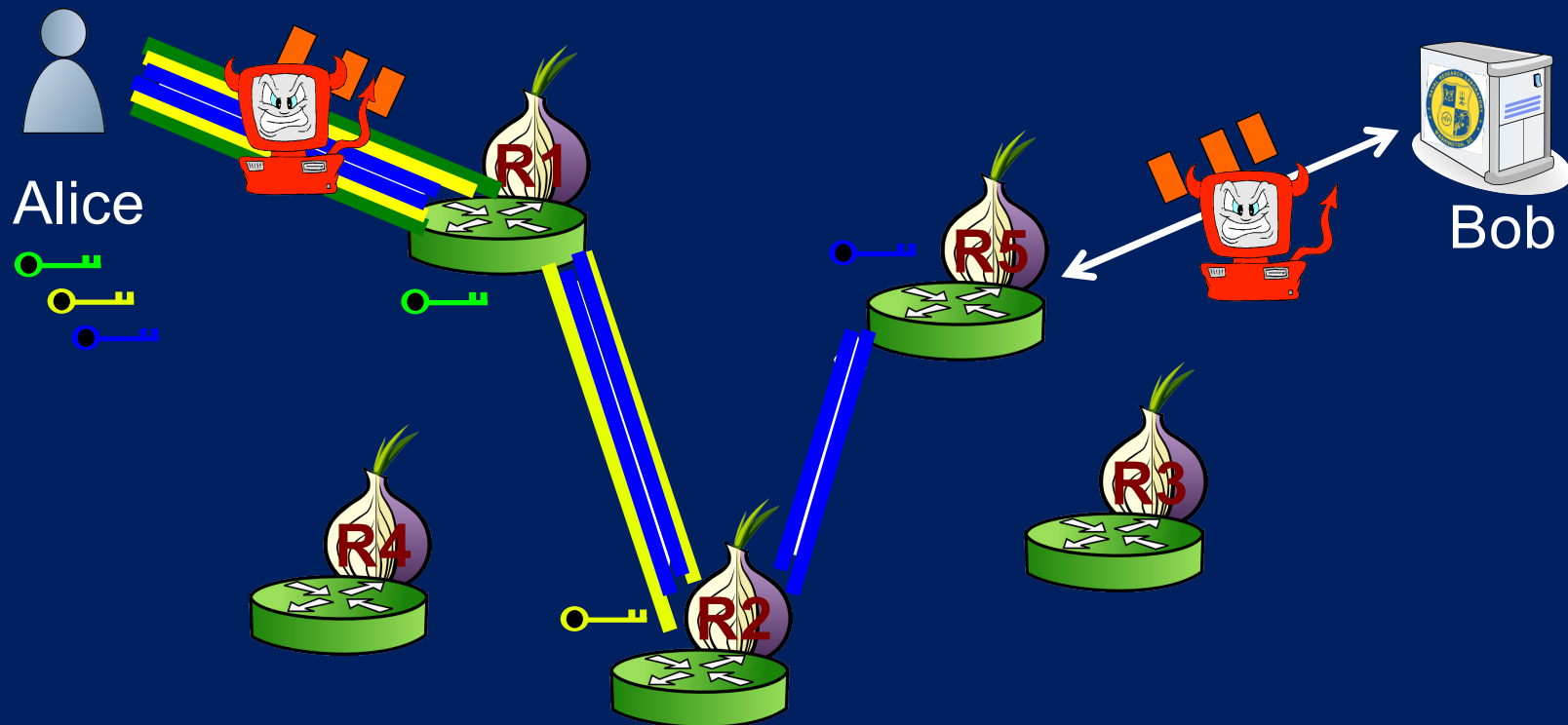


Adversaries can live on network links to/from onion routers too



Basic adversary model: Observing traffic entering & leaving network breaks onion routing

- “Location diversity in anonymity networks” Feamster-Dingledine. WPES 02004
- Adversaries live on network links as well as onion routers
- Metric: Path Independence – Does any single AS lie on both path between Alice & R1 and path between Bob & R5



Adversary Framework

Resource Types

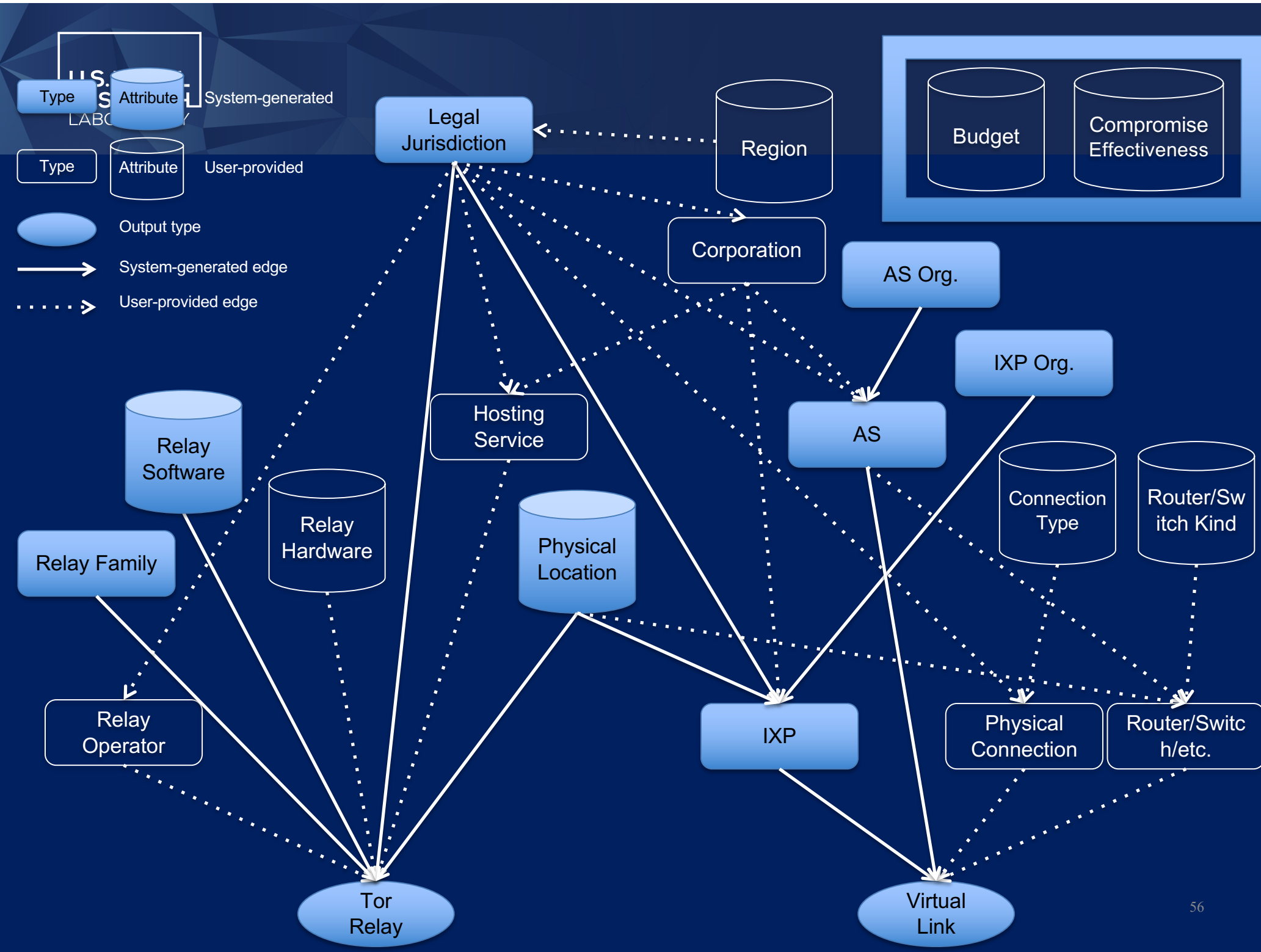
- Relays
- Bandwidth
- Autonomous Systems (ASes)
- Int. Exchange Points (IXPs)
- Undersea Cables
- Money
- MLATs

Resource Endowment

- Destination host
- 5% Tor bandwidth
- Source AS
- Equinix IXPs

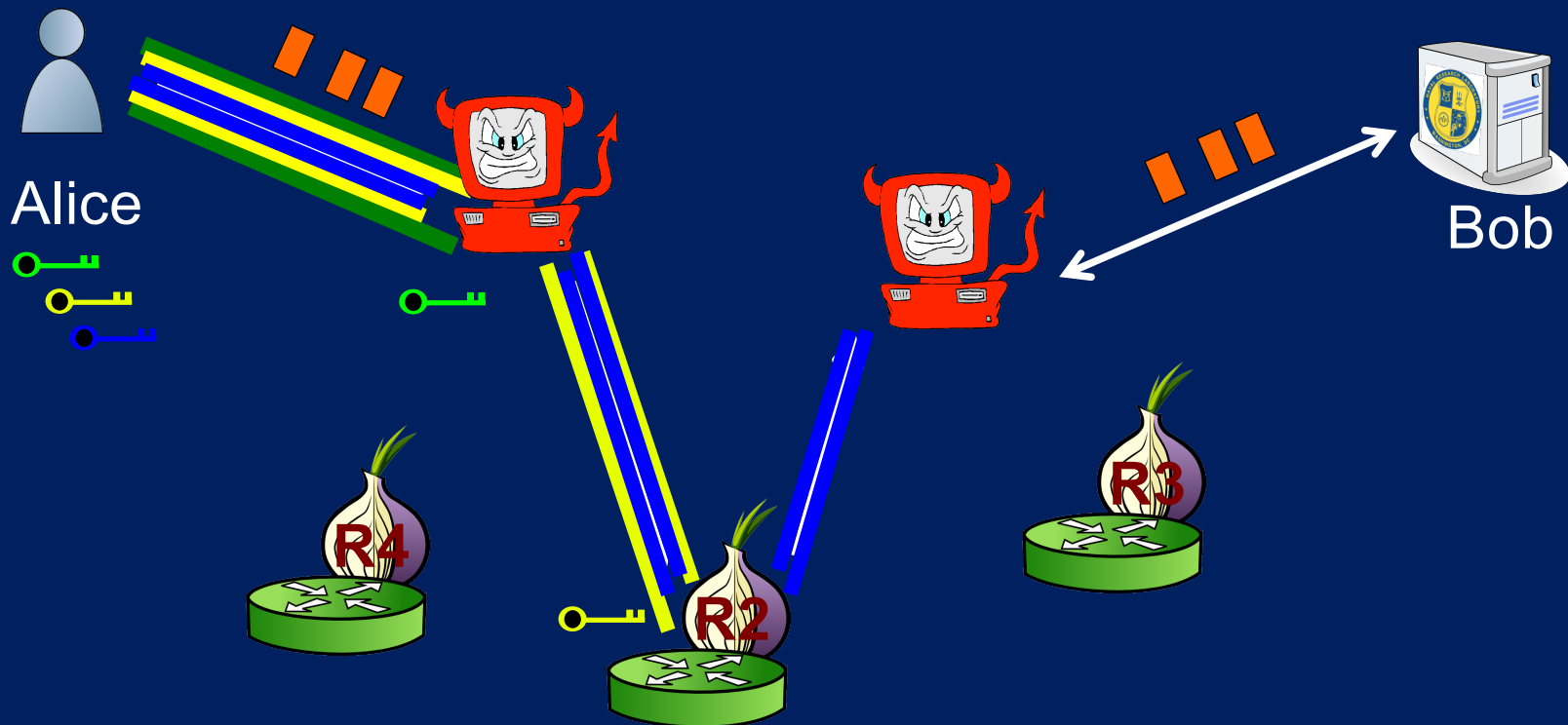
Goal

- Target a given user's comms
- Compromise as much traffic as possible
- Learn who uses Tor
- Learn what Tor is used for



Basic adversary model: Observing traffic entering & leaving network breaks onion routing

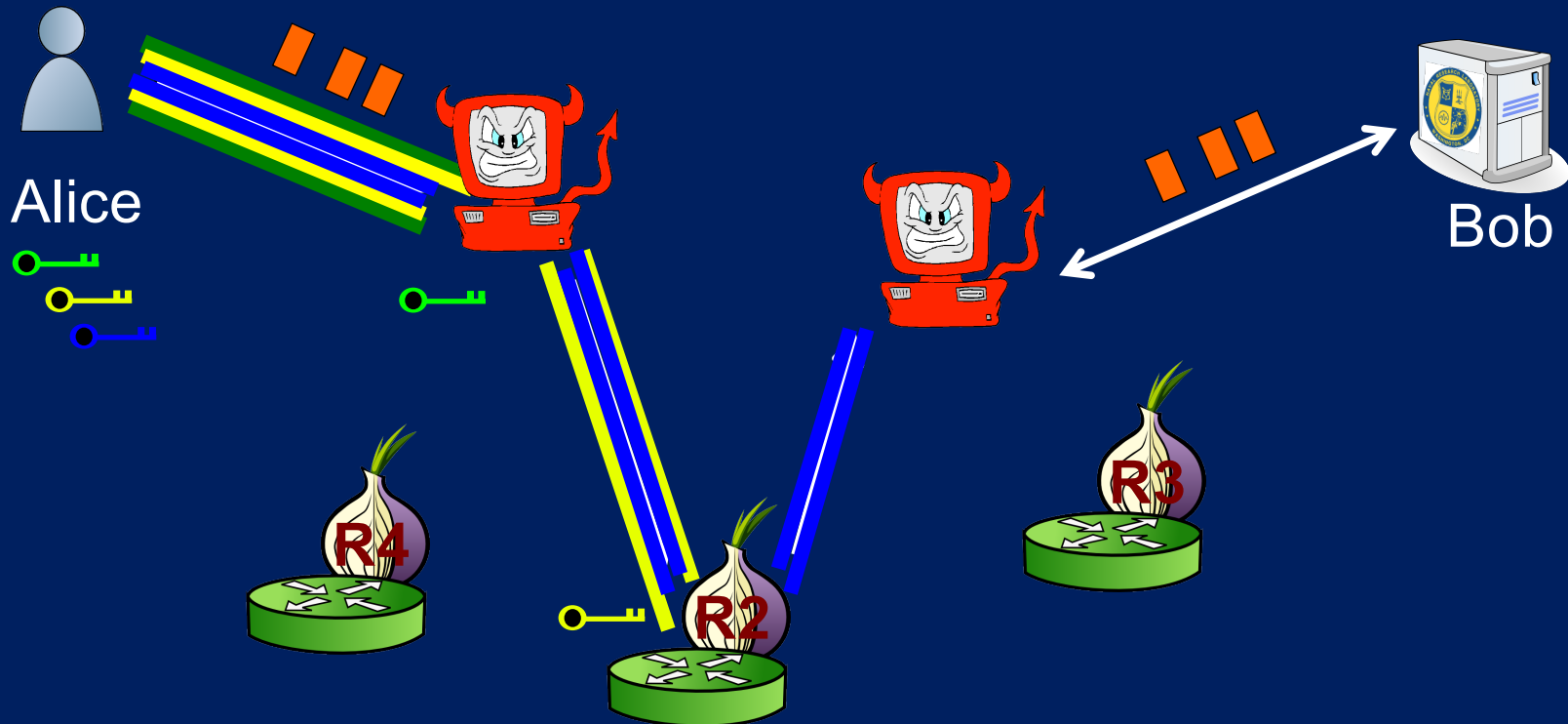
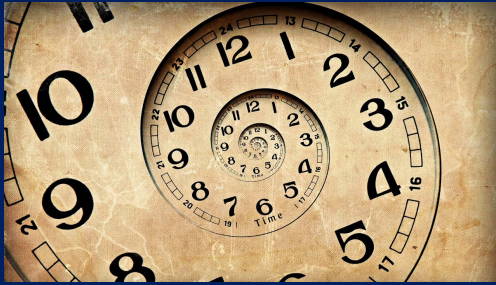
Are we still missing anything?



Basic adversary model: Observing traffic entering & leaving network breaks onion routing

Are we still missing anything?

- Time



Basic adversary model: Observing traffic entering & leaving network breaks onion routing

Are we still missing anything?

- Time



- Above definitions and metrics
 - Give results for all traffic on network:
 - average anonymity, worst anonymity
 - Are based on a snapshot
 - all messages/connections in system at a single time

Basic adversary model: Observing traffic entering & leaving network breaks onion routing

Are we still missing anything?

- Time



- Above definitions and metrics

- Give results for all traffic on network:
 - average anonymity, worst anonymity
- Are based on a snapshot
 - all messages/connections in system at a time

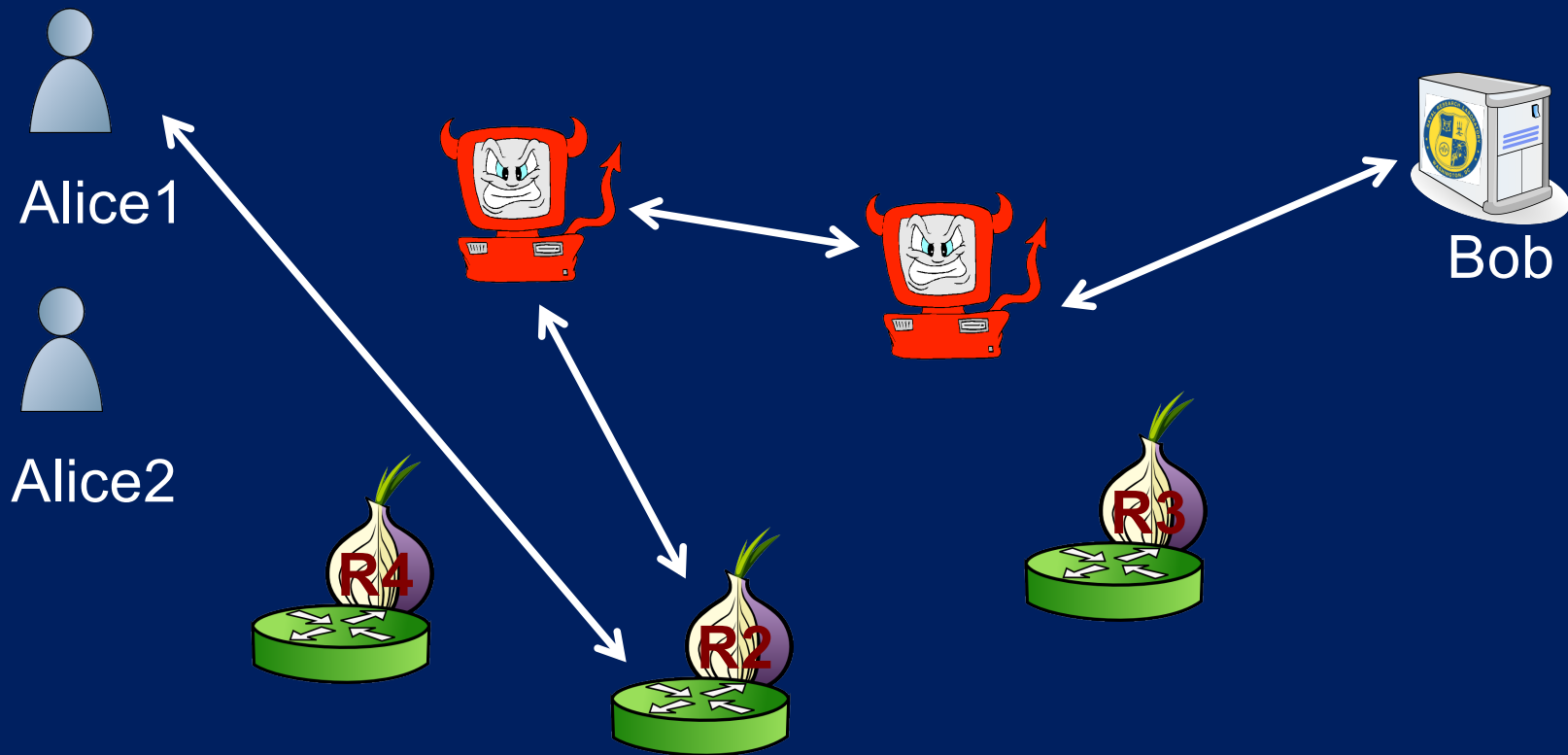
- What users actually need to know

- I'm going to use system S in context C in this way for that long
- How safe/screwed am I?

Basic adversary model: Observing traffic entering & leaving network breaks onion routing

Are we still missing anything?

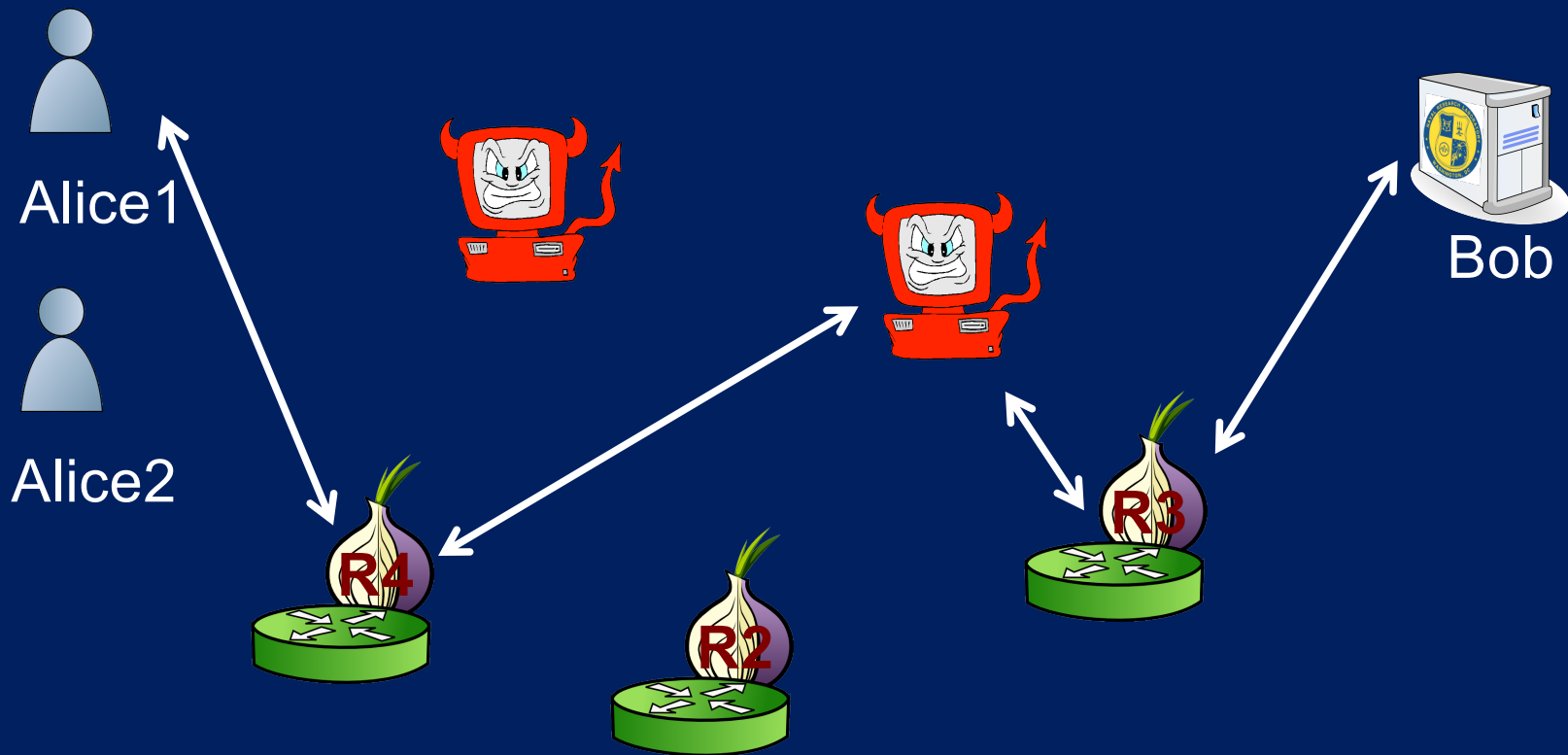
- Time



Basic adversary model: Observing traffic entering & leaving network breaks onion routing

Are we still missing anything?

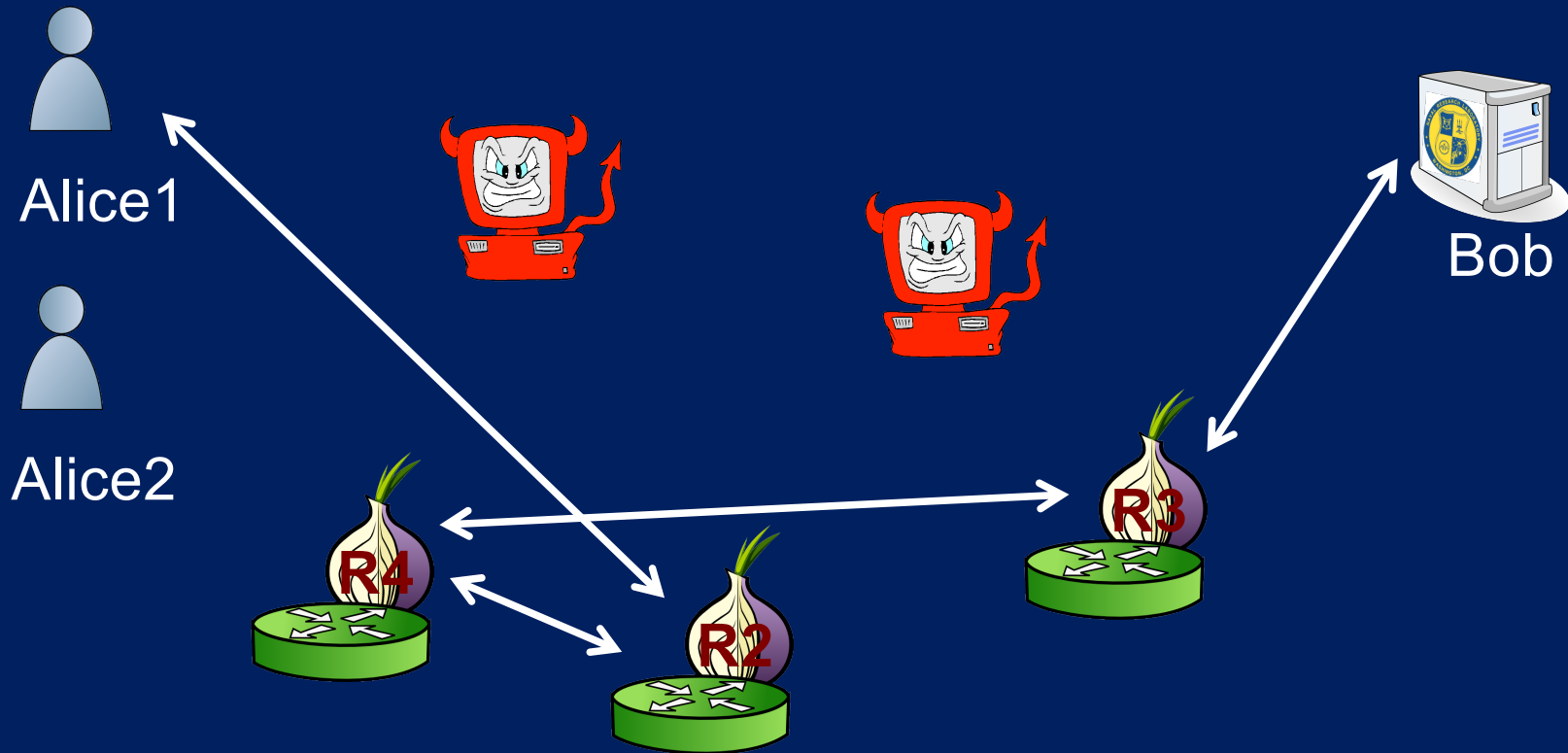
- Time



Basic adversary model: Observing traffic entering & leaving network breaks onion routing

Are we still missing anything?

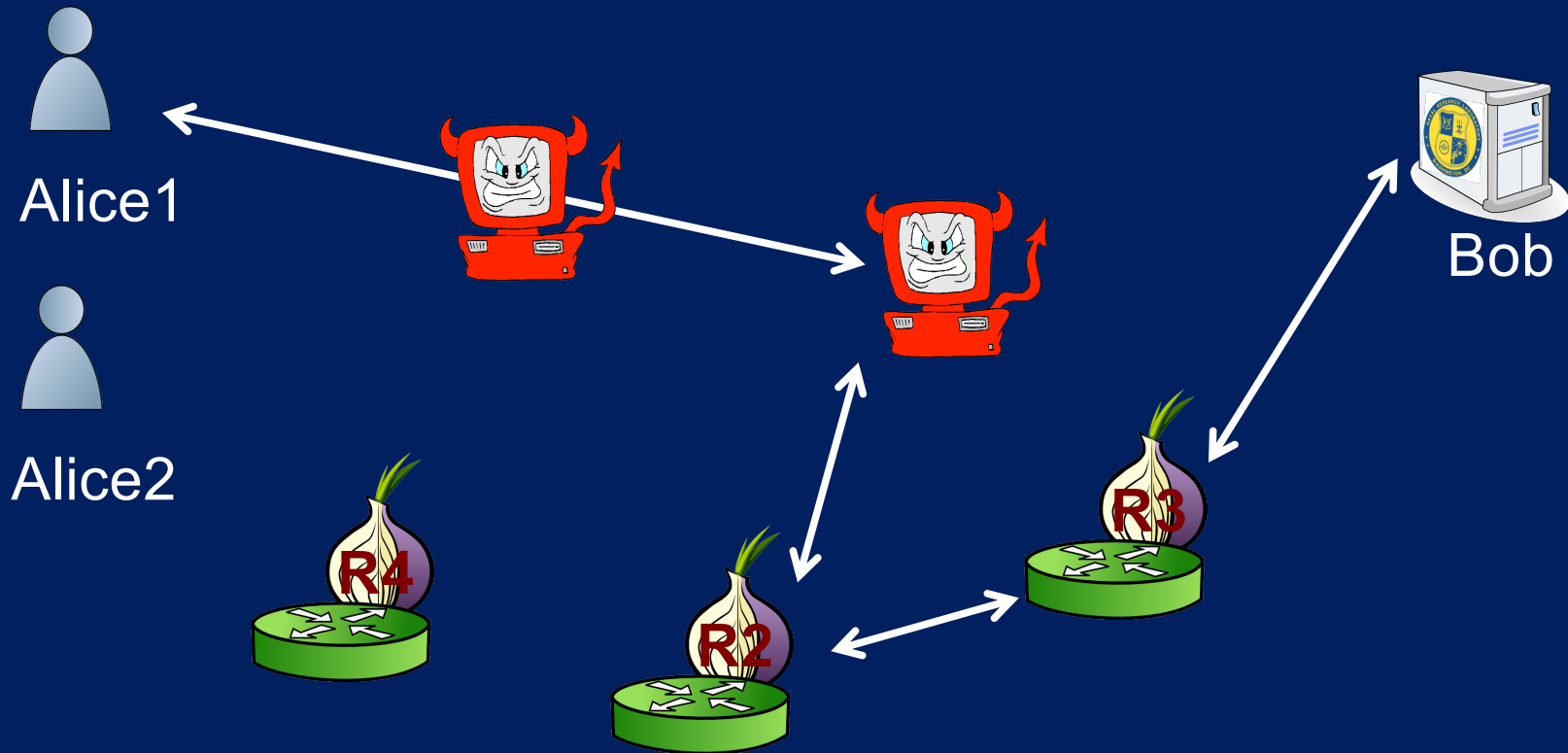
- Time



Basic adversary model: Observing traffic entering & leaving network breaks onion routing

Are we still missing anything?

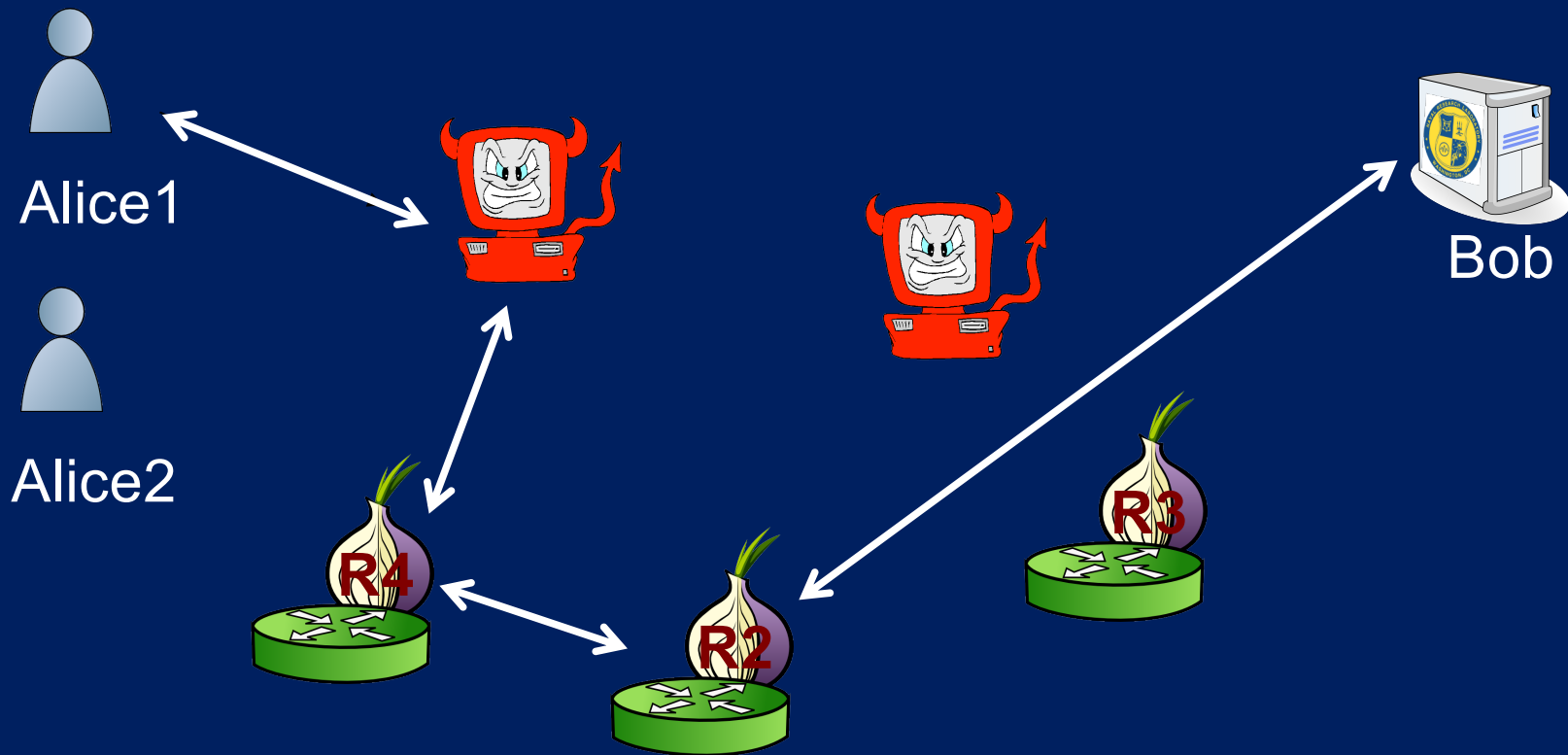
- Time



Basic adversary model: Observing traffic entering & leaving network breaks onion routing

Are we still missing anything?

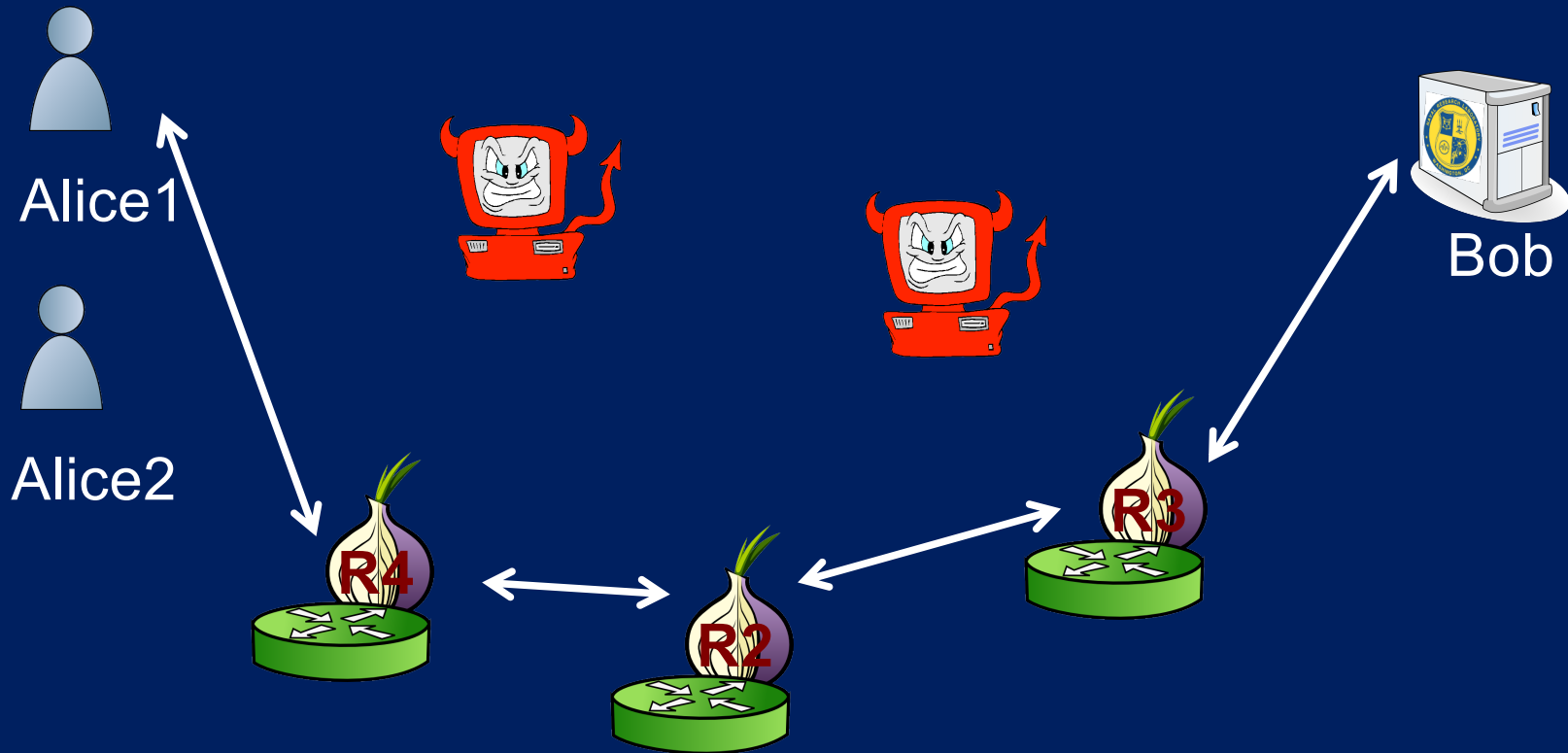
- Time



Basic adversary model: Observing traffic entering & leaving network breaks onion routing

Are we still missing anything?

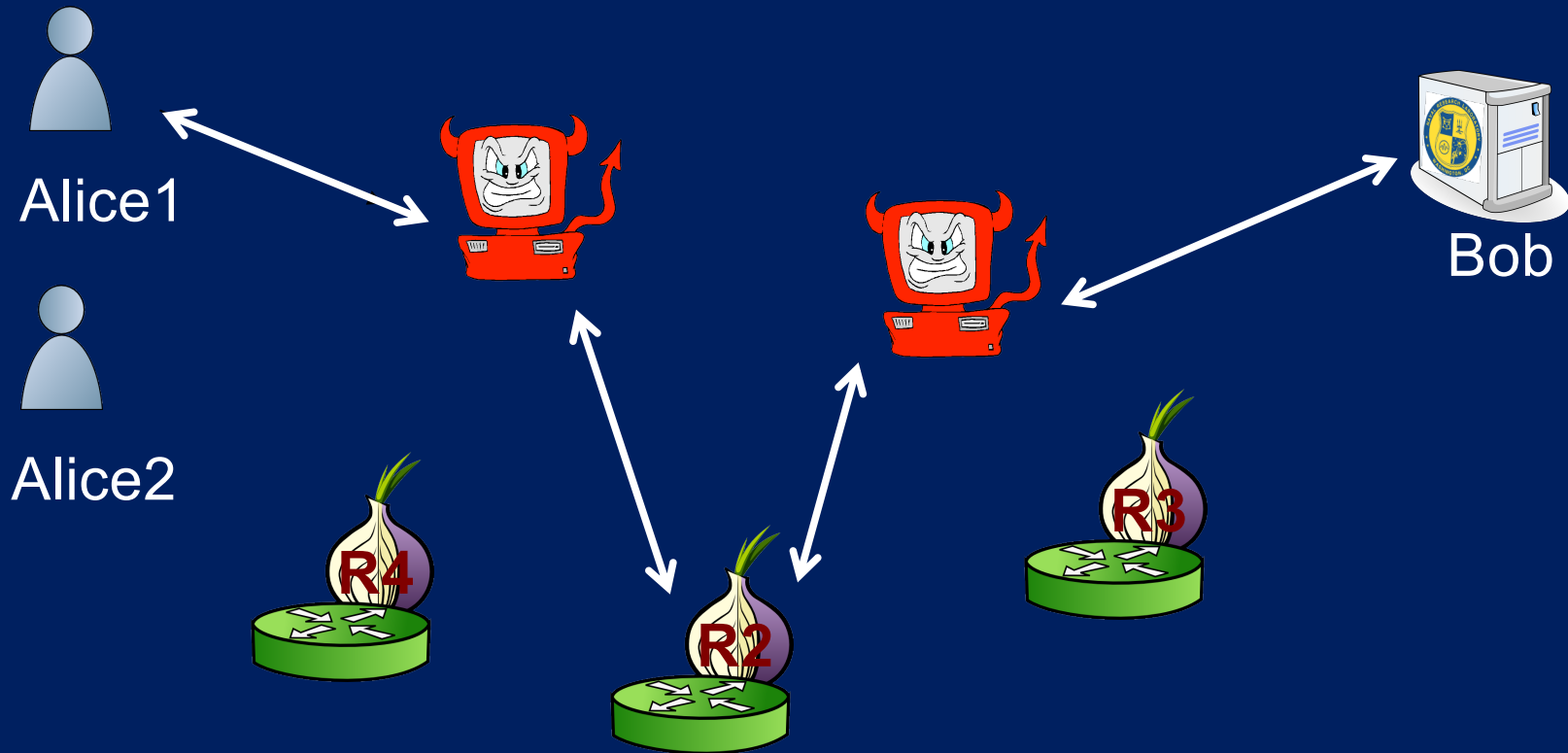
- Time



Basic adversary model: Observing traffic entering & leaving network breaks onion routing

Are we still missing anything?

- Time



Basic adversary model: Observing traffic entering & leaving network breaks onion routing

Are we still missing anything?

- Time



- Above analyses

- Give results for all communication:
 - average anonymity, worst anonymity
- Are based on a snapshot
 - all messages/connections in system at a time

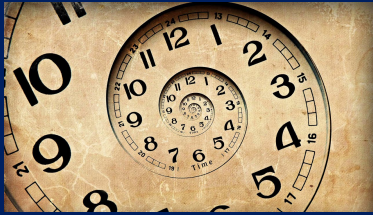
- What users actually need to know

- I'm going to use system S in context C in this way for that long
- How safe/screwed am I?

Basic adversary model: Observing traffic entering & leaving network breaks onion routing

Are we still missing anything?

- Time

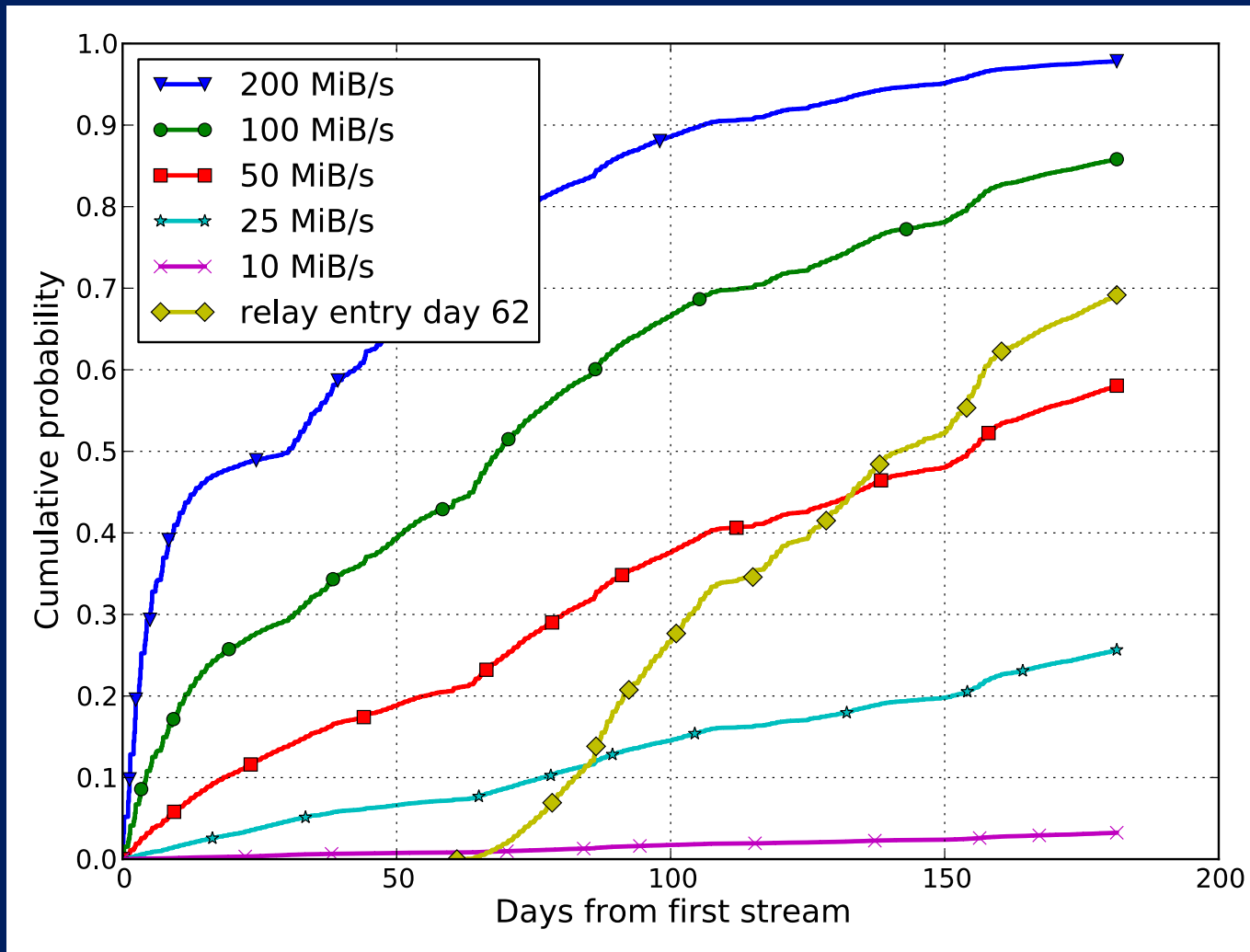


“Users Get Routed” Johnson et al. ACM CCS 02013

- Created models of various normal user behavior types
- Model of Tor network and of underlying internet (ASes, IXPs)
- Metric 1: For given behavior, what is time until first circuit compromise?
- Metric 2: For given behavior, what fraction of connections are compromised over a given period?

Basic adversary model: Observing traffic entering & leaving network breaks onion routing

“Users Get Routed” Johnson et al. ACM CCS 02013



Time to first circuit compromise,
10/12-3/13

Basic adversary model: Observing traffic entering & leaving network breaks onion routing

“Users Get Routed” Johnson et al. ACM CCS 02013

- 80% of all types of users may be deanonymized by moderate Tor-relay adversary within 6 months
- Bittorrent user by far worst off for fraction of connections compromised by Tor-relay adversary
- Against a single-AS adversary roughly 100% of users in some common locations are deanonymized within three months
- (or 95% in 3 months for a single IXP)
- 2-AS adversary reduces median time to the first client deanonymization by an order of magnitude:
 - from over 3 months to only 1 day for typical web user

- Part 1: Onion Routing and Tor
 - Background, Motivation, Basic Concepts, Basic Design
- Part 2: How Secure Is It?
 - Network and Adversary Models, Metrics
- **Part 3: Onion Services**
 - **Background, Motivation, Basic Concepts, Basic Design**
- Part 4: Self-Authenticating Traditional Addresses (SATAs)
 - Background, Motivation, Basic Concepts, Basic Design

Identity of Internet Sites is not secure

Address lookup is not secure



CDR Alice: overseas, lost &
late for meeting, looking for
route from Google Maps

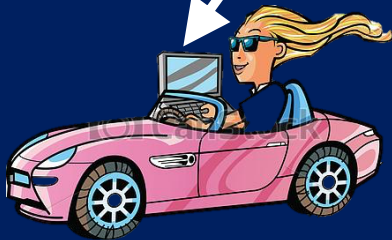
Identity of Internet Sites is not secure

Address lookup

DNS*
Server



Q:
maps.google.com
A:
172.217.1.174



CDR Alice: overseas, lost &
late for meeting, looking for
route from Google Maps



maps.google.com
IP Address:
172.217.1.174

*DNS: Domain Name System

Identity of Internet Sites is not secure

Address lookup

DNS*
Server



Q:
maps.google.com
A:
172.217.1.174



CDR Alice: overseas, lost &
late for meeting, looking for
route from Google Maps



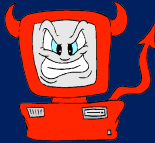
maps.google.com
IP Address:
172.217.1.174

*DNS: Domain Name System

Identity of Internet Sites is not secure

Address lookup is not secure

DNS*
Server



Q:
maps.google.com
A:
185.64.80.30

kktcmerkezbankasi.org
IP Address:
185.64.80.30



CDR Alice: overseas, lost &
late for meeting, looking for
route from Google Maps



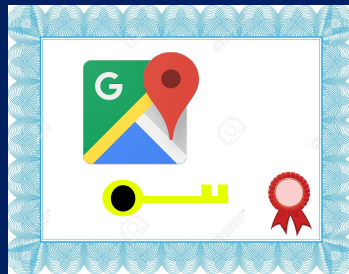
maps.google.com
IP Address:
172.217.1.174

*DNS: Domain Name System

Identity of Internet Sites is not secure

Crypto to the rescue

Certificate
Authority



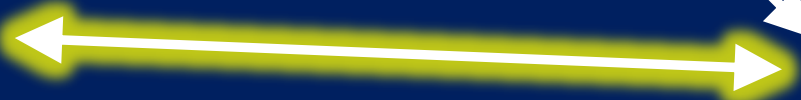
kktcmerkezbankasi.org
IP Address:
185.64.80.30



CDR Alice: overseas, lost &
late for meeting, looking for
route from Google Maps



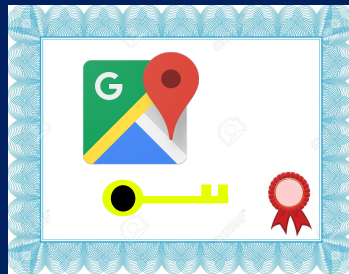
maps.google.com
IP Address:
172.217.1.174



Identity of Internet Sites is not secure

Crypto to the rescue?

Certificate
Authority



CDR Alice: overseas, lost &
late for meeting, looking for
route from Google Maps

kktcmerkezbankasi.org
IP Address:
185.64.80.30

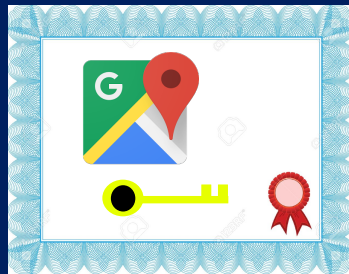


maps.google.com
IP Address:
172.217.1.174

Identity of Internet Sites is not secure

Crypto to the rescue?

Certificate
Authority



kktcmerkezbankasi.org
IP Address:
185.64.80.30



CDR Alice: overseas, lost &
late for meeting, looking for
route from Google Maps

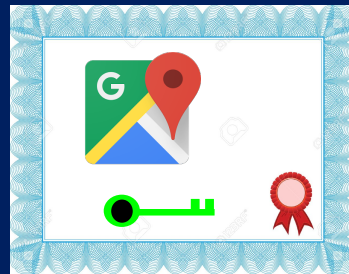


maps.google.com
IP Address:
172.217.1.174

Identity of Internet Sites is not secure

Site entrance is not secure

Certificate Authority 



kktcmerkezbankasi.org
IP Address:
185.64.80.30



CDR Alice: overseas, lost & late for meeting, looking for route from Google Maps

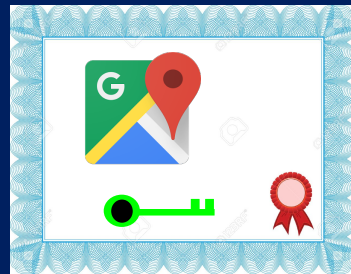


maps.google.com
IP Address:
172.217.1.174

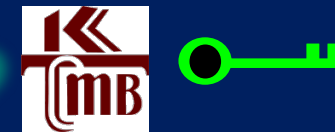
Identity of Internet Sites is not secure

Site entrance is not secure

Certificate Authority 



kktcmerkezbankasi.org
IP Address:
185.64.80.30



CDR Alice: overseas, lost & late for meeting, looking for route from Google Maps

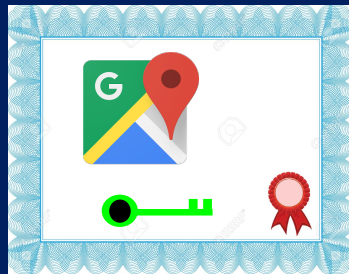


maps.google.com
IP Address:
172.217.1.174

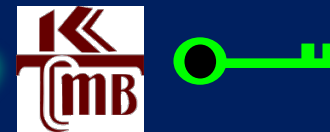
Is that *really* a plausible scenario?

Site entrance is not secure

Certificate Authority 



kktcmerkezbankasi.org
IP Address:
185.64.80.30



CDR Alice: overseas, lost & late for meeting, looking for route from Google Maps



maps.google.com
IP Address:
172.217.1.174

Site entrance is not secure



Krebs on Security
In-depth security news and investigation

03 Turkish Registrar Enabled Phishers to Spoof Google

JAN 13

[f](#) [t](#) [g+](#) [r](#) [p](#) [in](#) [e](#)

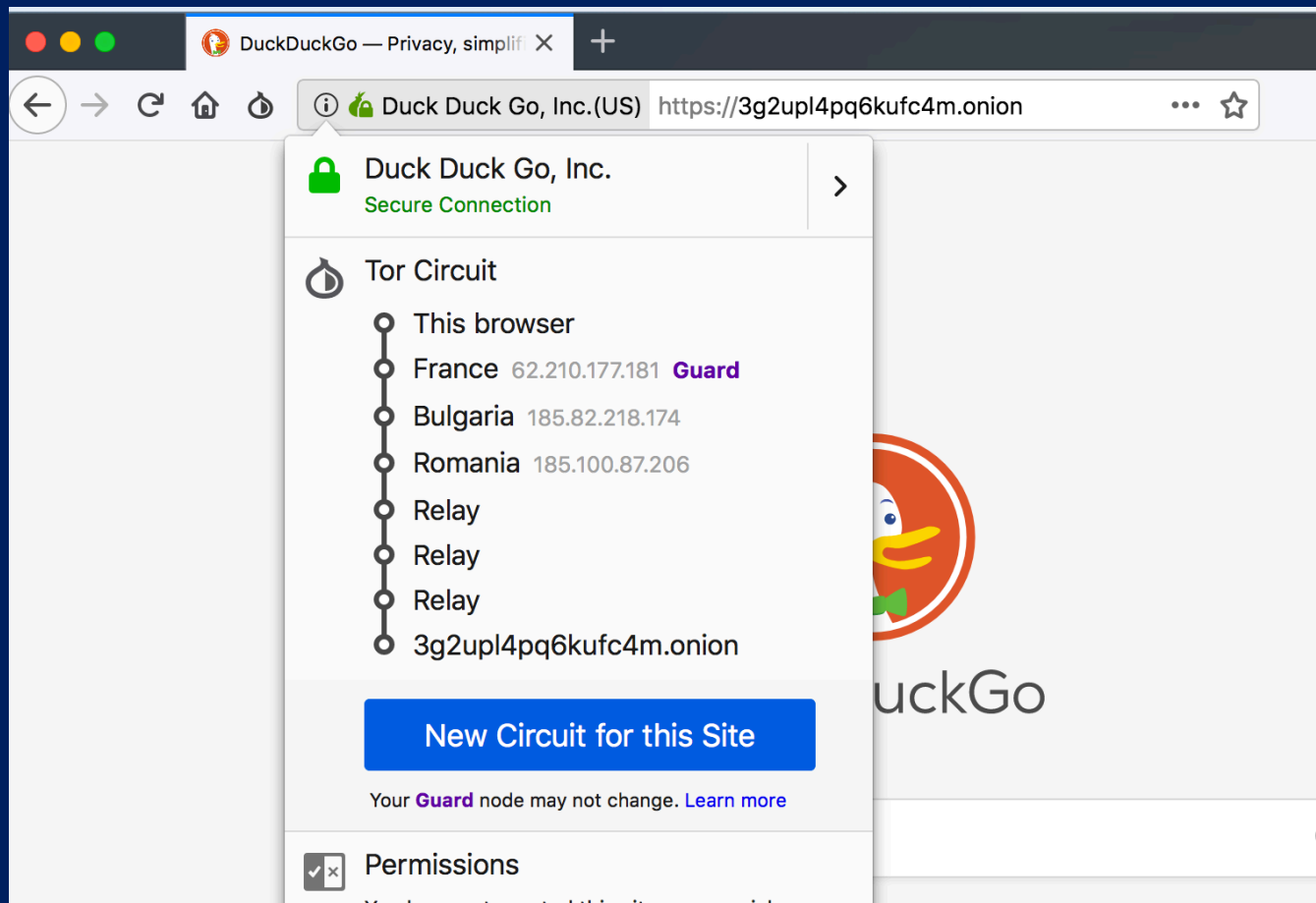
Google and **Microsoft** today began warning users about active phishing attacks against Google's online properties. The two companies said the attacks resulted from a fraudulent digital certificate that was mistakenly issued by a Turkish domain registrar.

In [a blog post](#) published today, Google said that on Dec. 24, 2012, its **Chrome** Web browser detected and blocked an unauthorized digital certificate for the "*.google.com" domain.

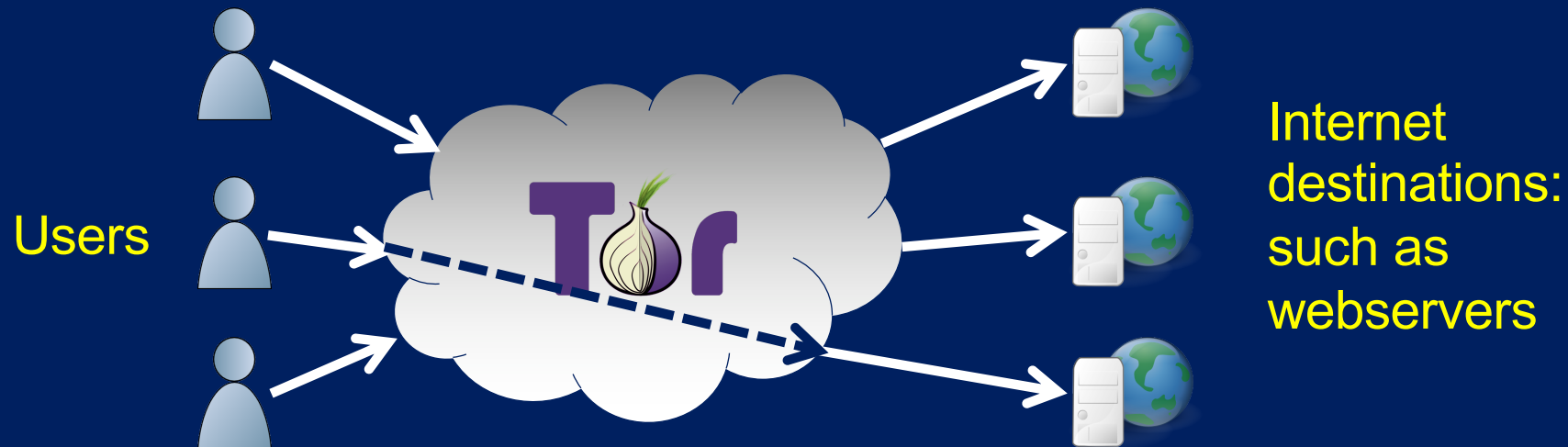
onion addresses are self authenticating

$3g2upl4pq6kufc4m = H(\text{Pubkey}(\text{DuckDuckGo}))$

- Not subject to Certificate hijacks
- Give site owner more control over address lookup
- Give site owner more control over site identity (authentication)

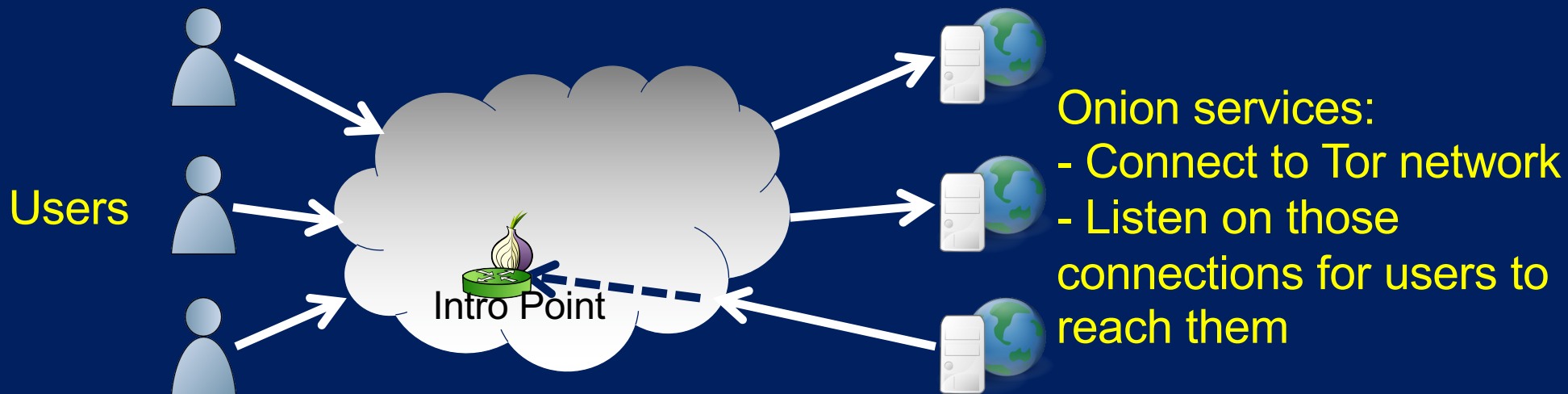


Recall: Vanilla Tor use



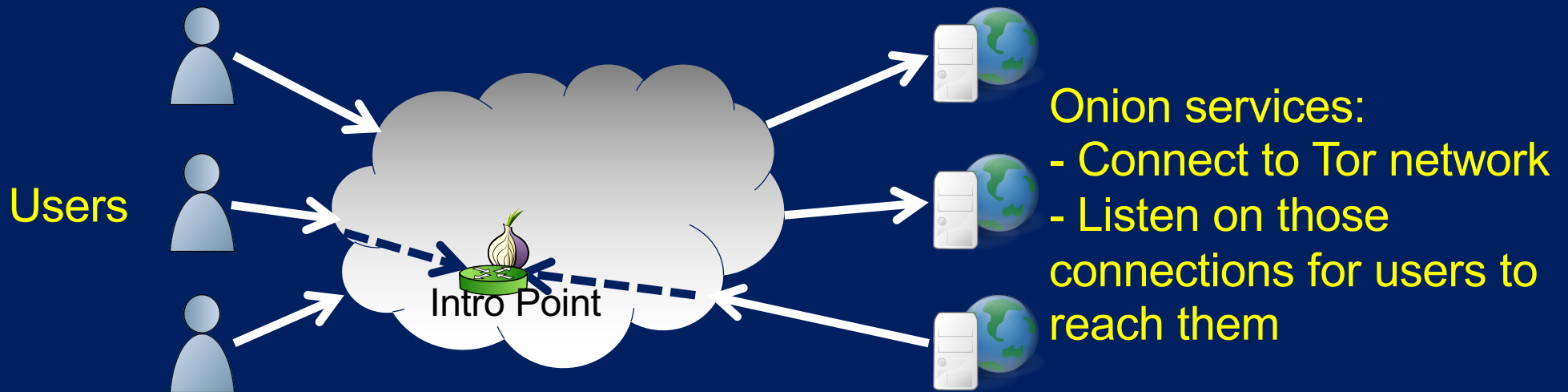
- Tor: Network primarily provides reachability and prevents source-destination linking for c. 2-8 million users
- Tor network: c. 7K volunteer run relays
- Vast majority of Tor traffic by volume is for such exit traffic
 - Only 5-10% is onion service traffic (cf. metrics.torproject.org)

(Very) short history of onion services



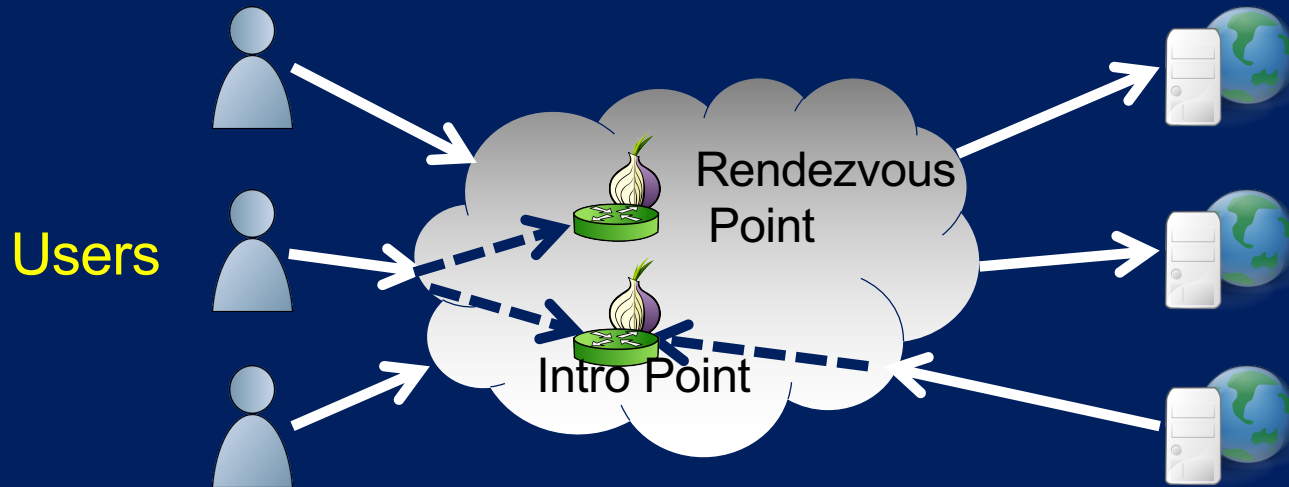
Cf. “Tor: The Second Generation Onion Router”
USENIX Security 02004

(Very) short history of onion services



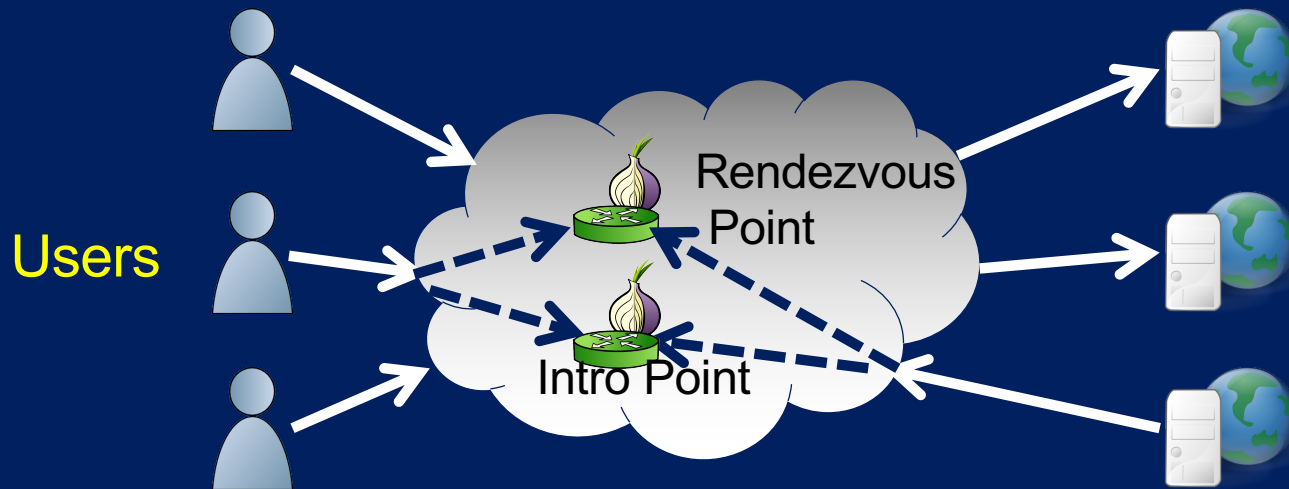
Cf. “Tor: The Second Generation Onion Router”
USENIX Security 02004

(Very) short history of onion services



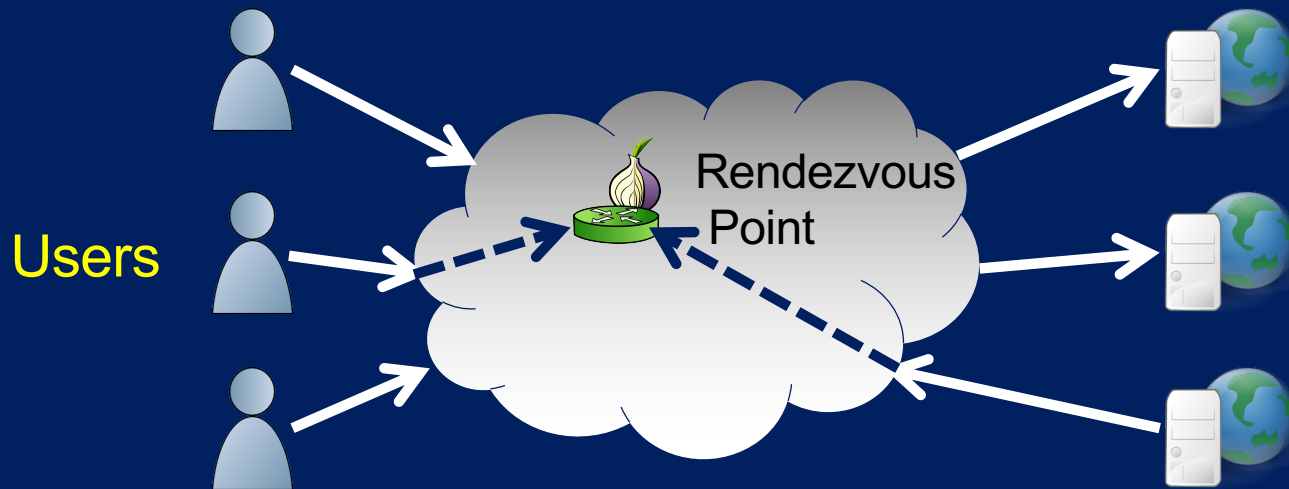
Cf. “Tor: The Second Generation Onion Router”
USENIX Security 02004

(Very) short history of onion services



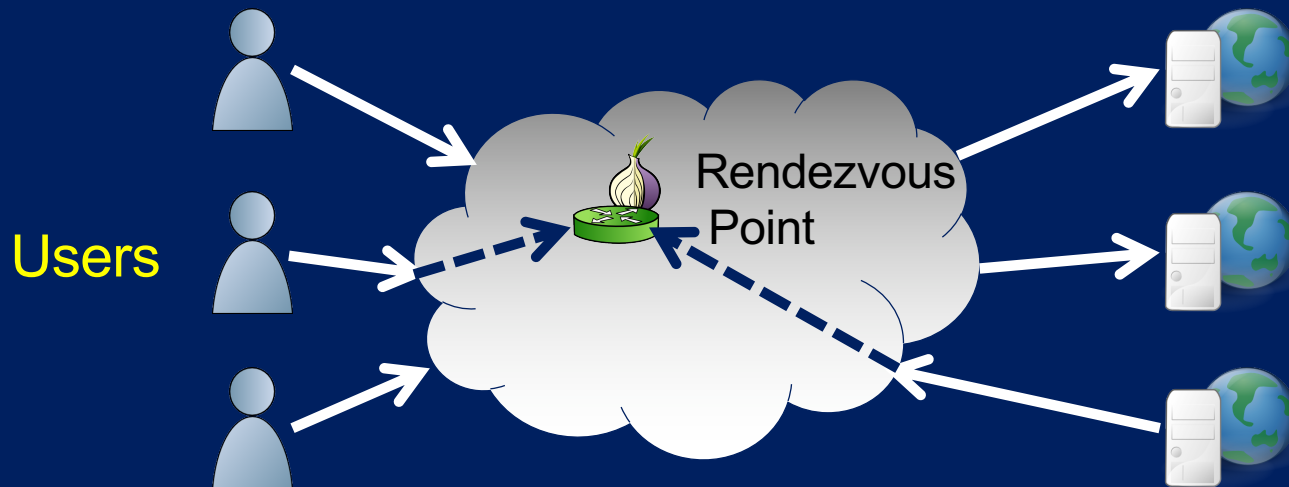
Cf. “Tor: The Second Generation Onion Router”
USENIX Security 02004

(Very) short history of onion services



Cf. "Tor: The Second Generation Onion Router"
USENIX Security 02004

(Very) short history of onion services



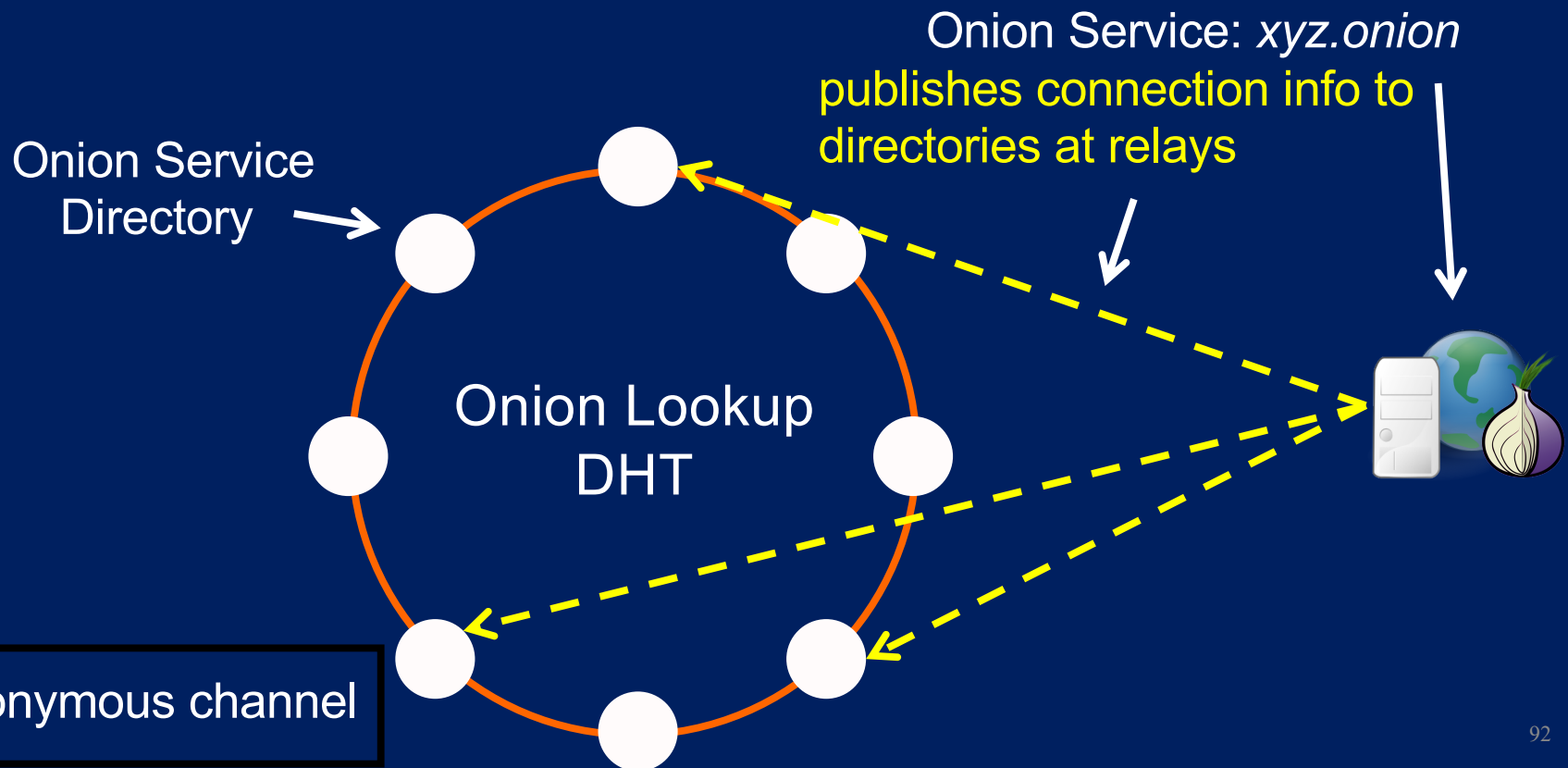
- Onion services:
 - reachable without exposing network location
 - Site-owner control over authentication of site address and entrance

Cf. “Tor: The Second Generation Onion Router”
USENIX Security 02004

Onion address listing and lookup (02004)

Onion address directory system is a Distributed Hash Table (DHT)

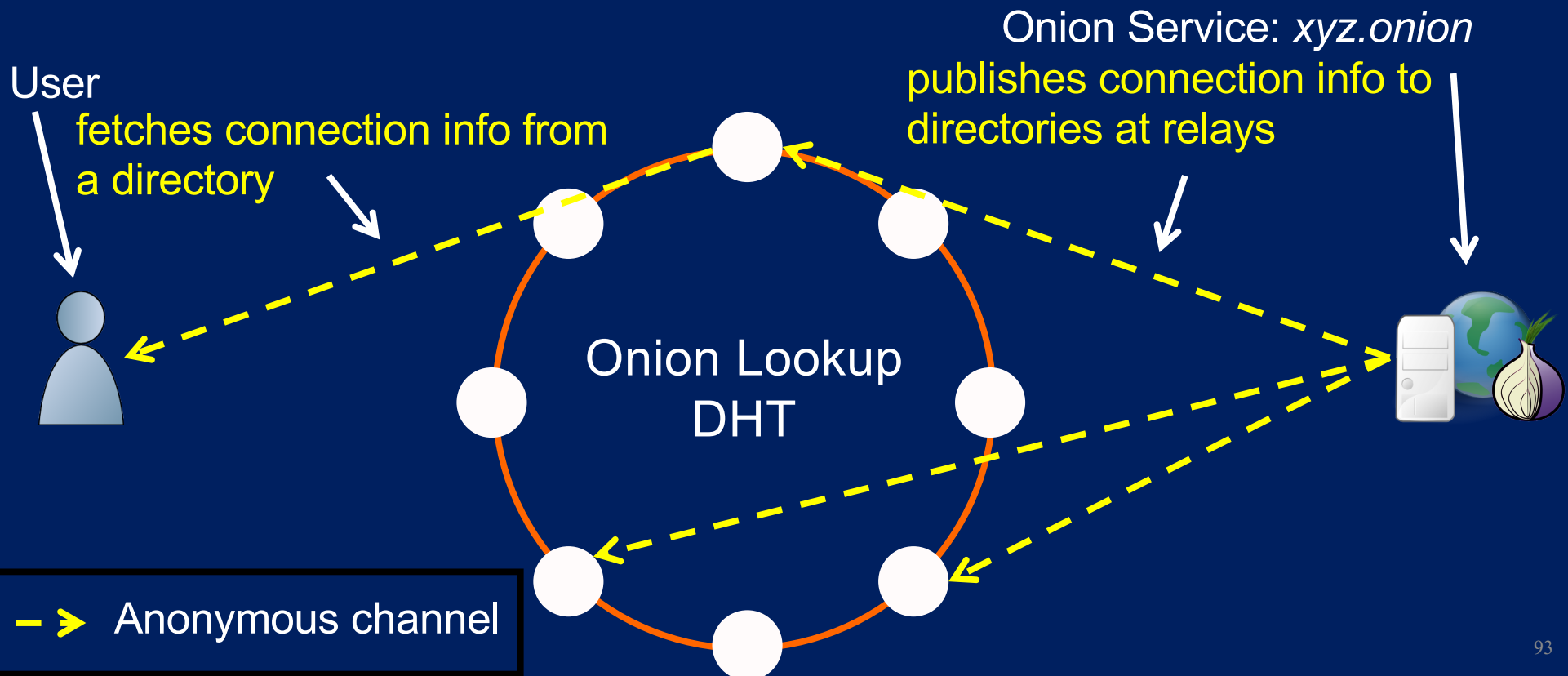
- Each onion address published to 6 Tor relays



Onion address listing and lookup (02004)

Onion address directory system is a Distributed Hash Table (DHT)

- Each onion address published to 6 Tor relays
- User knows onion address and uses it to do lookup



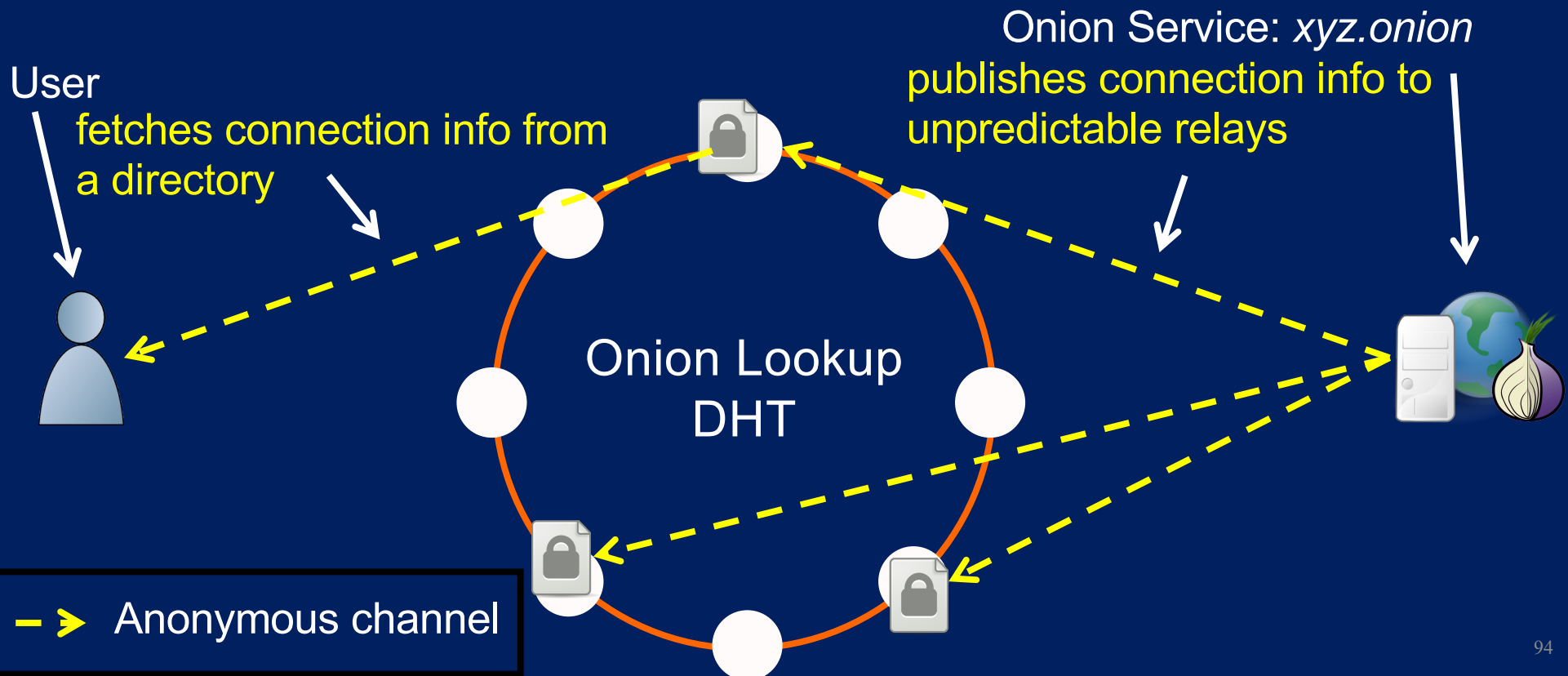
Onion address lookup no longer subject to active or passive mining (02017)

Onion address directory system is a Distributed Hash Table (DHT)

- Each onion address published to 6 unpredictable Tor relays*
- Must know onion address to do lookup (relay can't tell what addresses it holds)

*Distributed randomness from DirAuths used for address location in DHT

Can't harvest onion addresses or target them for censorship/analysis



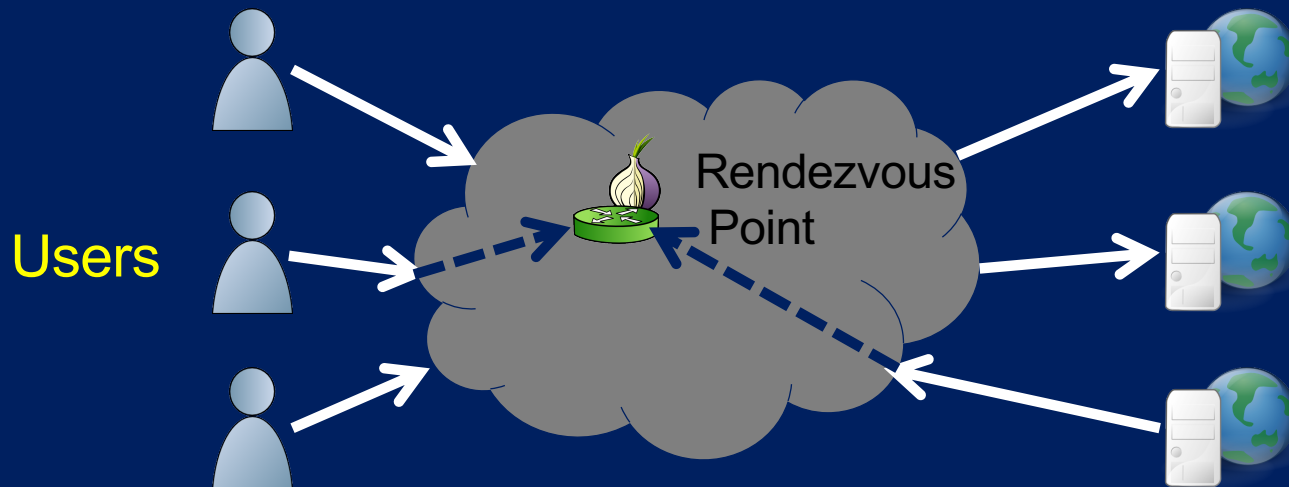
- Old onion keys are weak
 - 1024 bit RSA
- Old onion addresses are weak on weak
 - First 80 bits of SHA-1 hash of 1024 bit RSA key

- Old onion keys are weak
 - 1024 bit RSA
- Old onion addresses are weak on weak
 - First 80 bits of SHA-1 hash of 1024 bit RSA key
- New onion keys and addresses are stronger
 - Elliptic curve keys based on Ed25519
 - Old onion addresses were 16 characters

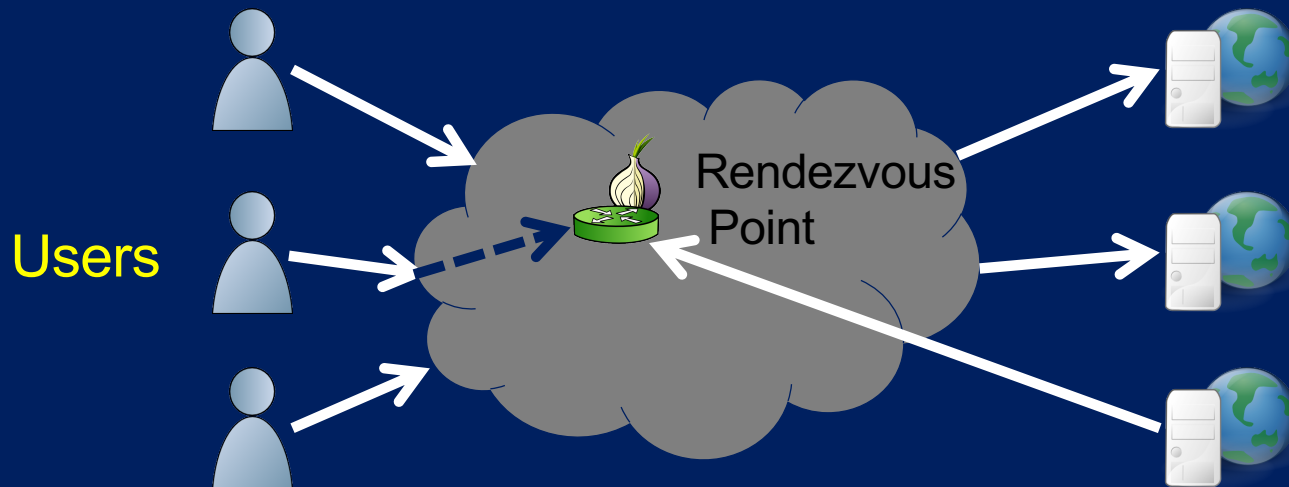
`nzh3fv6jc6jskki3.onion`

- New onion addresses are 52 characters

`a1uik0w1gmfq3i5ievxdm9ceu27e88g6o7pe0rdw9jmntwkdsd.onion`



- Onion services:
 - reachable without exposing network location
 - **Site-owner control over authentication of site address and entrance**

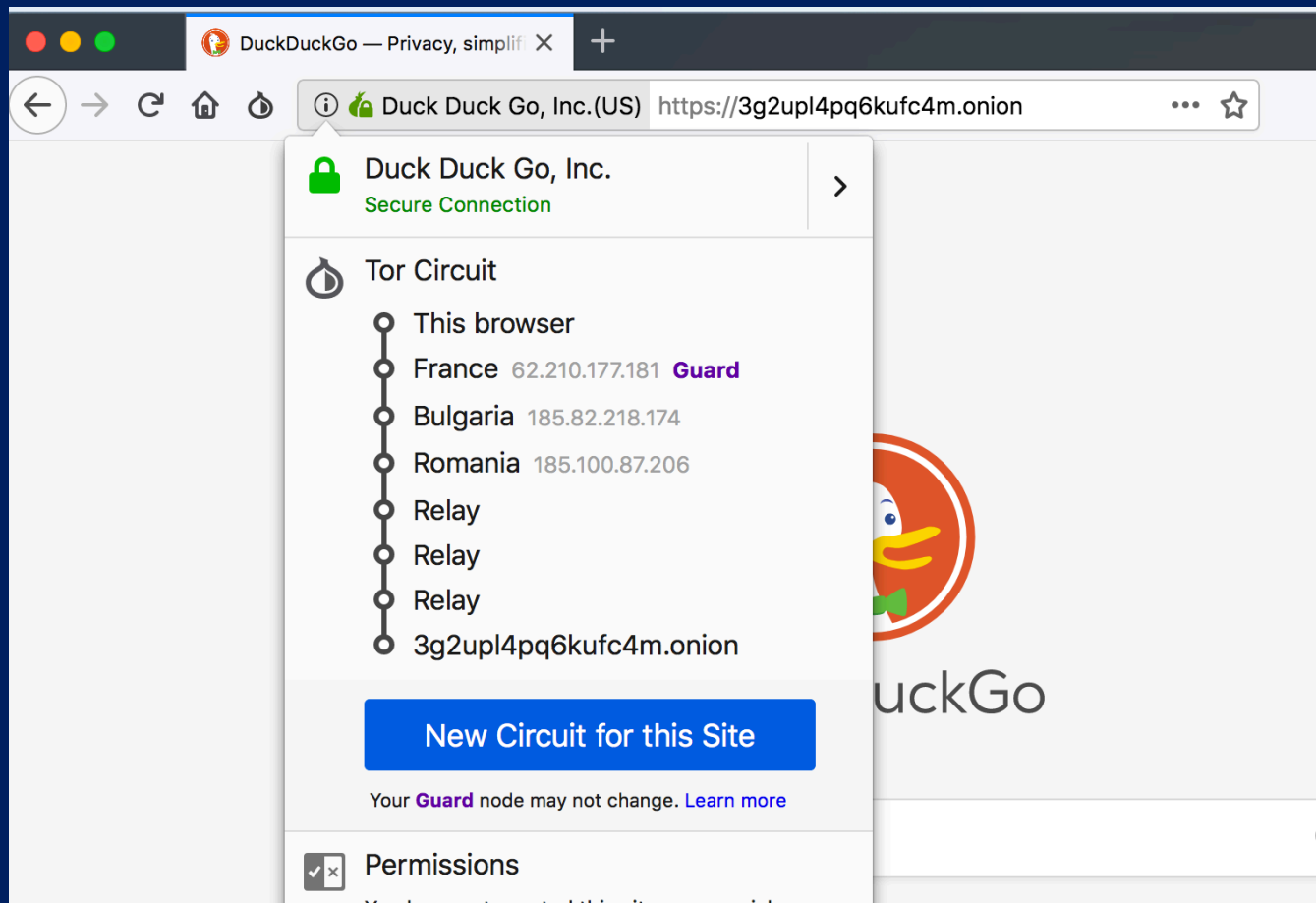


- Single-onion services:
 - ~~reachable without exposing network location~~
 - Site-owner control over authentication of site address and entrance

onion addresses are self authenticating

$3g2upl4pq6kufc4m = H(\text{Pubkey}(\text{DuckDuckGo}))$

- Not subject to Certificate hijacks
- Give site owner more control over address lookup
- Give site owner more control over site identity (authentication)



IETF RFC 7686: In 02015 .onion officially a reserved Top Level Domain standard

Internet Engineering Task Force (IETF)
Request for Comments: 7686
Category: Standards Track
ISSN: 2070-1721

The

The ".onion" Special-Use Domain Name

Abstract

This document registers the ".onion" Special-Use Domain Name.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community, which has received public review and has been approved for publication by the IETF.

IETF RFC 7686: In 02015 .onion officially a reserved Top Level Domain standard

- Wait, where's the evil deep dark web?



The iceberg of ignorance



The iceberg of ignorance



The Dark Web is an illusion!

The Dark Web is an illusion!



The Dark Web is an illusion!



The Dark Web is an illusion!



The Dark Web is an illusion!

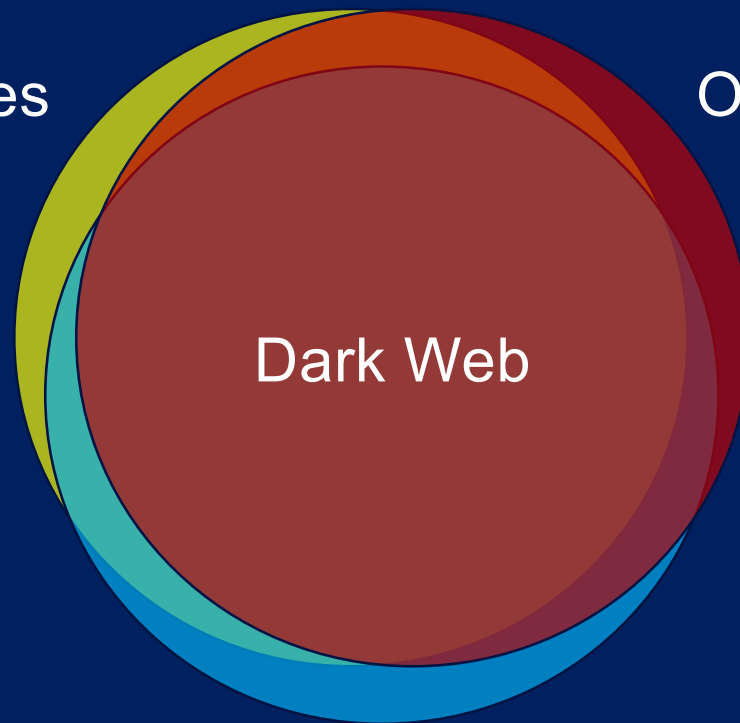


The Dark Web is an illusion!

The “Dark Web” as popularly depicted

Onion services

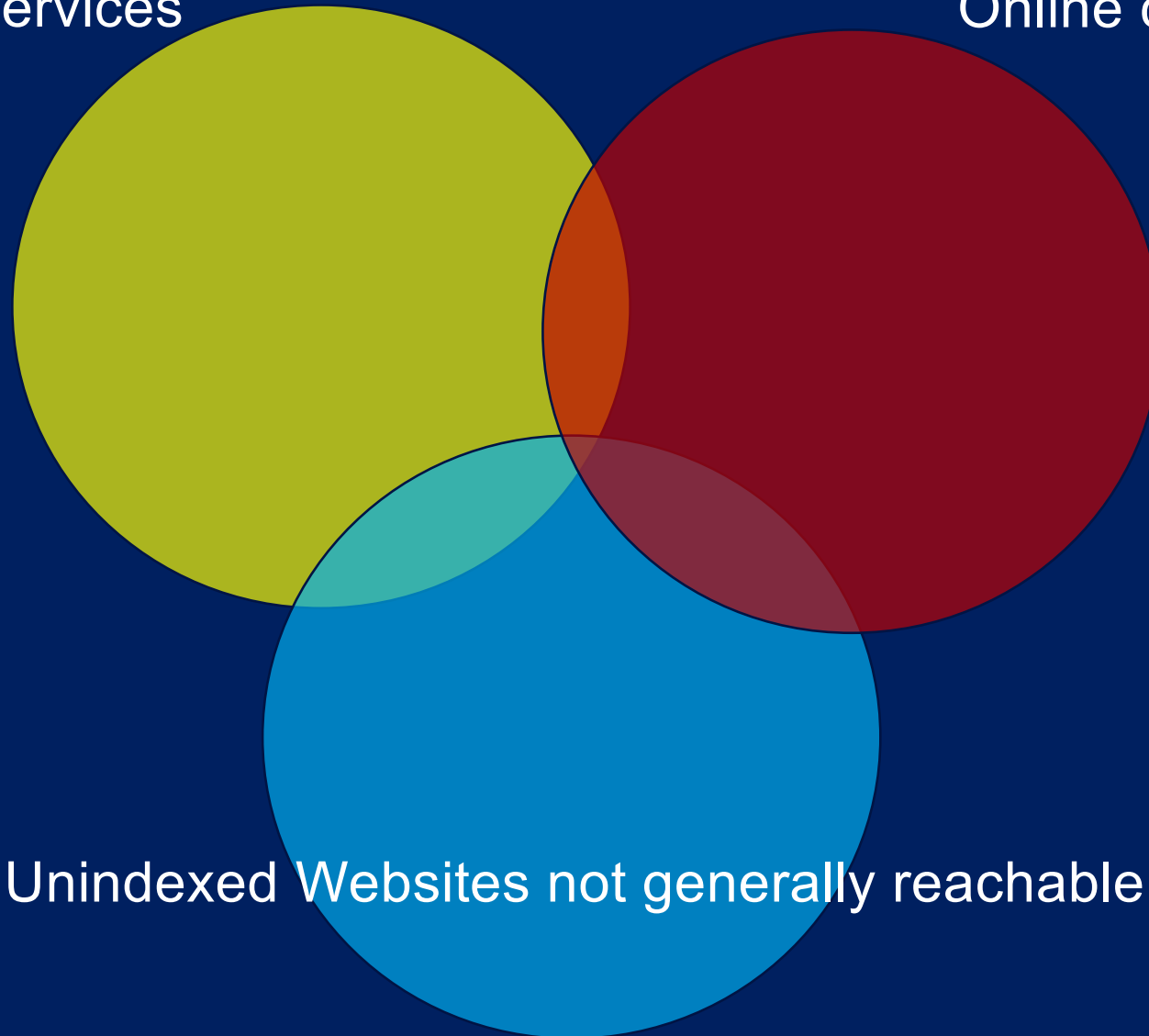
Online criminal activity



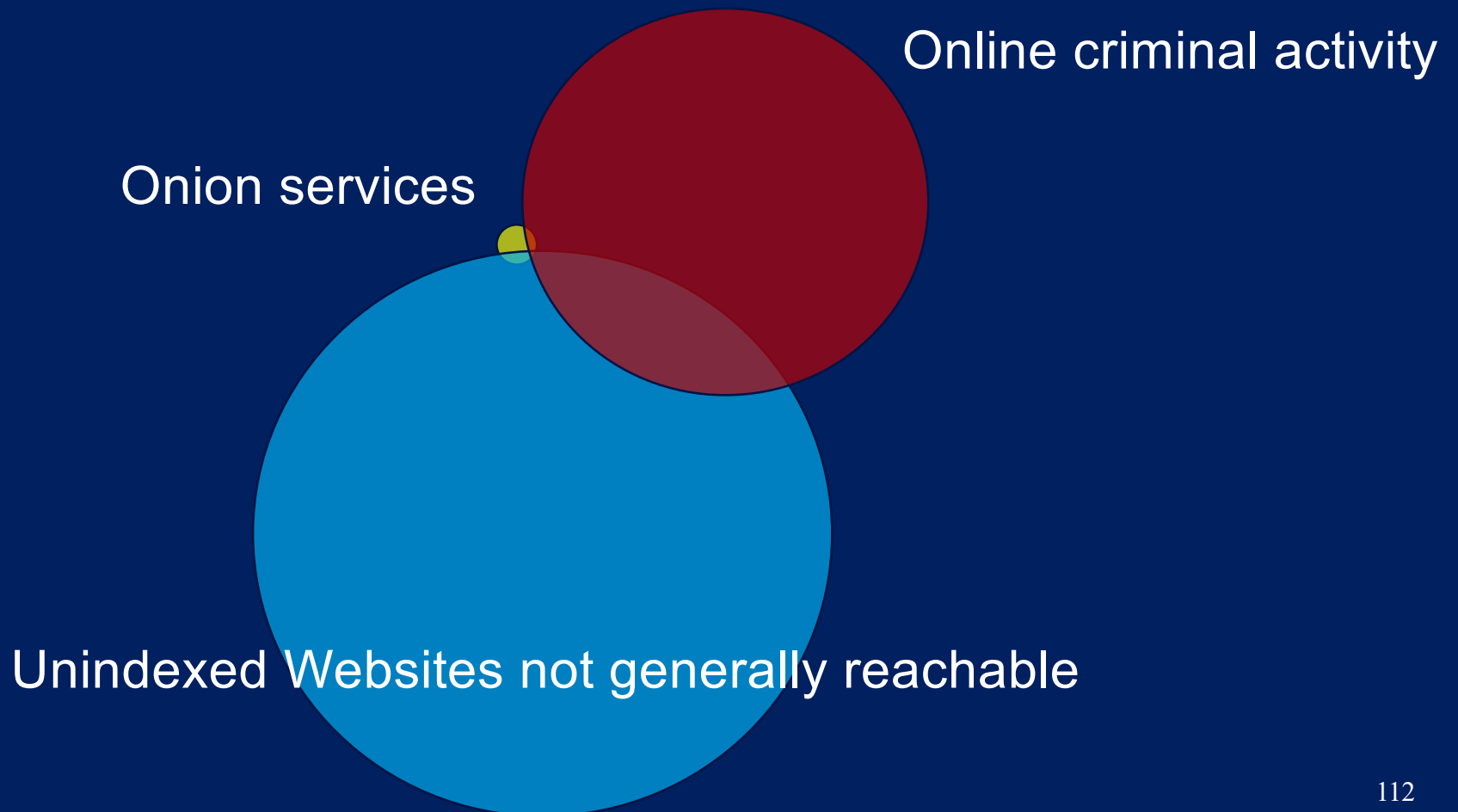
Unindexed Websites not generally reachable

Onion services

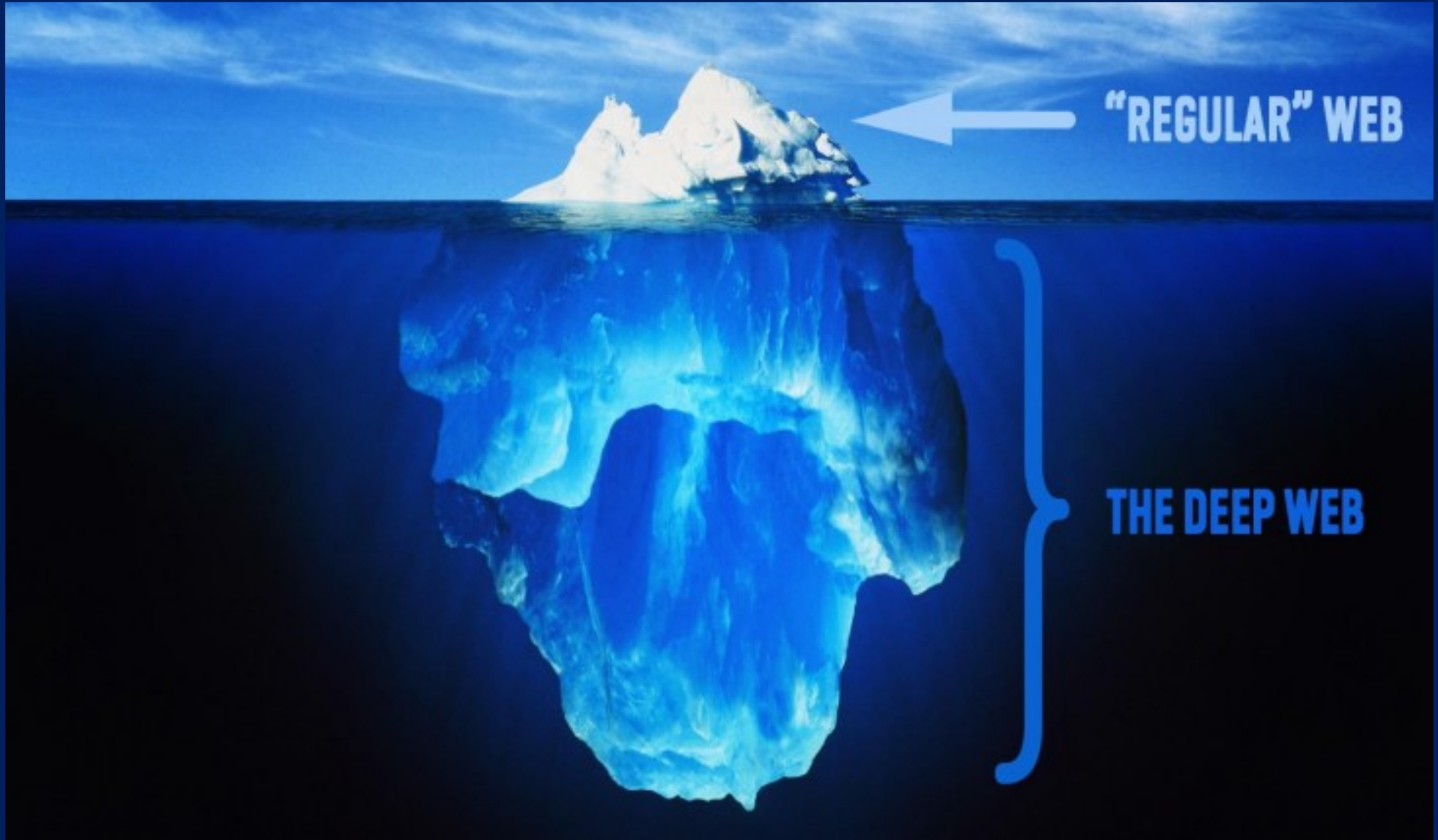
Online criminal activity



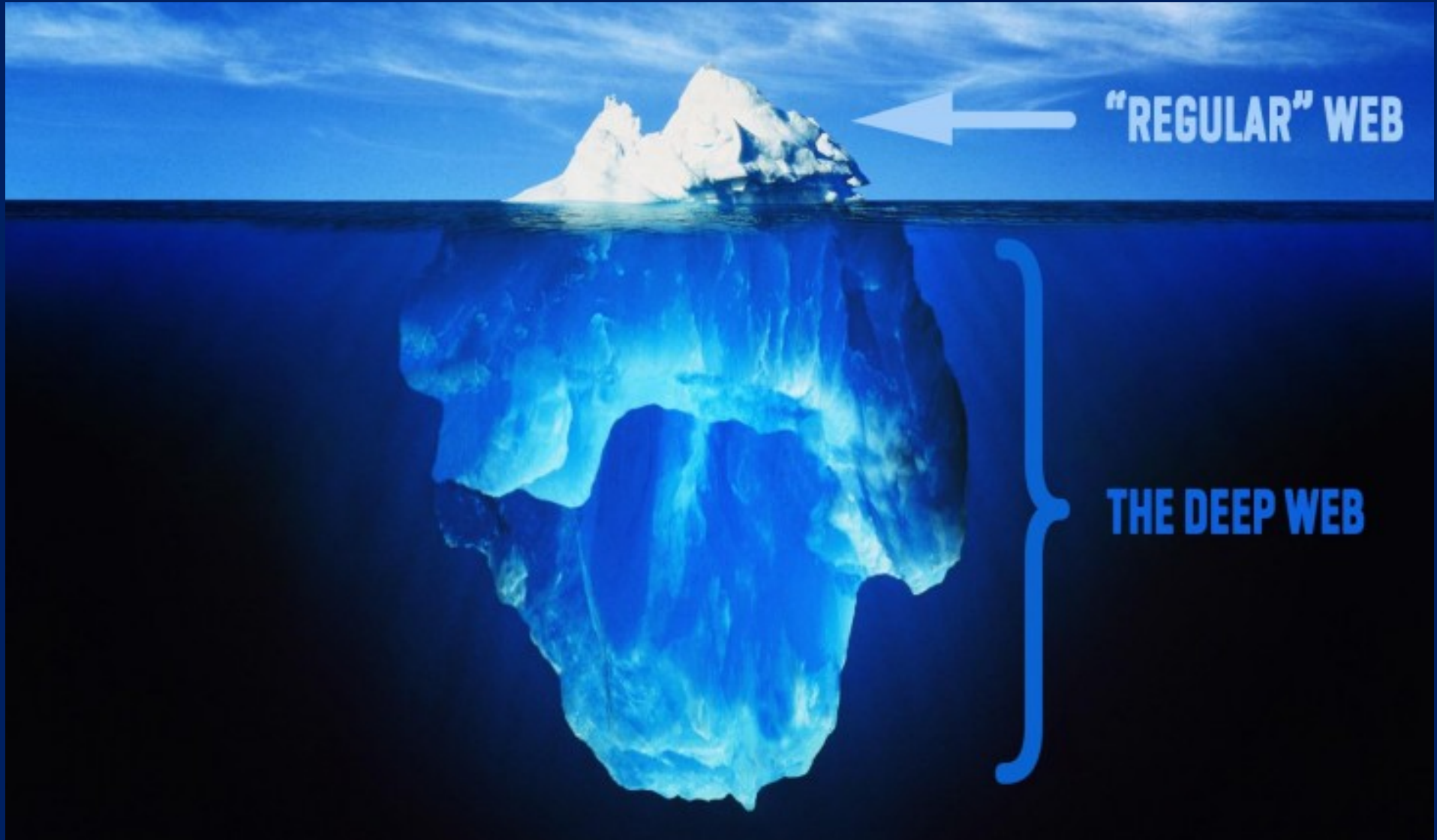
Reality to Scale



The iceberg of ignorance



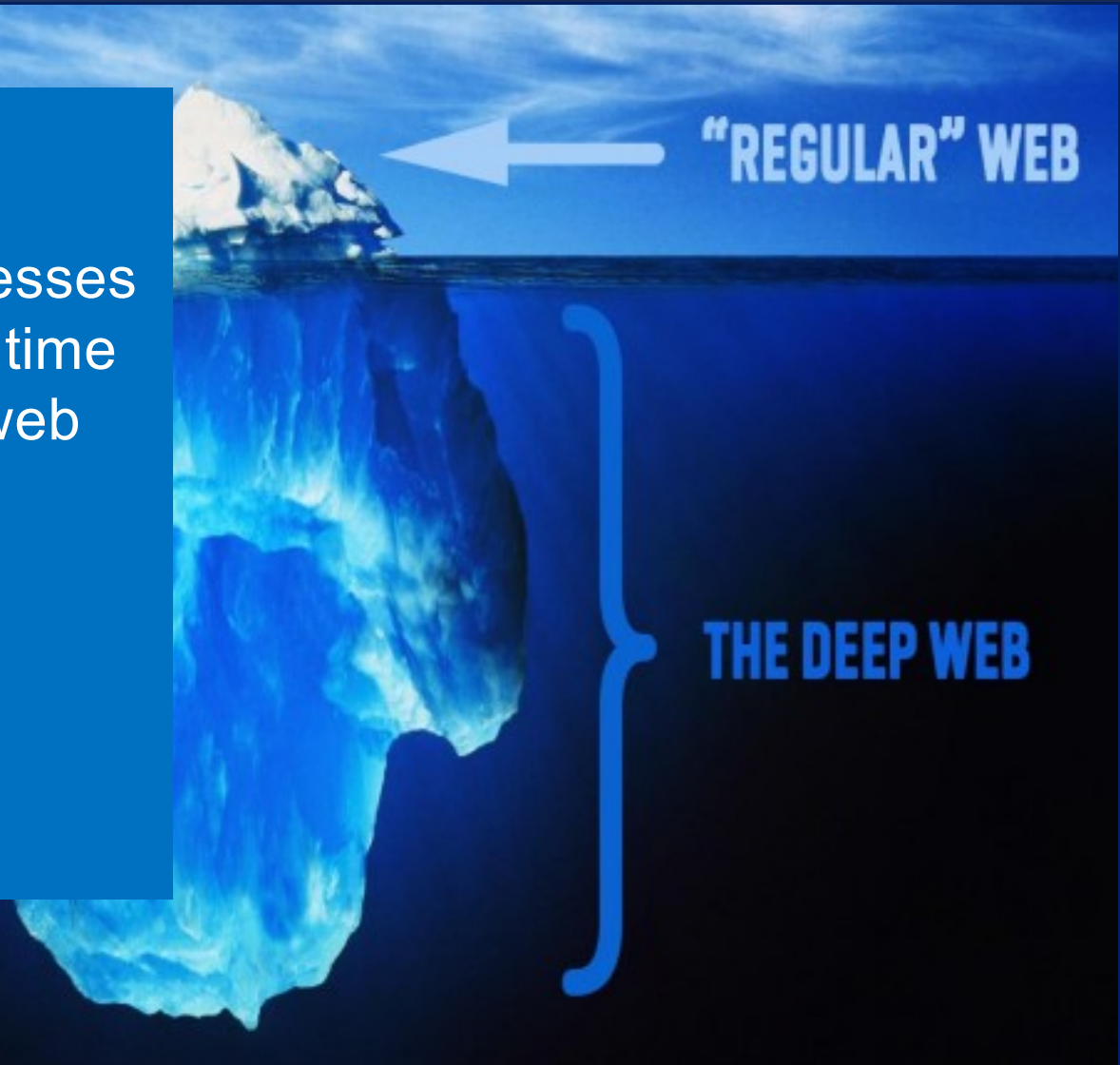
Onionspace Myth 1: Onionspace is way bigger than the “regular” web



Onionspace Myth 1: Onionspace is way bigger than the “regular” web

Currently:

thousands of onion addresses
directly reachable at any time
vs. millions less-secure web
addresses

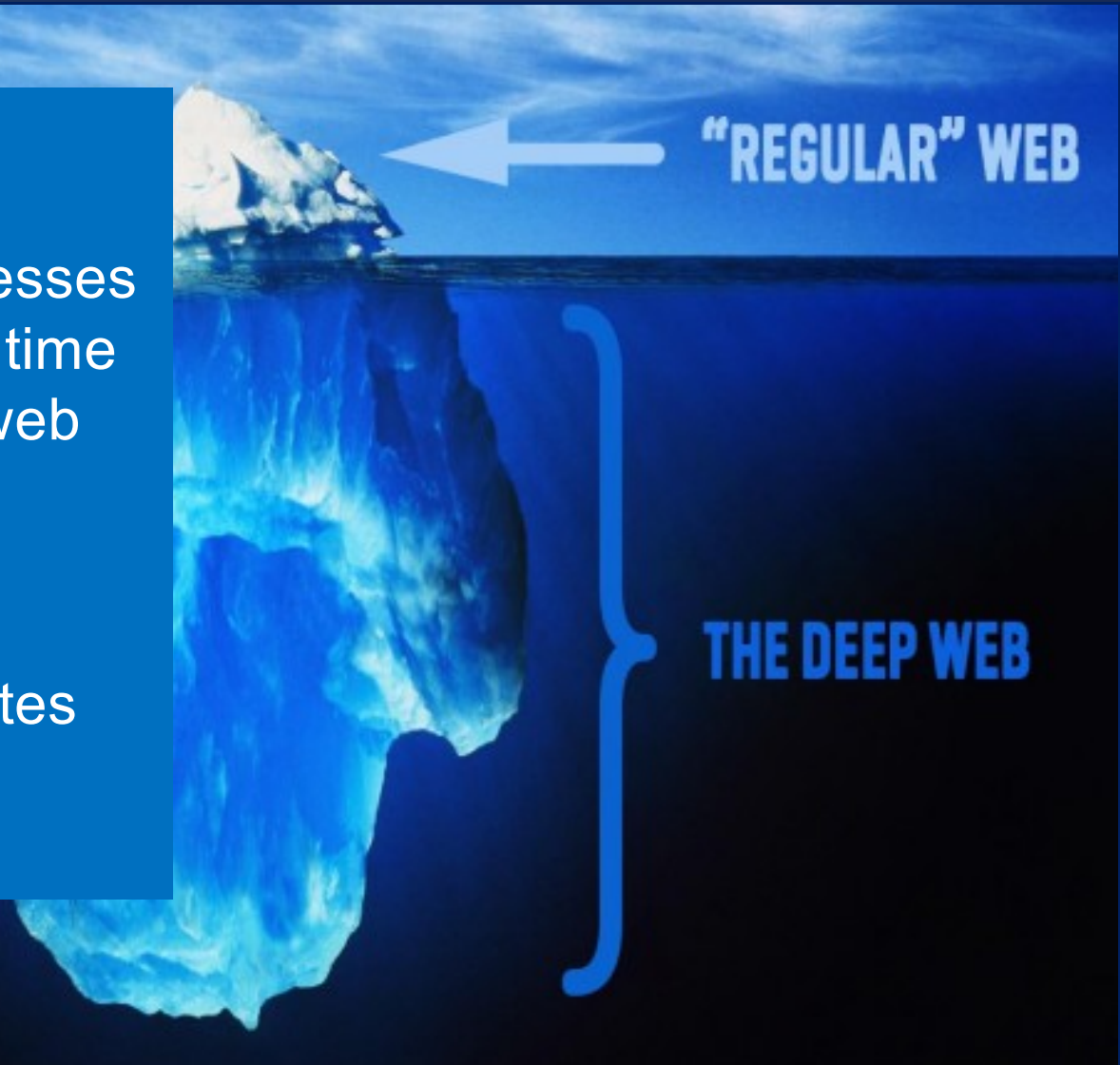


Onionspace Myth 2: Most Tor activity is on connections to .onion sites

Currently:

thousands of onion addresses
directly reachable at any time
vs. millions less-secure web
addresses

90% of Tor traffic to less-
secure sites, not onion sites



Invert the iceberg of ignorance



What's wrong with this picture?



Onionspace Myth 3: Onionspace is not indexed

Search results for propubli... x +

https://ahmia.fi/search/?q=propublica

AHMIA propublica Search

About Ahmia Statistics Add Service i2p search

Omitted very similar entries. Displaying 2 matches in 0.31 seconds. Page 1 of 1 .

[Home – ProPublica](#)

Home
sxdyc2ebgvlbrmrj.onion – 3 weeks, 6 days ago – [Report Abuse](#)

[Mike Tigas](#)

Mike Tigas is a developer, journalist, photographer, civic hacker, and security/privacy tinkerer at ProPublica.
tigas3l7uusztiqu.onion – 2 weeks, 4 days ago – [Report Abuse](#)

Grain of truth: Ordinary search engines don't index onionspace...yet/much. Can still get .onion addresses.

The screenshot shows a web browser window with the DuckDuckGo search engine. The search query is "new york times onion service". The results page displays three search results, each with a title, a short description, and a URL. The first result is titled "The New York Times is Now Available as a Tor Onion Service" and includes a URL starting with "https://open.nytimes.com/". The second result is titled "The New York Times Now Accessible Via Tor Onion Service ..." and includes a URL starting with "https://darkwebnews.com/". The third result is titled "The New York Times is now a Tor onion service / Boing Boing" and includes a URL starting with "https://boingboing.net/". A red circle highlights the ".onion" part of the URL in the third result. In the bottom right corner of the browser window, there is a "Send feedback" button.

new york times onion servi... x +

Duck Duck Go, Inc. (US) | <https://duckduckgo.com/?q=new+york+times+onion+service> Search

new york times onion service

Web Images Videos News

All Regions Safe Search: Strict Any Time

The New York Times is Now Available as a Tor Onion Service
Today we are announcing an experiment in secure communication, and launching an alternative way for people to access our site: we are making the nytimes.com website available as a Tor Onion Service...
<https://open.nytimes.com/https-open-nytimes-com-the-new-york-times...>

The New York Times Now Accessible Via Tor Onion Service ...
The New York Times has just announced that the internationally renowned publication is now accessible on the dark web. The media outlet is set to have its own .onion service, and users can only access the site through the Tor browser.
<https://darkwebnews.com/anonymity/nyt-tor/>

The New York Times is now a Tor onion service / Boing Boing
The New York Times is now available as an "Onion Service" on the Tor network, at the address <https://www.nytimes3xbfgragh.onion/> meaning that anyone with Tor access can securely and privately access the Times without giving away any information about what they're looking at, even to state-level ...
<https://boingboing.net/2017/10/27/routing-around-censorship.html>

Send feedback

Grain of truth: Ordinary search engines don't index
onionspace...yet/much. Can still get .onion addresses.

← → ↻ 🏠 🔒 https://encrypted.google.com/search?hl=en

Google propublica onion

All News Images Shopping Videos More

About 60,200 results (0.45 seconds)

A More Secure and Anonymous ProPublica Using
<https://www.propublica.org> > The Nerd Blog ▼

Jan 13, 2016 - Once you've got it installed, copy and paste this URL
<http://www.propub3r6espa33w.onion/> This is called a "Tor hidden se
relays (and a web browser that uses the network) that protects your
habits from your ...

What else is wrong with this picture?



What else is wrong with this picture?



What is the largest source of pages in onionspace?

Onionspace Myth 4: Sites in onionspace are not part of “regular” web

What is the largest source of pages in onionspace?

All of Facebook is available at <https://facebookcorewwi.onion>



Onionspace Myth 4: Sites in onionspace are not part of “regular” web

What is the largest source of pages in onionspace?

All of Facebook is available at <https://facebookcorewwi.onion>

All sites hosted by Cloudflare available through their onion services



Related Onionspace Myth 5: Onionspace is all for criminal activity

What is the largest source of pages in onionspace?

All of Facebook is available at <https://facebookcorewwi.onion>

All sites hosted by Cloudflare available through their onion services



Onion services legally required for reporting corruption on Web in Italy



The image is a screenshot of a web browser window. The address bar shows the URL <https://blog.torproject.org>. The page title is "Italian Anti-Corruption Authority (ANAC) Adopts Onion Services" in a purple font. Below the title, it says "by steph | February 13, 2018". The main content area features a large black rectangle with a green outline of a Tor onion service icon. Below the image, there is a paragraph of text: "Anonymity technologies are becoming a legal requirement for public agency and corporate anti-corruption compliance."

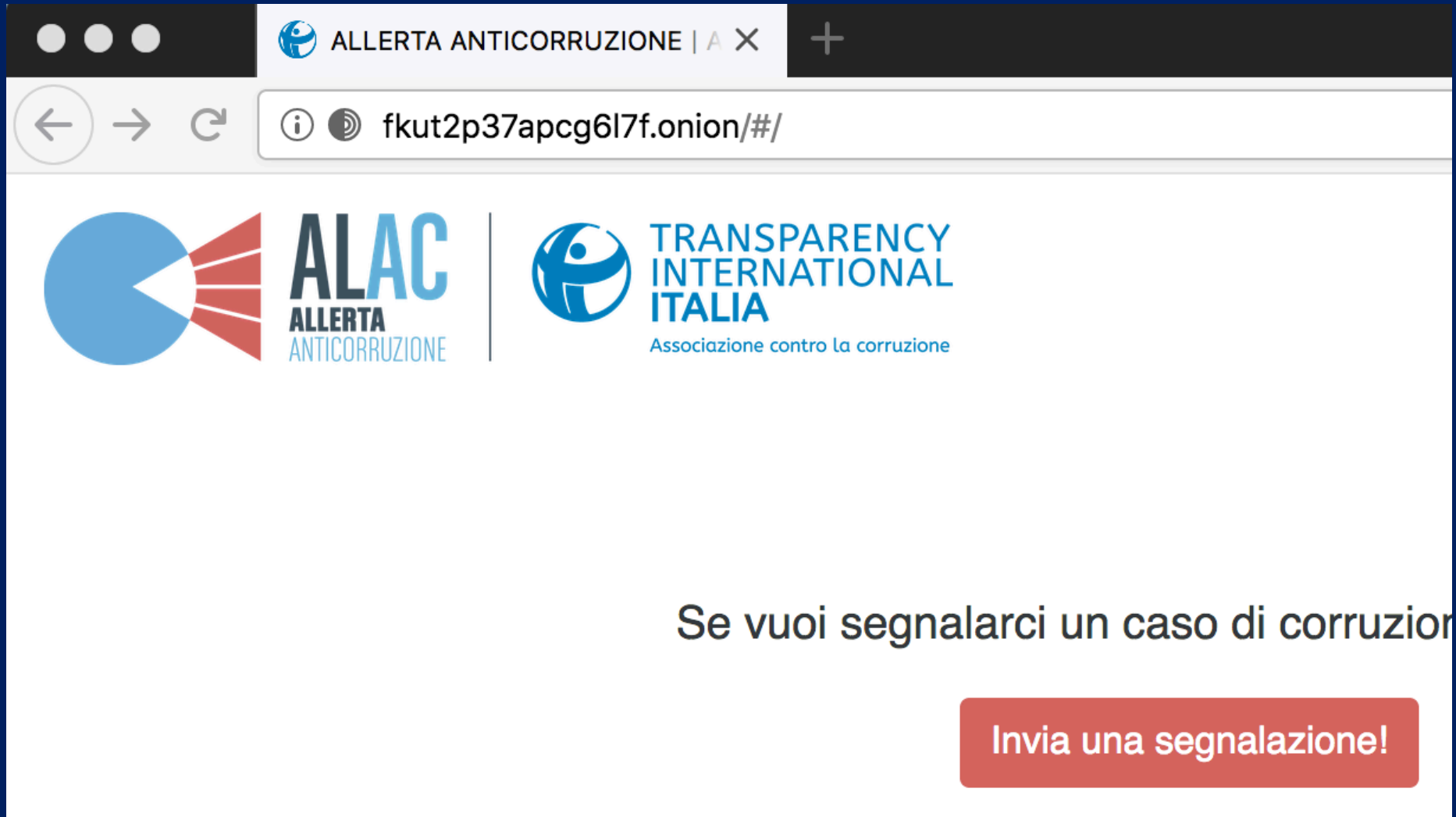
Italian Anti-Corruption Authority (ANAC) Adopts Onion Services

by steph | February 13, 2018



Anonymity technologies are becoming a legal requirement for public agency and corporate anti-corruption compliance.

Onion services legally required for reporting corruption on Web in Italy



The screenshot shows a web browser window with the following elements:

- Browser Tab:** ALLERTA ANTICORRUZIONE | A X
- Address Bar:** fkut2p37apcg6l7f.onion/#/
- Logos:**
 - ALAC ALLERTA ANTICORRUZIONE:** A logo consisting of a blue circle on the left and a red shape resembling a megaphone on the right.
 - TRANSPARENCY INTERNATIONAL ITALIA:** A logo featuring a stylized blue globe with a white figure inside, and the text "TRANSPARENCY INTERNATIONAL ITALIA" and "Associazione contro la corruzione" below it.
- Text:** "Se vuoi segnalarci un caso di corruzione"
- Button:** "Invia una segnalazione!" (Send a report!)

Onionsites, they're not just for web

- Administering systems behind firewalls
- Secure file transfer <https://onionshare.org>
- Securing the Internet of (insecure) things: smarthome

The screenshot shows a web browser window with the address bar displaying <https://www.home-assistant.io/docs/ecosystem/tor/>. The page header includes the Home Assistant logo and navigation links: Getting started, Components, Docs, Examples, Blog, and Need help. The main heading is **// Tor Onion Service Configuration**, with a link to [Edit this page on GitHub](#). The text below the heading reads: "This article guides your through the configuration of Tor to provide a secure access to your Home Assistant inst as an Onion site, through [Tor's Hidden Service](#) feature, from remote. With this enabled, you do not need to oper firewall ports or setup HTTPS to enable secure remote access." Below this is a sub-heading "This is useful if you want to have:" followed by a bulleted list:

- Access your Home Assistant instance remotely without opening a firewall port or setting up a VPN.
- Don't want to or know how to get an SSL/TLS certificate and HTTPS configuration setup.
- Want to block attackers from even being able to access/scan your port and server at all.
- Want to block anyone from knowing your home IP address and seeing your traffic to your Home Assistant

Onion Services Summary

- Not part of the dark web illusion
 - Not where most of the internet crime is
 - Not a subset of the deep web
- Not part of the deep web
 - Already indexed and ranked some
 - Will be indexed/ranked more as that becomes more fruitful
 - Many popular websites available as onion service
- Does give site owners control over address lookup
 - Not subject to DNS hijack
- Does give site owners control over authentication
 - Not subject to TLS Certificate hijack
- Lots of uses, not just for websites

- Part 1: Onion Routing and Tor
 - Background, Motivation, Basic Concepts, Basic Design
- Part 2: How Secure Is It?
 - Network and Adversary Models, Metrics
- Part 3: Onion Services
 - Background, Motivation, Basic Concepts, Basic Design
- Part 4: Self-Authenticating Traditional Addresses (SATAs)
 - Background, Motivation, Basic Concepts, Basic Design

The World Wide Web



- Directed graph: nodes (URLs) and arcs (hyperlinks)
- Lots of security
 - TLS, Browser Security, DNSSEC, Certificate Authorities, CT, ...

The World Wide Web



- Directed graph: nodes (URLs) and arcs (hyperlinks)
- Lots of security
 - TLS, Browser Security, DNSSEC, Certificate Authorities, CT, ...
- That's all U-bolted on, the Web itself has no security built in
- Goal: Cyber-retrofit built-in security for existing less-secure Web

Self-Authenticating Traditional Address (SATA) properties

- Web-embedded Security
- Authority Independence
- Backwards Compatibility
- Dirt Simple Trust

Free Bonus:

- Provide TLS Certificate revocation that
 - is lower overhead than CRLs or OCSP (or OCSP stapling)
 - does not have privacy issues of OCSP
 - does not require interactions with Cert. Authorities at all

Connecting to news and social media



Connecting to news and social media: Hijacked by authorities?

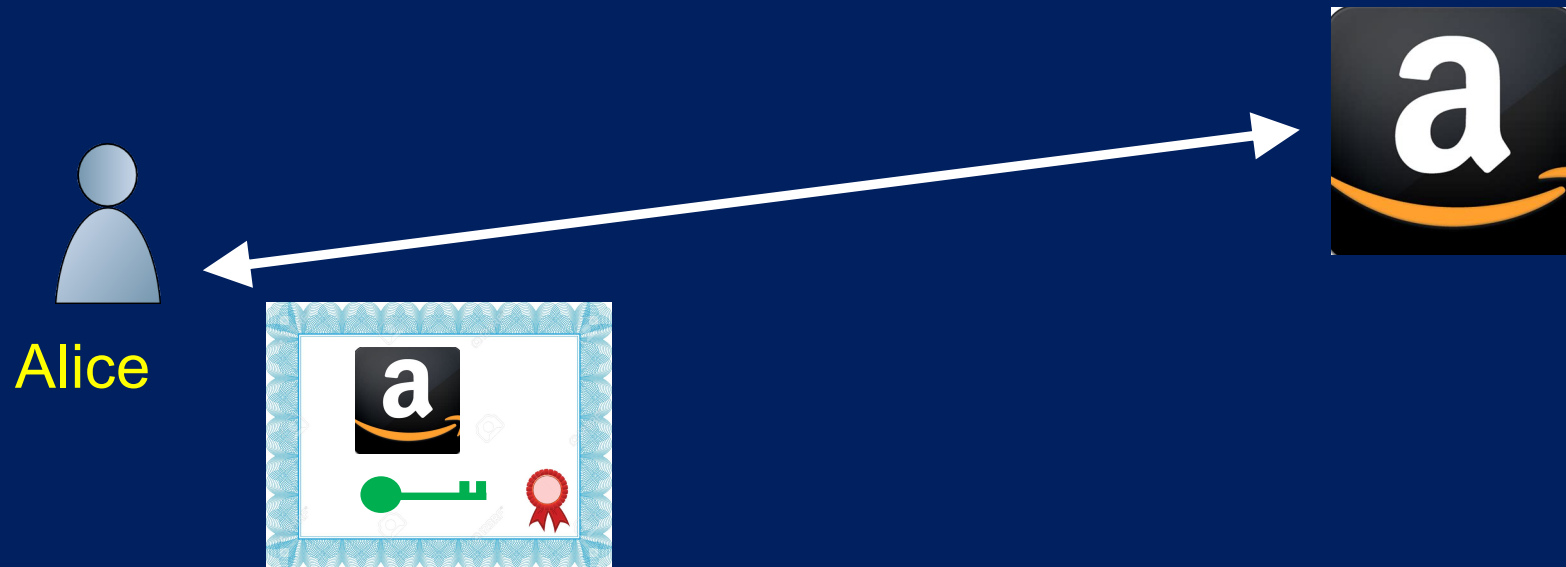


Connecting to commercial sites: Hijacked by criminals?



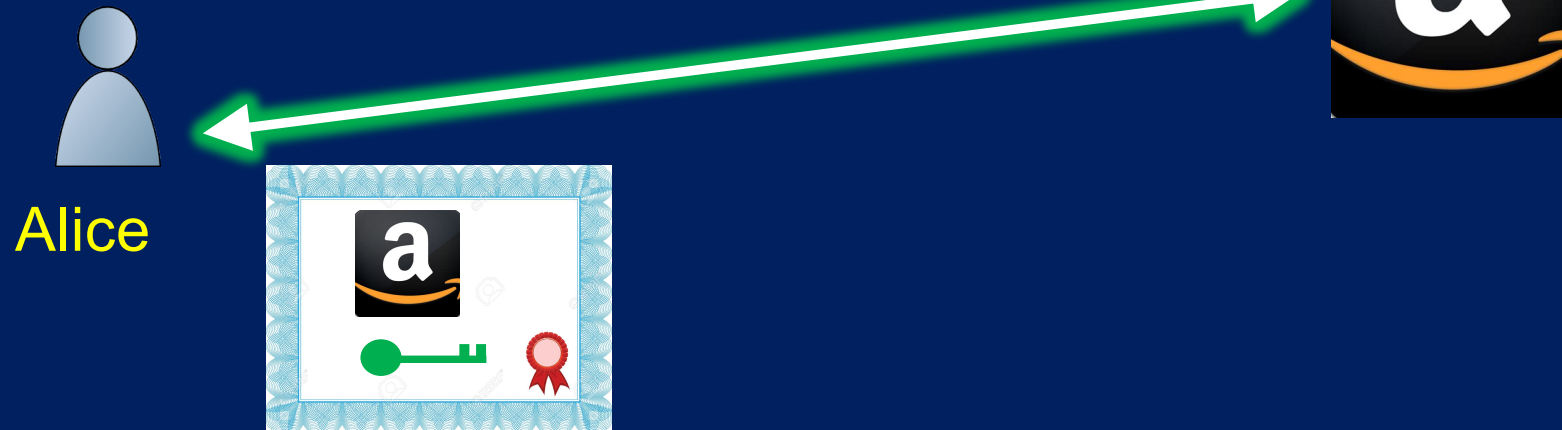
Connecting to commercial sites: Hijacked by criminals?

Alice can be protected with certified TLS authentication



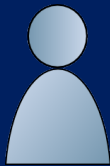
Connecting to commercial sites: Hijacked by criminals?

Alice can be protected with certified TLS authentication



Connecting to commercial sites: Hijacked by criminals?

Alice can be protected with certified TLS authentication, which can also be hijacked



Alice

KrebsonSecurity

In-depth security news and investigation

03 Turkish Registrar Enabled Phishers to Spoof Google

JAN 13



Google and **Microsoft** today began warning users about active phishing attacks against Google's online properties. The two companies said the attacks resulted from a fraudulent digital certificate that was mistakenly issued by a Turkish domain registrar.

In a [blog post](#) published today, Google said that on Dec. 24, 2012, its **Chrome** Web browser detected and blocked an unauthorized digital certificate for the "*.google.com" domain.

"We investigated immediately and found the certificate was issued by an **intermediate certificate authority** (CA) linking back to **TURKTRUST**, a Turkish certificate authority," wrote **Adam Langley**, a Google software engineer. "Intermediate CA certificates carry the full authority of the CA, so anyone who has one can use it to create a certificate for any website they wish to impersonate."



HAVE CERTIFICATE: WILL HACK —

A DNS hijacking wave is targeting companies at an almost unprecedented scale

Clever trick allows attackers to obtain valid TLS certificate for hijacked domains.

DAN GOODIN - 1/10/2019, 8:15 PM






CISA
CYBER+INFRASTRUCTURE

Emergency Directive 19-01

Original Release Date: January 22, 2019

Applies to: All Federal Executive Branch Departments and Agencies, Except for the Department of Defense, Central Intelligence Agency, and Office of the Director of National Intelligence

FROM:

Christopher C. Krebs 
Director, Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

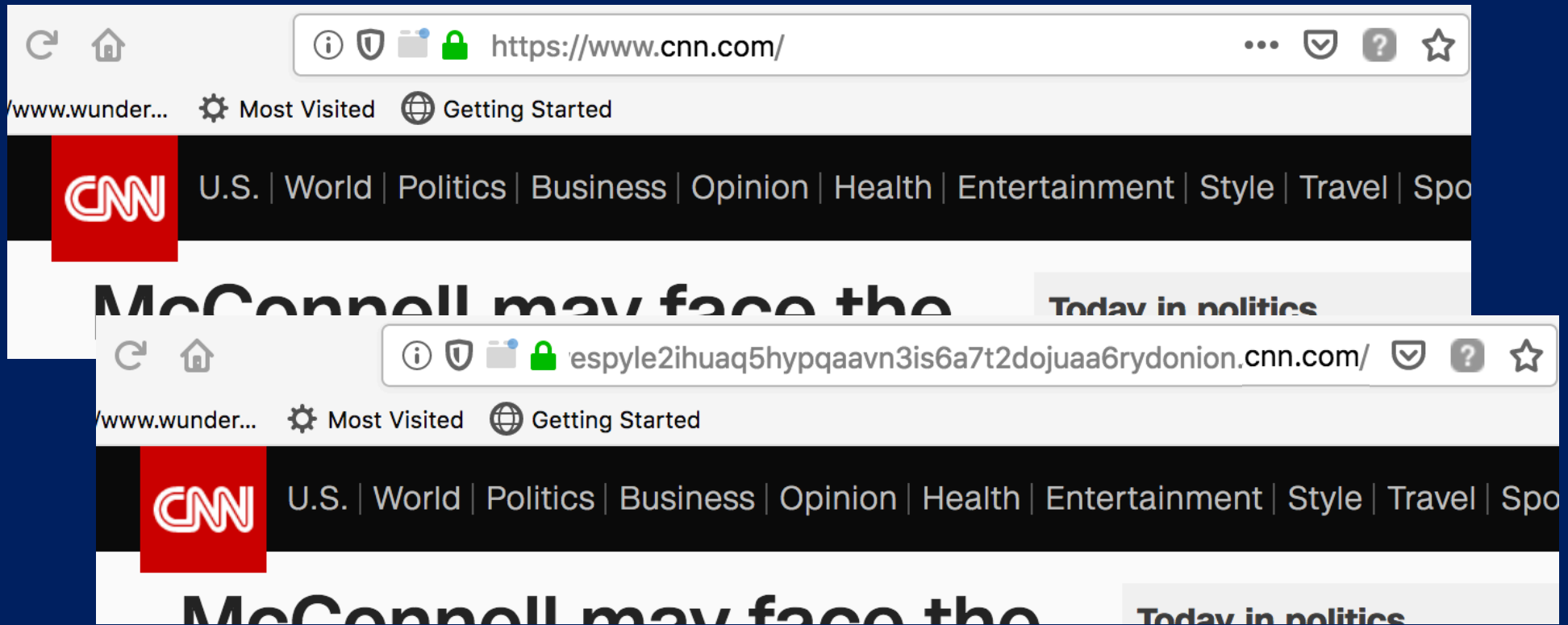
CC:

Russell T. Vought
Director (Acting), Office of Management and Budget

SUBJECT:

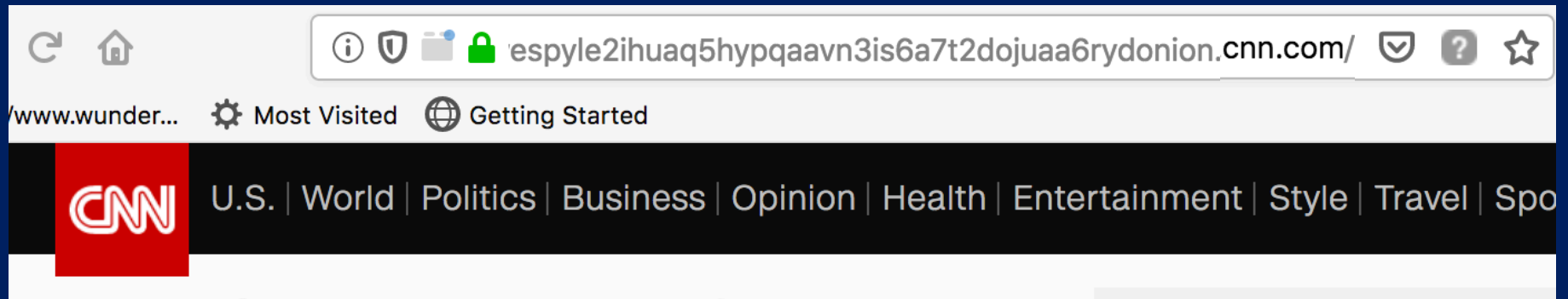
Mitigate DNS Infrastructure Tampering

Embed public key in ordinary domain name



- “Self-authenticating Traditional Domains” Syverson and Traudt. IEEE Secure Development Conference (SecDev) 02019

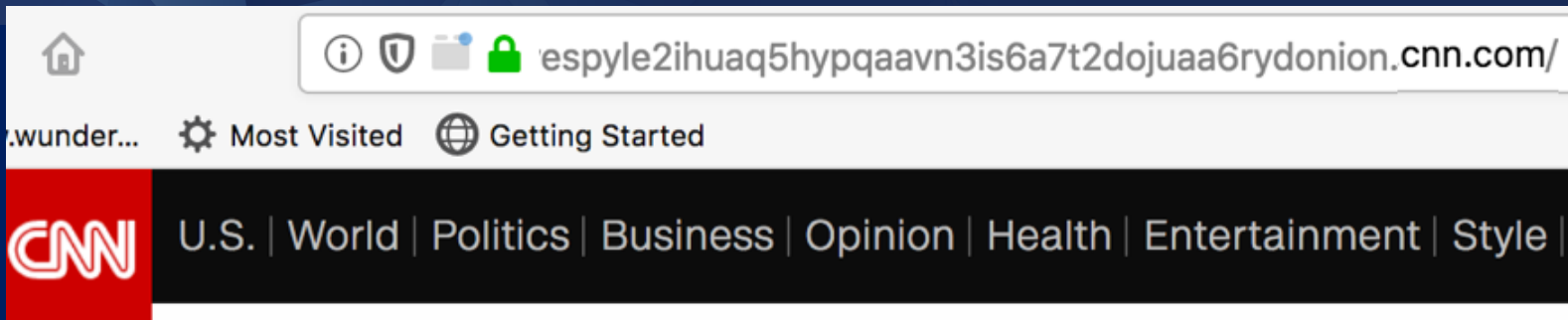
Embed public key in ordinary domain name



espyle2ihuaq5hypqaavn3is6a7t2dojuaa6ryd = Pubkey(CNN)

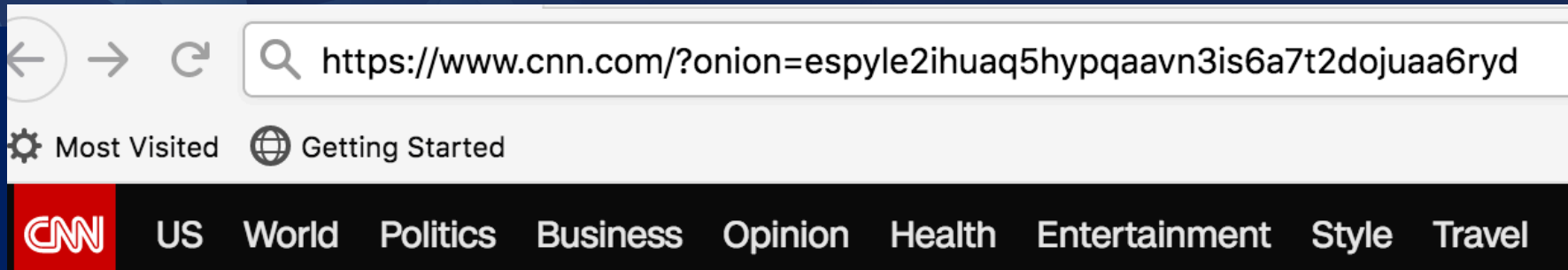
- Self-authenticating
 - Only someone with associated private key can authenticate this address
- Not subject to Certificate hijacks
- Gives site owner control over authentication
 - Authority Independent: Domain can't be usurped by certificate authorities

Backwards compatibility



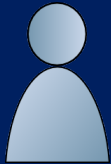
- Self-Authenticating **Traditional** domain names
 - Uses ordinary understood domain names resolvable in DNS
- Can get TLS certificate for SAT domain (DV)
- Don't need separate URL for browsers that check/don't-check self-authentication
- Works in ordinary existing browsers
 - If browser does not know about SAT addresses, performs ordinary security checks from the less-secure Web. (Synergizes with TLS.)

Backwards compatibility more usable



- Self-Authenticating **Traditional** Addresses (SATAs)
 - Uses ordinary understood domain names resolvable in DNS
- Can get TLS certificate for SAT domain (and use for SATA)
- Don't need separate URL for browsers that check/don't-check self-authentication
- Works in ordinary existing browsers
 - If browser does not know about SAT addresses, performs ordinary security checks from the less-secure Web. (Synergizes with TLS.)
- “when examining confusing URL transforms, we found that users were least able to understand URLs with long subdomains/FQDNs.” --- Measuring identity confusion with uniform resource locators, Reynolds et al. ACM CHI 02020

Securely Connecting to a SAT domain

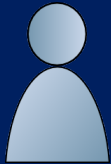


Alice



hllvtjcmneltczwespyle2ihuaq5hypqaavn3is6a7t2dojuaa6rydonion.satis.system33.pw

Securely Connecting to a SAT domain



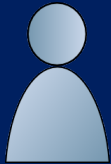
Alice



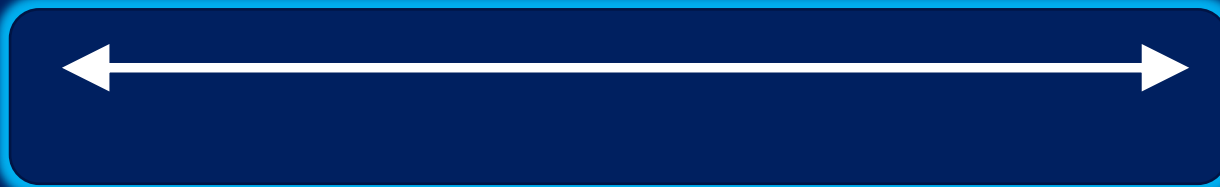
hllvtjcjomneltczwespyle2ihuaq5hypqaavn3is6a7t2dojuaa6rydonion.satis.system33.pw

Securely Connecting to a SAT domain

TLS Handshake



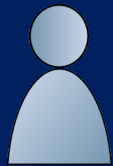
Alice



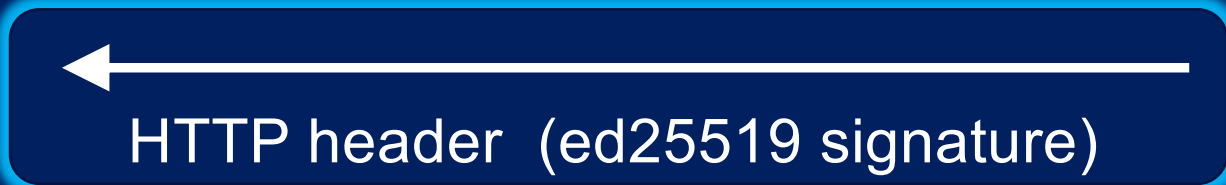
hllvtjcjomneltczwespyle2ihuaq5hypqaavn3is6a7t2dojuaa6rydonion.satis.system33.pw

Securely Connecting to a SAT domain

TLS Connection



Alice

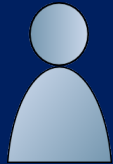


hllvtjcjomneltczwespyle2ihuaq5hypqaavn3is6a7t2dojuaa6rydonion.satis.system33.pw

sign [sk(onion), (timestamp, SAT domain name, TLS-cert fingerprint)]

Securely Connecting to a SAT domain

TLS Connection



Alice



HTTP header (ed25519 signature)

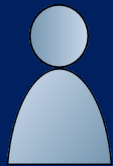


hllvtjcjomneltczwespyle2ihuaq5hypqaavn3is6a7t2dojuaa6rydonion.satis.system33.pw

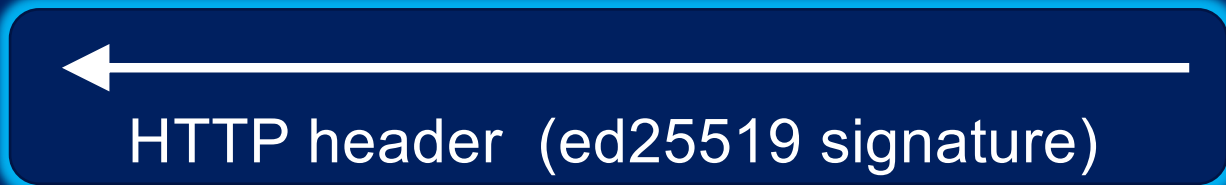
sign [sk(onion), (timestamp, SAT domain name, TLS-cert fingerprint)]

Securely Connecting to a SAT domain

TLS Connection



Alice

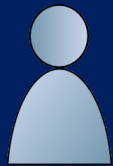


~~nllvtjciomneltczwespyle2ihuaq5hypqaavn3is6a7t2dojuaa6rydonion.satis.system33.pw~~

sign [sk(onion), (timestamp, SAT domain name, TLS-cert fingerprint)]

Securely Connecting to a SAT domain

TLS Connection



Alice



HTTP header (ed25519 signature)



hllvtjcmneltczwespyle2ihuaq5hypqaavn3is6a7t2dojuaa6rydonion.satis.system33.pw

sign [sk(onion), (timestamp, SAT domain name, TLS-cert fingerprint)]

Alice's Browser Extension Checks

1. URL In SAT format?
2. SAT domain included in TLS cert?

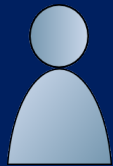
SAT Domain listed alt name (SAN) in Cert

The image shows a web browser window on the left and a Certificate Viewer window on the right. The browser window displays the website identity for `https://hllvtjcmjcomneltczwespile2ihuaq5hypqaavn3is6a7t2dojuaa6rydonion.satis.system33.pw/`. The Certificate Viewer window shows the certificate hierarchy and fields. The 'Certificate Subject Alt Name' field is circled in red, showing the following values:

```
Not Critical
DNS Name:
hllvtjcmjcomneltczwespile2ihuaq5hypqaavn3is6a7t2dojuaa6rydonion.satis.system33.pw
DNS Name:
hllvtjcmjcomneltczwespile2ihuaq5hypqaavn3is6a7t2dojuaa6rydonion.satis.system33.pw
DNS Name: satis.system33.pw
```

Securely Connecting to a SAT domain

TLS Connection



Alice



HTTP header (ed25519 signature)



hllvtjcmneltczwespyle2ihuaq5hypqaavn3is6a7t2dojuaa6rydonion.satis.system33.pw

sign [sk(onion), (timestamp, SAT domain name, TLS-cert fingerprint)]

Alice's Browser Extension Checks

1. URL In SAT format?
2. SAT domain included in TLS cert?
3. HTTP header signed by ed25519 key from SAT domain name?
4. Current time within signature validity window?
5. Visited URL = SAT domain named in ed25519 signature?
6. TLS-cert fingerprint same as in signed header?

What if a WebExt check fails?

Extension (SAT Domain Tools) | moz-extension://b7c3cf0e-51 ... Search

d

Oh no! Something went wrong.

The fingerprint in the TLS cert doesn't match the one in the SAT HTTP header.

Validity period

Not before	Sun Feb 17 2019 22:20:56 GMT-0500 (Eastern Standard Time)
Not after	Sun Feb 24 2019 22:20:56 GMT-0500 (Eastern Standard Time)
Current time	Fri Feb 22 2019 01:30:39 GMT-0500 (Eastern Standard Time)

TLS Certificate

In use	E11073AE3A38C644AAE26FE4F25C194D3E6A0C85219F02F5150B401E09FC4B7C
Expected	DEADBEEF111111111111

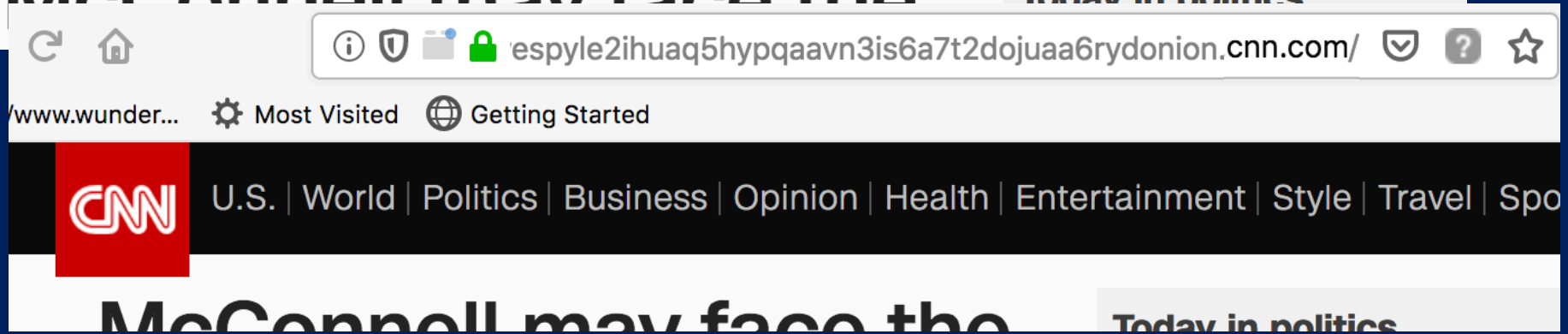
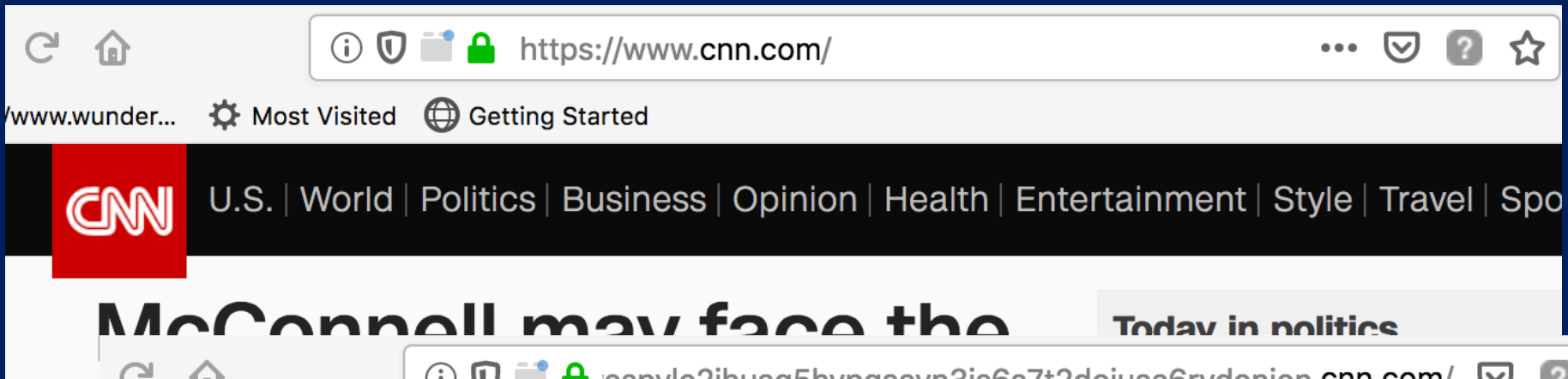
Domain Name

Visiting	hllvtjcjomneltczwespile2ihuaq5hypqaavn3is6a7t2dojuaa6rydonion.satis.system33.pw
Expected	hllvtjcjomneltczwespile2ihuaq5hypqaavn3is6a7t2dojuaa6rydonion.satis.system33.pw

Connecting to news and social media: Hijacked by authorities?



Embed public key in ordinary domain name

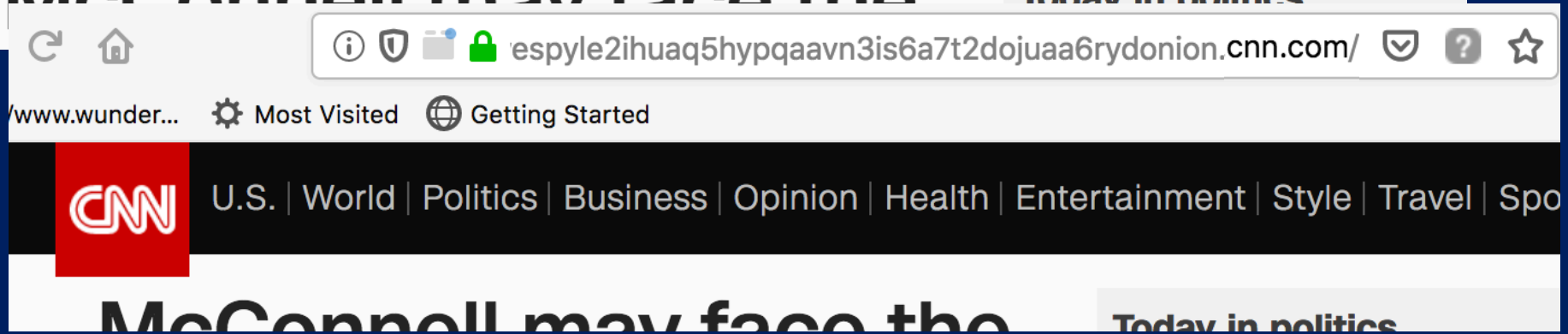
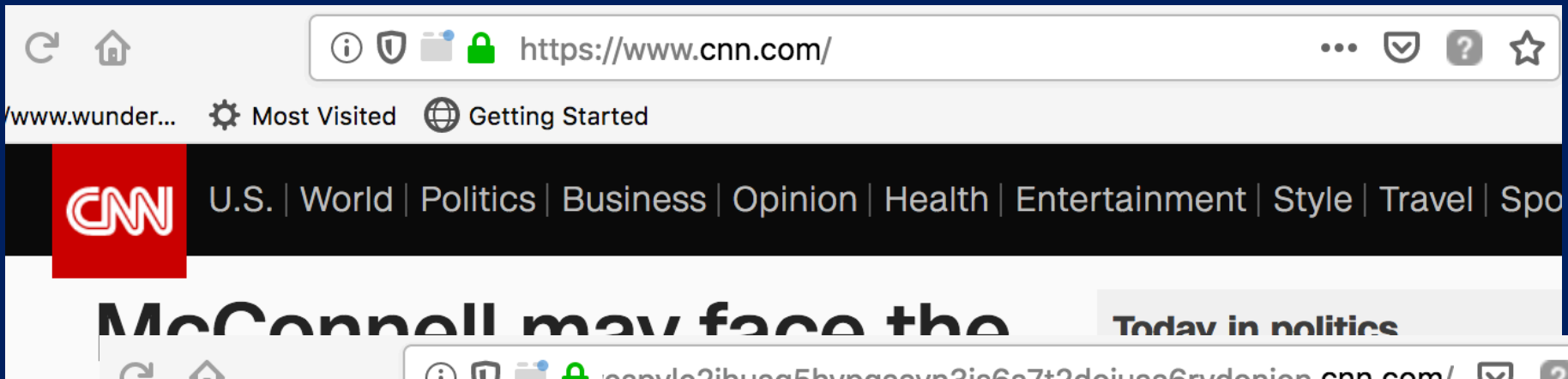


Connecting to news and social media: Hijacked by authorities?

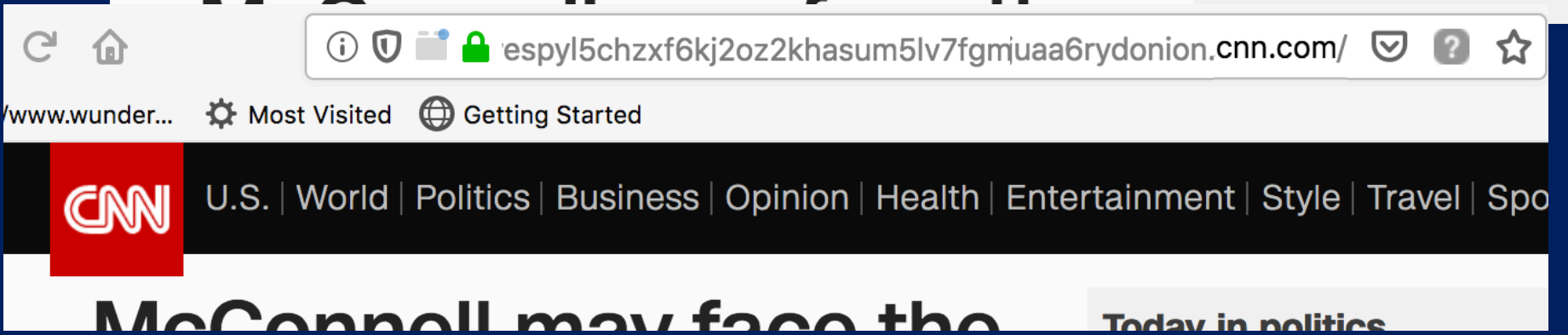
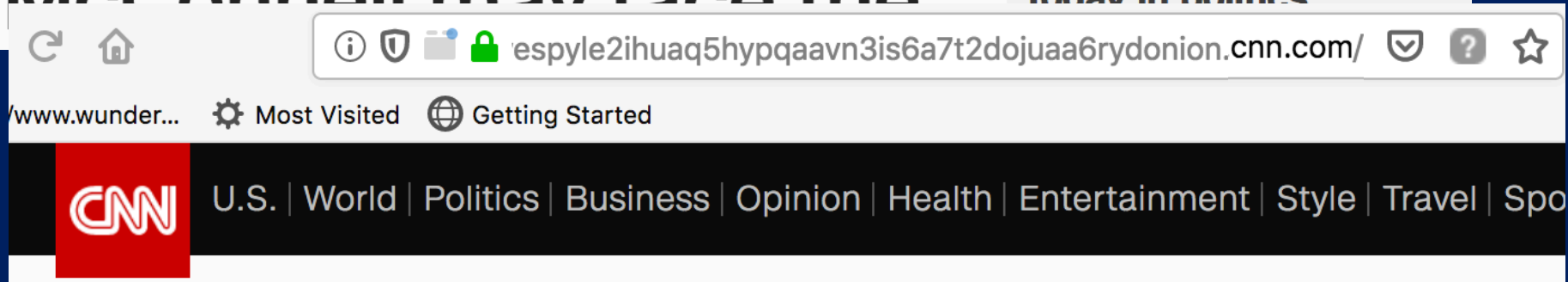
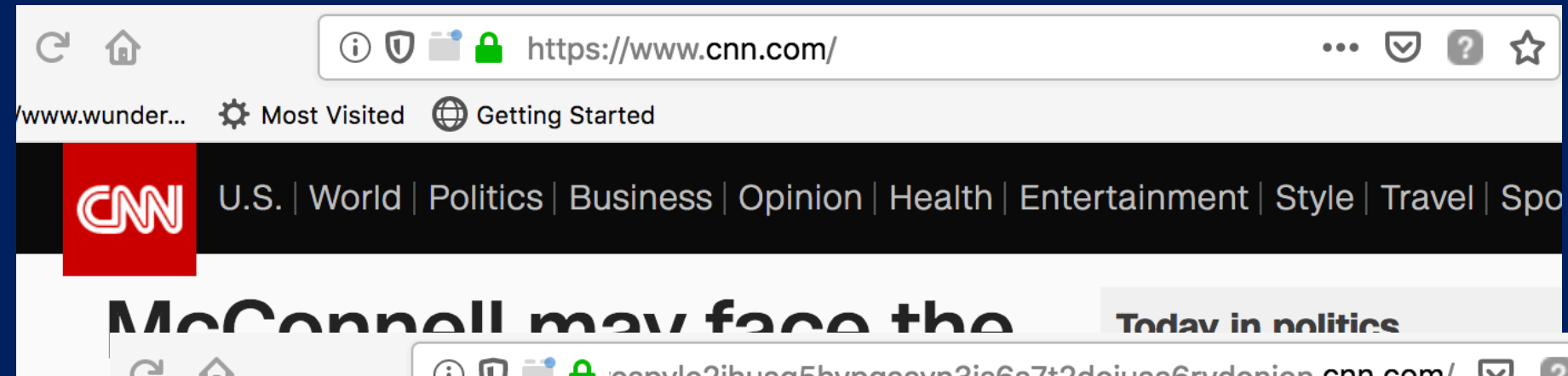


- Alice cannot be tricked to accept hijacked cert for SAT sites

Embed public key in ordinary domain name



Embed public key in ordinary domain name



Connecting to news and social media: Hijacked by authorities?



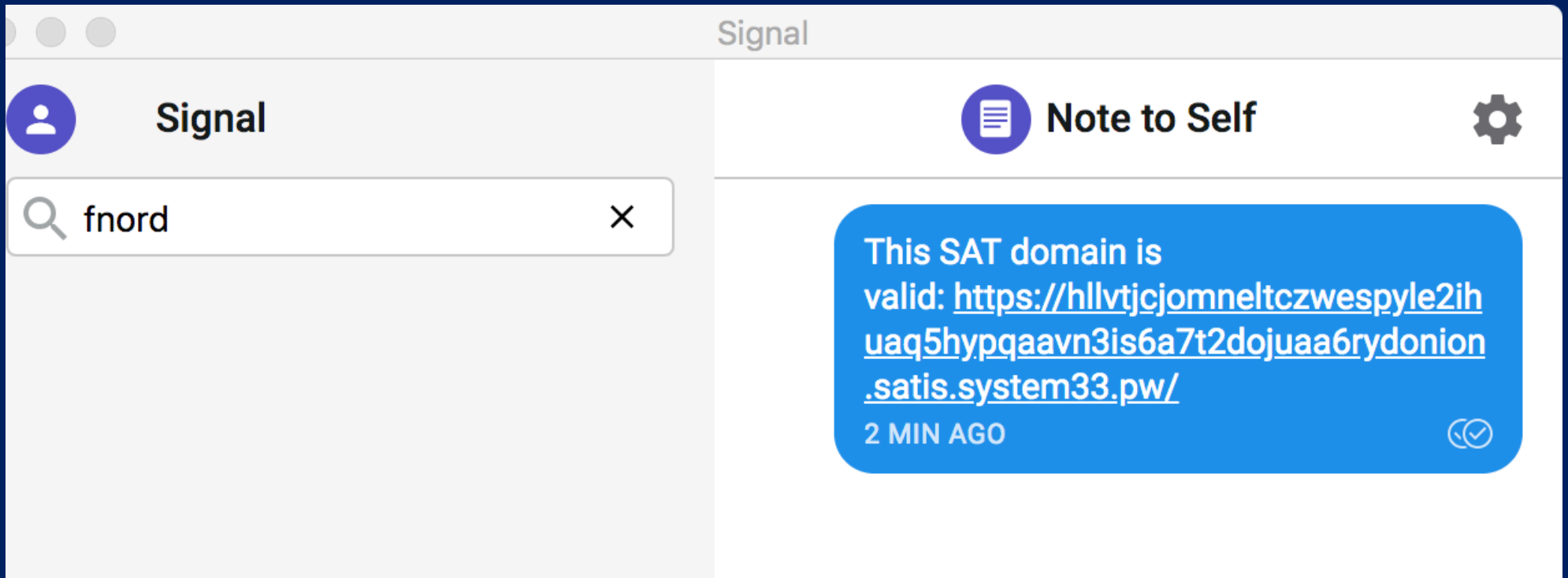
- Alice cannot be tricked to accept hijacked cert for SAT sites
- Alice can still be tricked to accept cert for SAT sites
 - With hijacked cert
 - With doppelganger self-auth subdomain
- Solution: SAT domains support Dirt Simple Trust

Dirt Simple Trust

- Receiving an address from someone you trust is all you need for a validated hijack resistant connection

Dirt Simple Trust

- Receiving an address from someone you trust is all you need for a validated hijack resistant connection



Dirt Simple Trust

- Receiving an address from someone you trust is all you need for a validated hijack resistant connection
- Written on a business card
- Sent in a signal message
- Sent in a PGP signed message
- Etc.

Connecting to news and social media: Hijacked by authorities?



- Alice trusts Tom
- Tom sends validated SAT domains to Alice via auth. channel
- Alice can still be tricked to accept cert for SAT sites?
 - With hijacked cert
 - With doppelganger self-auth subdomain

Connecting to news and social media: Not hijacked by authorities



- Alice trusts Tom
- Tom sends validated SAT domains to Alice via auth. channel
- Alice cannot still be tricked to accept cert for SAT sites
 - With hijacked cert
 - With doppelganger self-auth subdomain

Connecting to news and social media: Not hijacked by authorities



- Alice trusts Tom
- Tom sends validated SAT domains to Alice via auth. channel
- Alice cannot still be tricked to accept cert for SAT sites
 - With hijacked cert
 - With doppelganger self-auth subdomain
- What about scaling up? What about updates? What about keeping track of trust?

Dirt Simple Trust: Sattestation

- Receiving an address from someone you trust is all you need for a validated hijack resistant connection
- Written on a business card
- Sent in a signal message
- Sent in a PGP signed message
- Etc.
- Sent in **sattestation** header from trusted sattestor destination
 - Client and server software have been implemented

Sattestation scaling and automation

- DHS, GSA, or ? runs sattestation site for any .gov and .mil SAT domains.
- SAT domains cannot be hijacked for any client trusting U.S. Govt. sattestor.

U.S. Department of Homeland Security
Washington, DC 20528



Emergency Directive 19-01
Original Release Date: January 22, 2019
Applies to: All Federal Executive Branch Departments and Agencies, Except for the Department of Defense, Central Intelligence Agency, and Office of the Director of National Intelligence

FROM: Christopher C. Krebs 
Director, Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

CC: Russell T. Vought
Director (Acting), Office of Management and Budget

SUBJECT: **Mitigate DNS Infrastructure Tampering**

- Mandating use of browsers checking attestation for government employees/contractors also guards against system breaches, data or credential theft, etc.

Sattestation: other example use cases

- Personal friends for whatever you trust them about
- Media reliability/safety org can sattest news & media sites:
Freedom of the Press Foundation, Berkman-Klein Center, etc.
- DHS or GSA or ... for all .gov and .mil domains
- Corporation for sites it owns:
Microsoft for microsoft.com, microsoftonline.com, live.com, office.com, office.net, etc.
- Corporate or government enterprises for internal sites not meant for public access
Employees working remotely can't be tricked into accepting the wrong VPN or portal and leak sensitive customer data

TLS Certification

- Structural
- Global
- Does not scale down well

PGP Web of Trust

- Local
- Structural
 - Assigned degree of trust, weighted sum of trust values
- Does not scale up well

Sattestation design intended for contextual trust

- Scales across local-global range
 - Scales up (e.g. all of .gov and .mil)
 - Scales down (e.g. sites Tom says are good)
- Context could just be structural
 - CAs could offer sattestation sites
 - Users/organizations can decide which CAs to trust for sattestation while still trusting any valid CA for TLS certs

SATA Summary

- SAT addresses counter certificate hijack
- Client & Server code at satis.system33.pw and github (along with demo videos, etc.)
- Run a SATA site of your own please!
- SATAs enable Dirt Simple Trust
- SATAs compatible with any browser, not Tor only
- Sattestation: scalable, contextual basis for trust
- SAT addresses weave security into fabric of Web
- SATAs provide TLS Cert revocation cheaper and more securely than existing mechanisms

- Part 1: Onion Routing and Tor
 - Background, Motivation, Basic Concepts, Basic Design
- Part 2: How Secure Is It?
 - Network and Adversary Models, Metrics
- Part 3: Onion Services
 - Background, Motivation, Basic Concepts, Basic Design
- Part 4: Self-Authenticating Traditional Addresses (SATAs)
 - Background, Motivation, Basic Concepts, Basic Design

Main take-aways

- Tor and onion services are primarily just ways to access ordinary internet sites more securely.
- They are today where web encryption (https) was around 02001.
- There are no stupid questions: please ask.