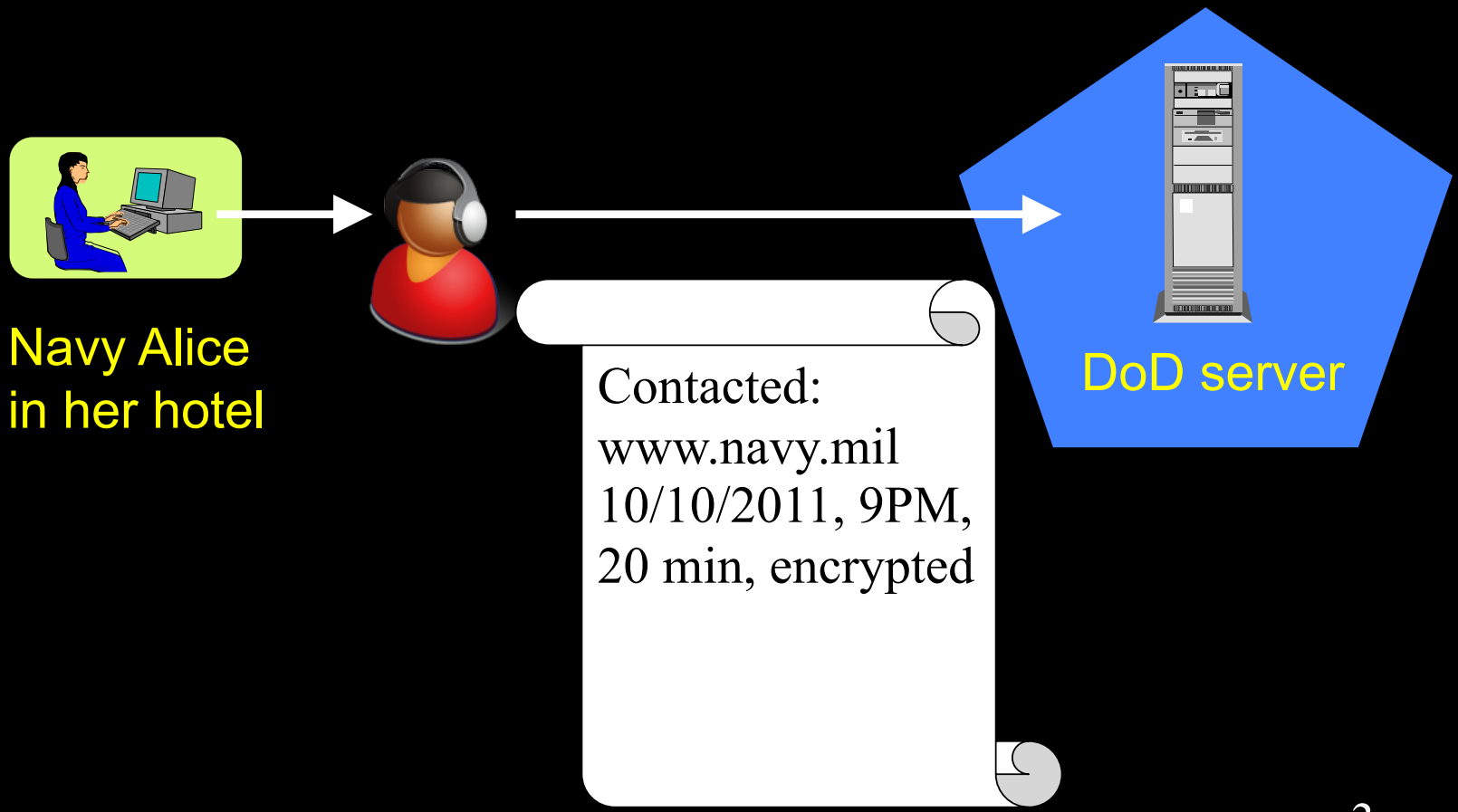
Onion Routing 101 and Trust for Traffic Security Resilience

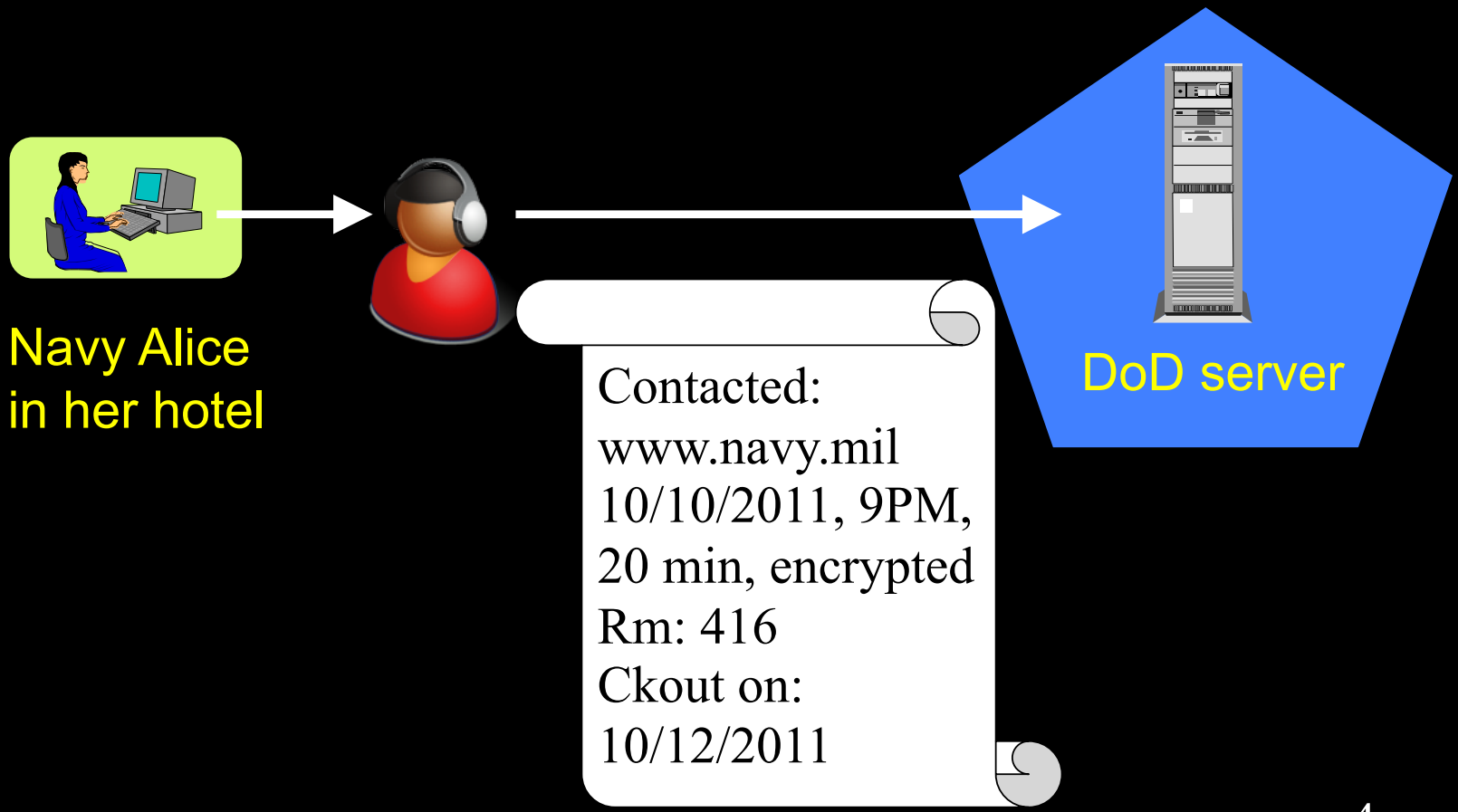
Paul Syverson
U.S. Naval Research Laboratory
Center for High Assurance Computer Systems

Checking in to work from overseas

Checking in to work from overseas



Checking in to work from overseas



Practical questions

How can we protect “road warriors” and their missions and activities?

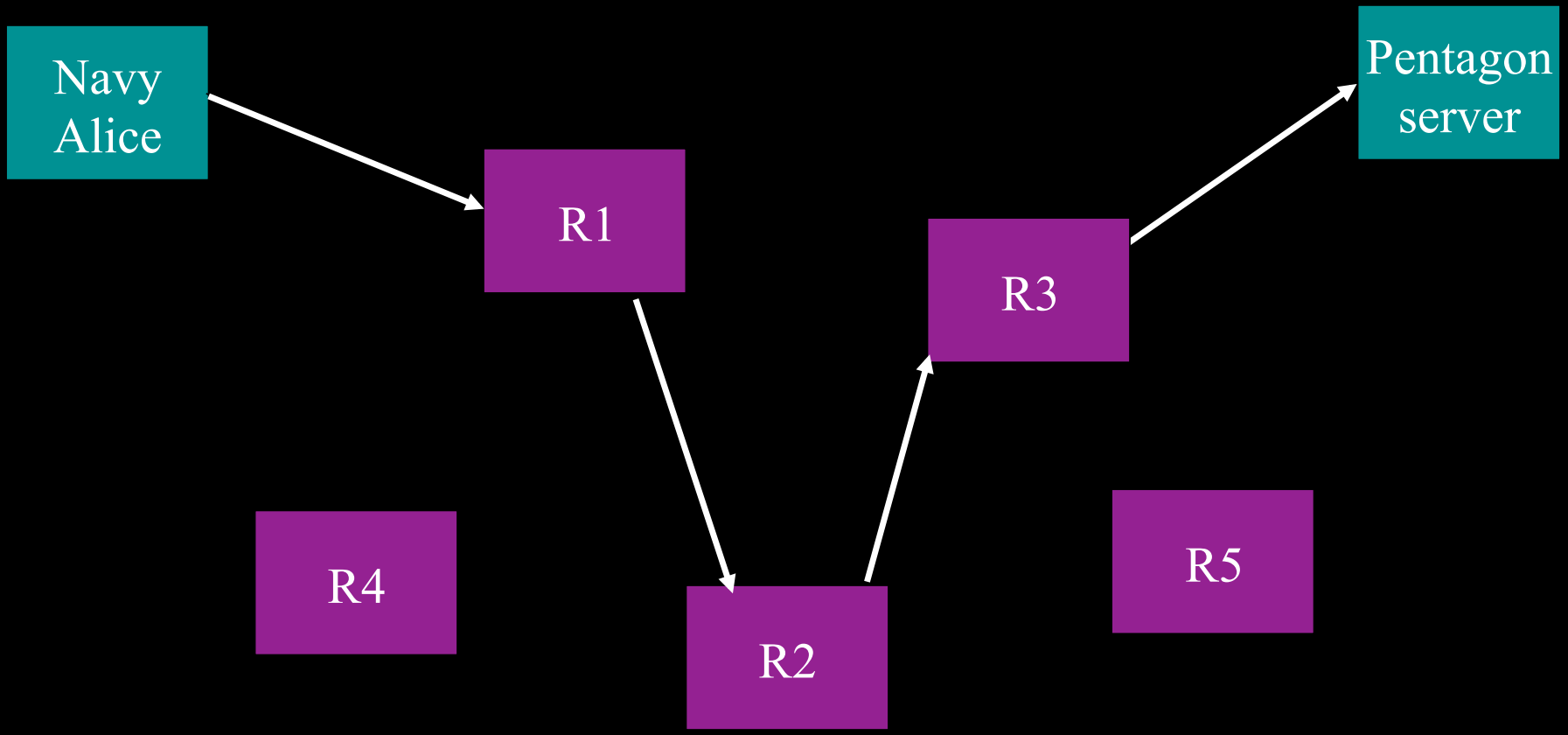
How can we protect sensitive communication via public networks, such as open source intelligence gathering?

Technical Goal: Separate Identification from Routing

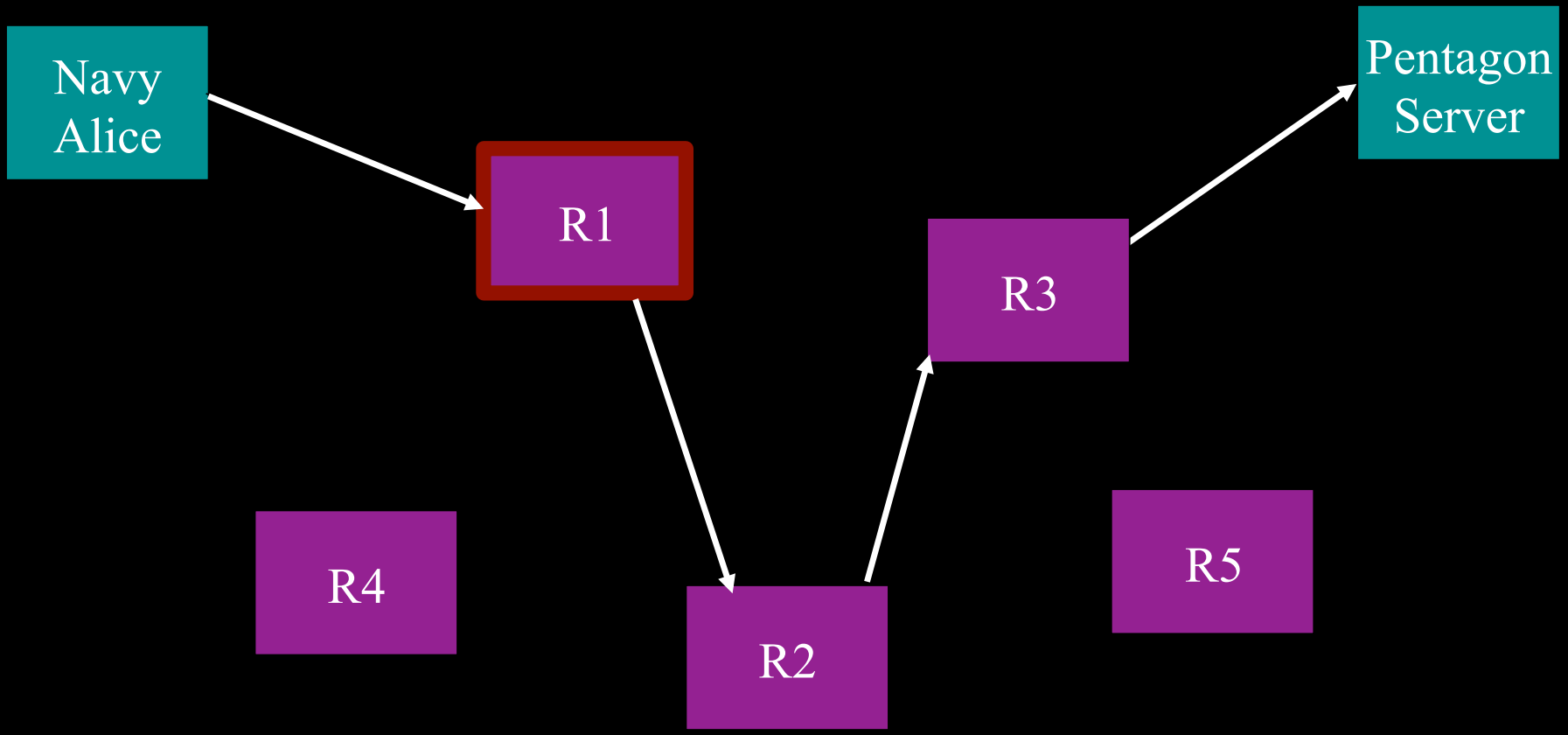
Onion routing separates identification from routing by bouncing communication around the network

Cryptography makes sure each computer in the connection only knows about adjacent computers

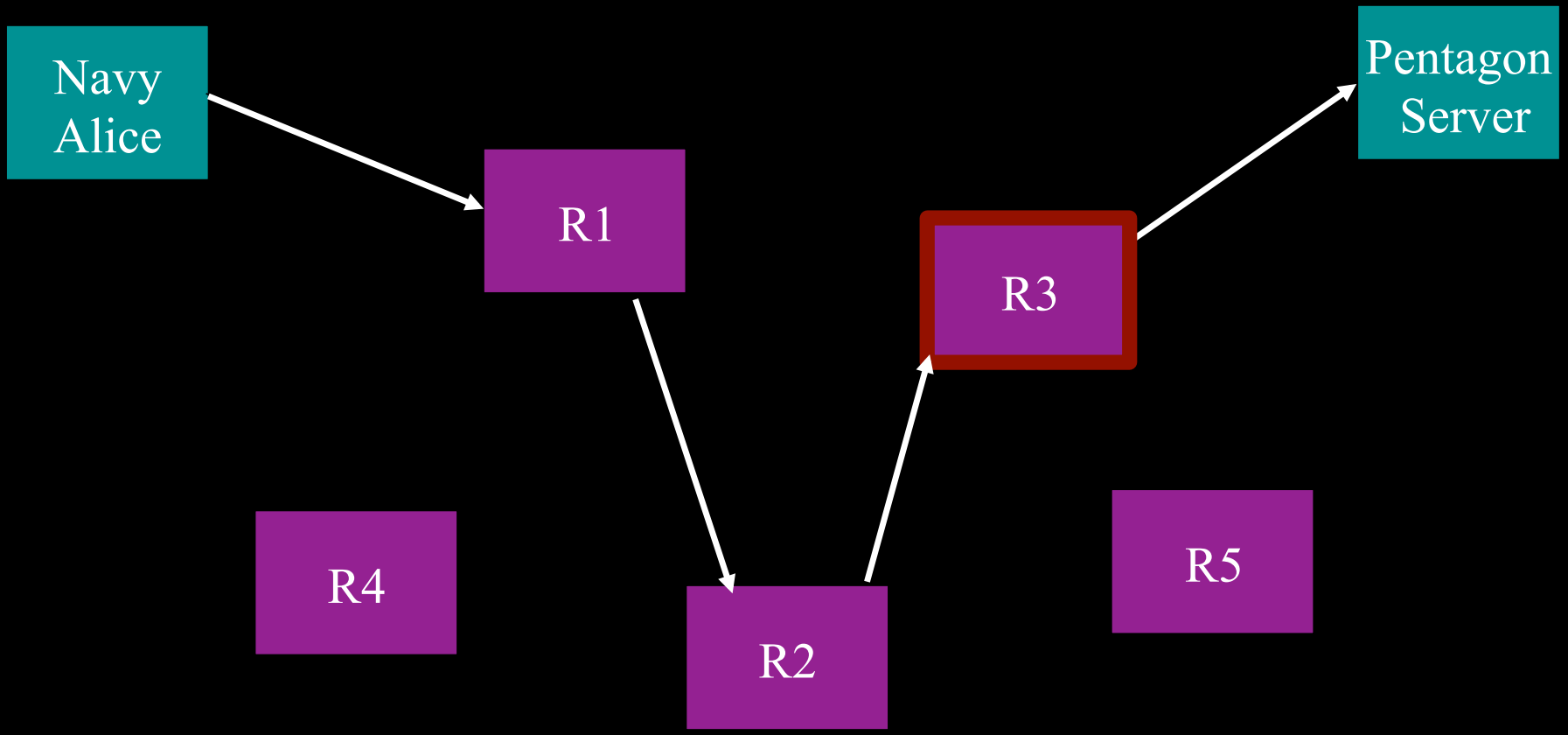
Onion routing bounces Alice's communication around the network



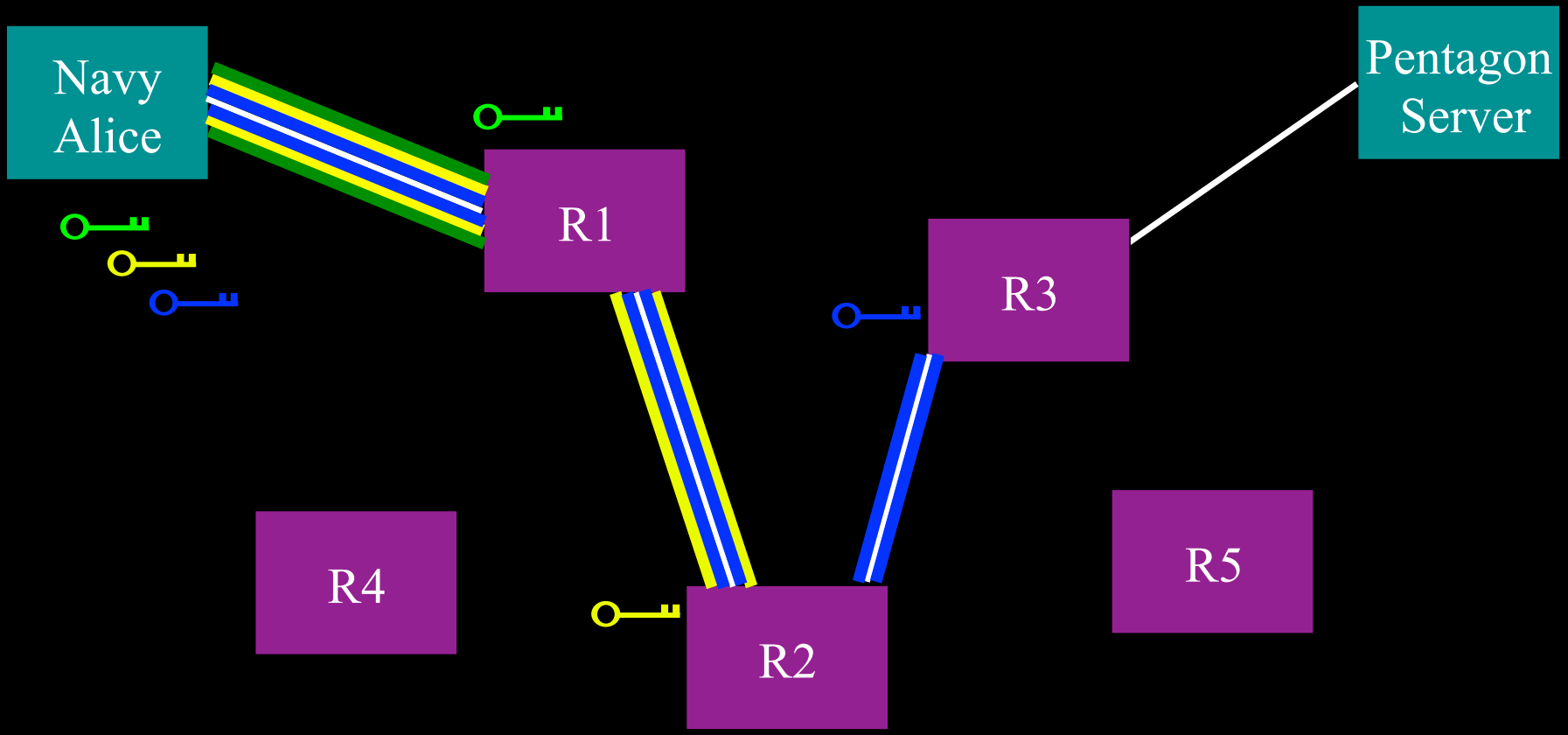
A corrupt first hop can tell that Alice is talking, but not to whom



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



Onion encryption makes communication look different at each point in the route



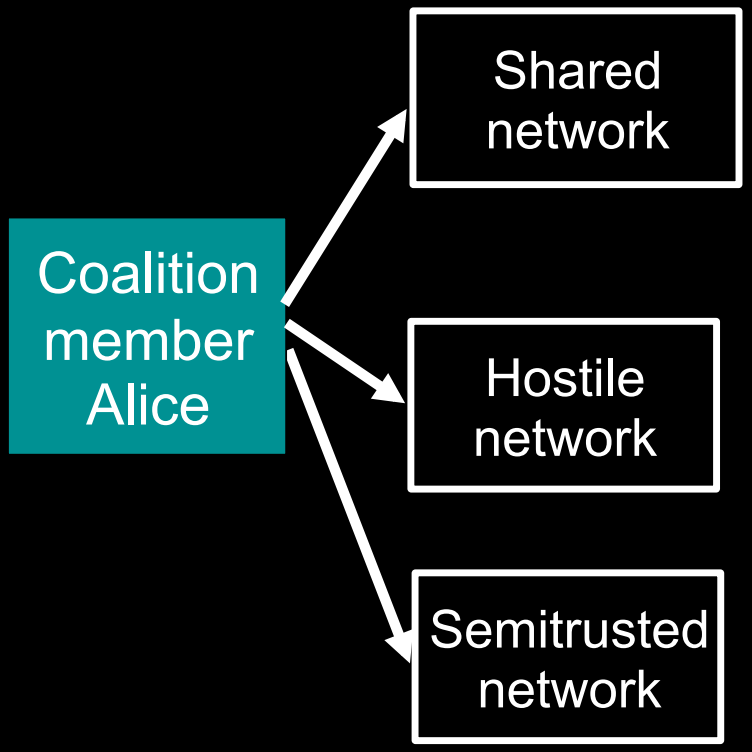
DoD threats countered by onion routing

"What will you bid for a list of Baghdad IP addresses that get email from .gov?"

"What bid for the hotel room from which someone just logged in to foo.navy.mil?"

"What *does* the DIA Google for?"

DoD threats countered by onion routing



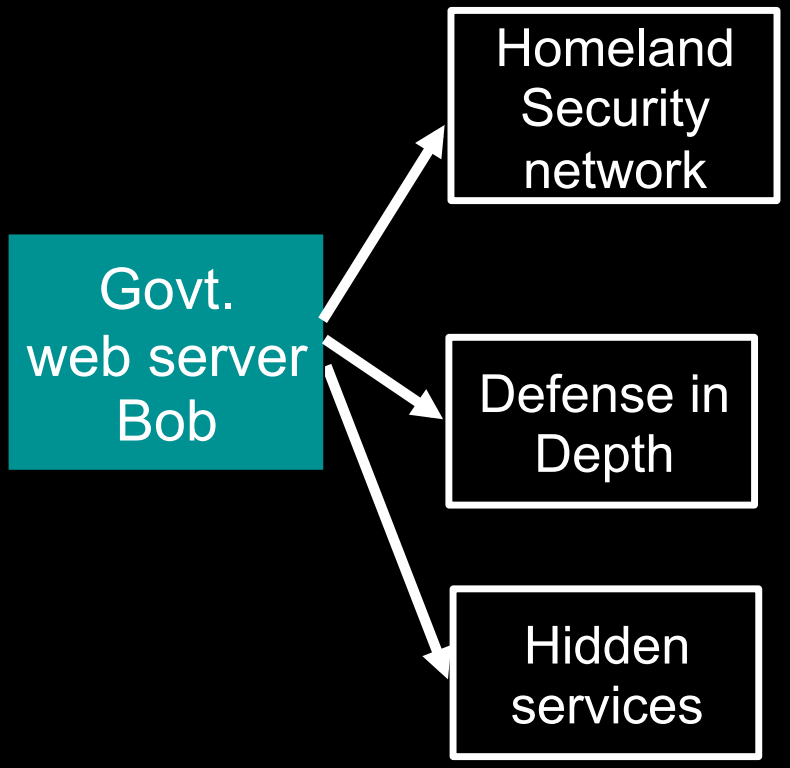
"Do I really want to reveal my internal network topology?"

"Do I want all my partners to know extent/pattern of my comms with other partners?"

"How can I establish communication with locals without a trusted network?"

"How can I avoid selective blocking of my communications?"

DoD threats countered by onion routing



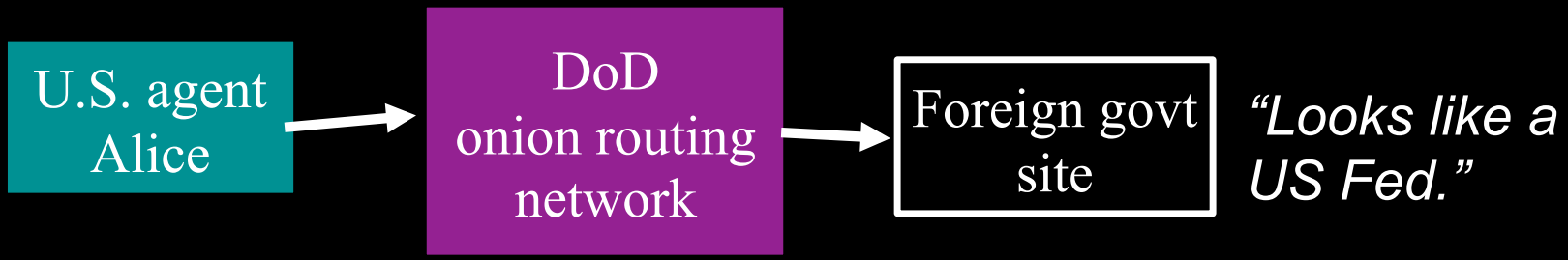
"How can I securely and quickly exchange vital info with every sheriff's dept and Hazmat transporter without bringing them into my secure network?"

"Do I want every SIPRNET node to know where all the traffic on it is headed?"

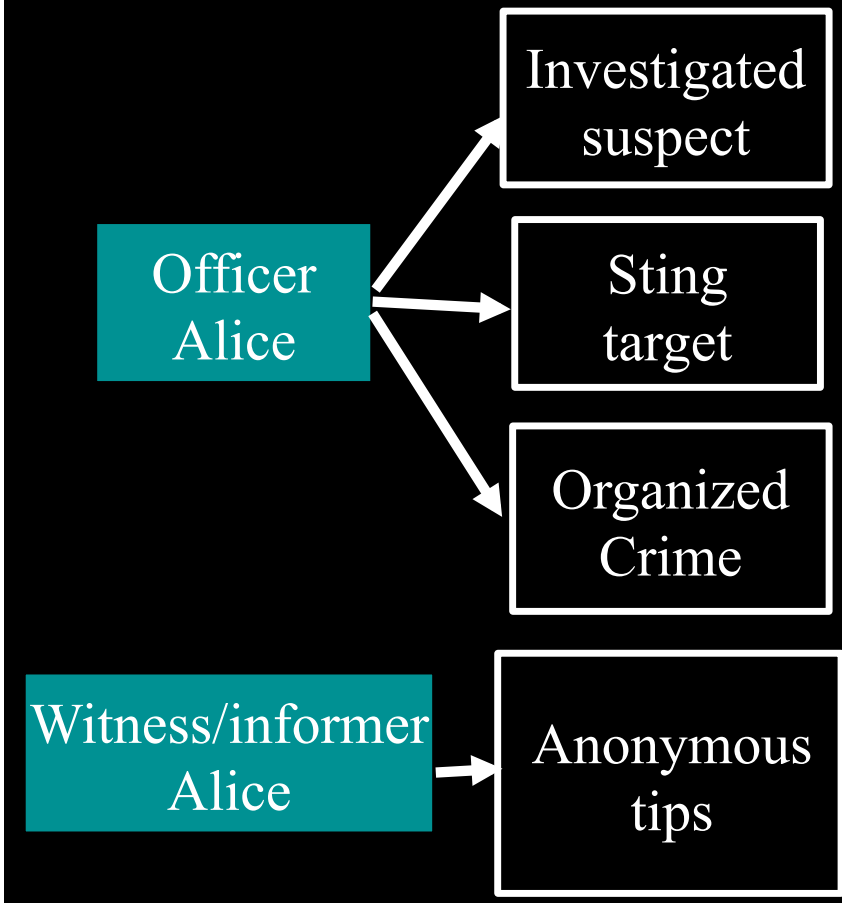
"Can I hide where my MLS chat server/my automated regrader is?"

Can my servers resist DDoS and physical attack even by authorized users?"

You can't be anonymous by yourself: private solutions are ineffective...



Law enforcement also needs anonymity to get the job done



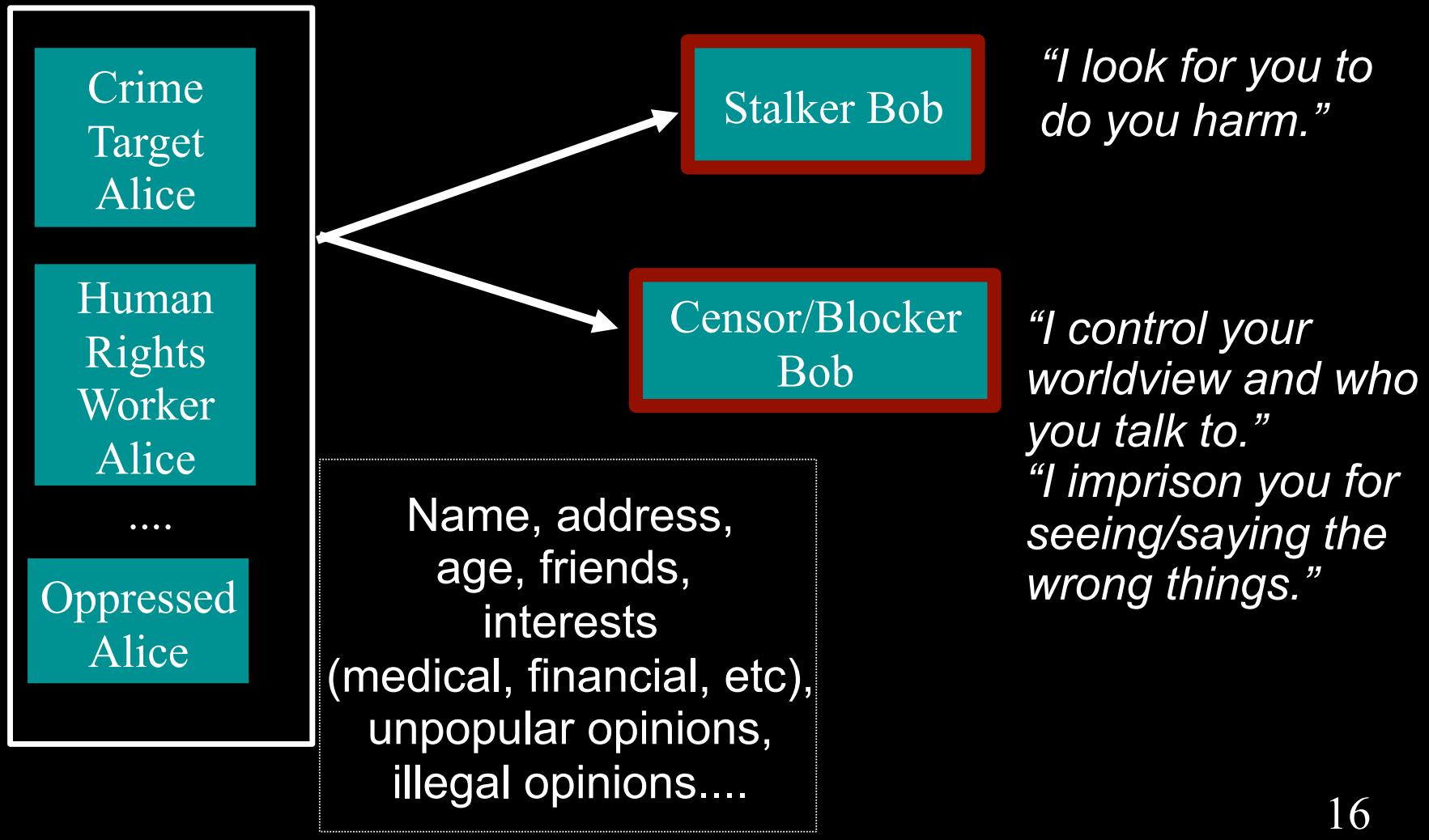
"Why is alice.fbi.gov reading my website?"

"Why no, alice.localpolice.gov! I would never sell counterfeits on ebay!"

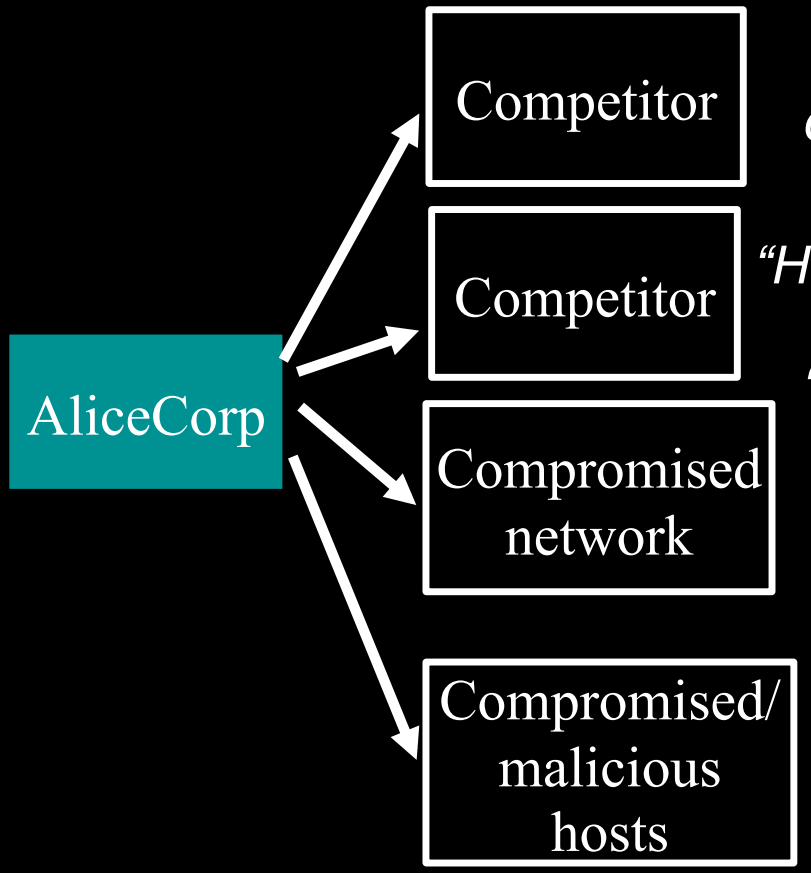
"Is my family safe if I go after these guys?"

"Are they really going to ensure my anonymity?"

Regular citizens don't want to be watched and tracked



Businesses need to protect trade secrets... and their customers



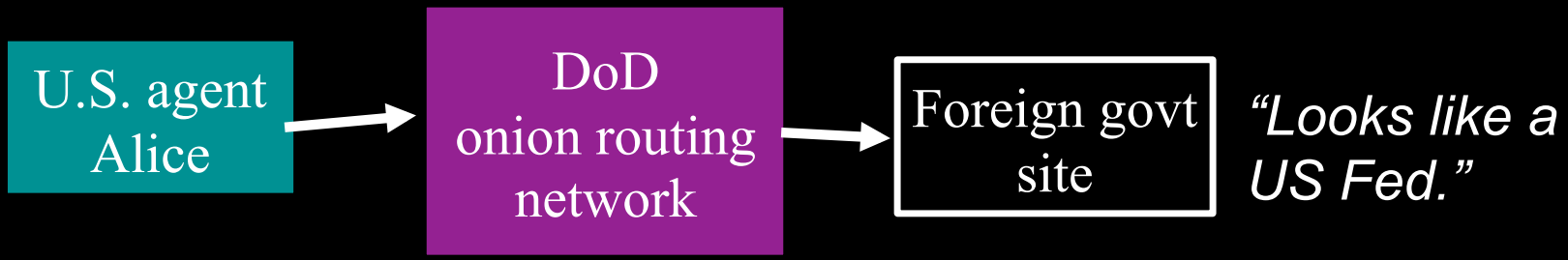
"Oh, your employees are reading our patents/jobs page/product sheets?"

"Hey, it's Alice! Give her the 'Alice' version!"

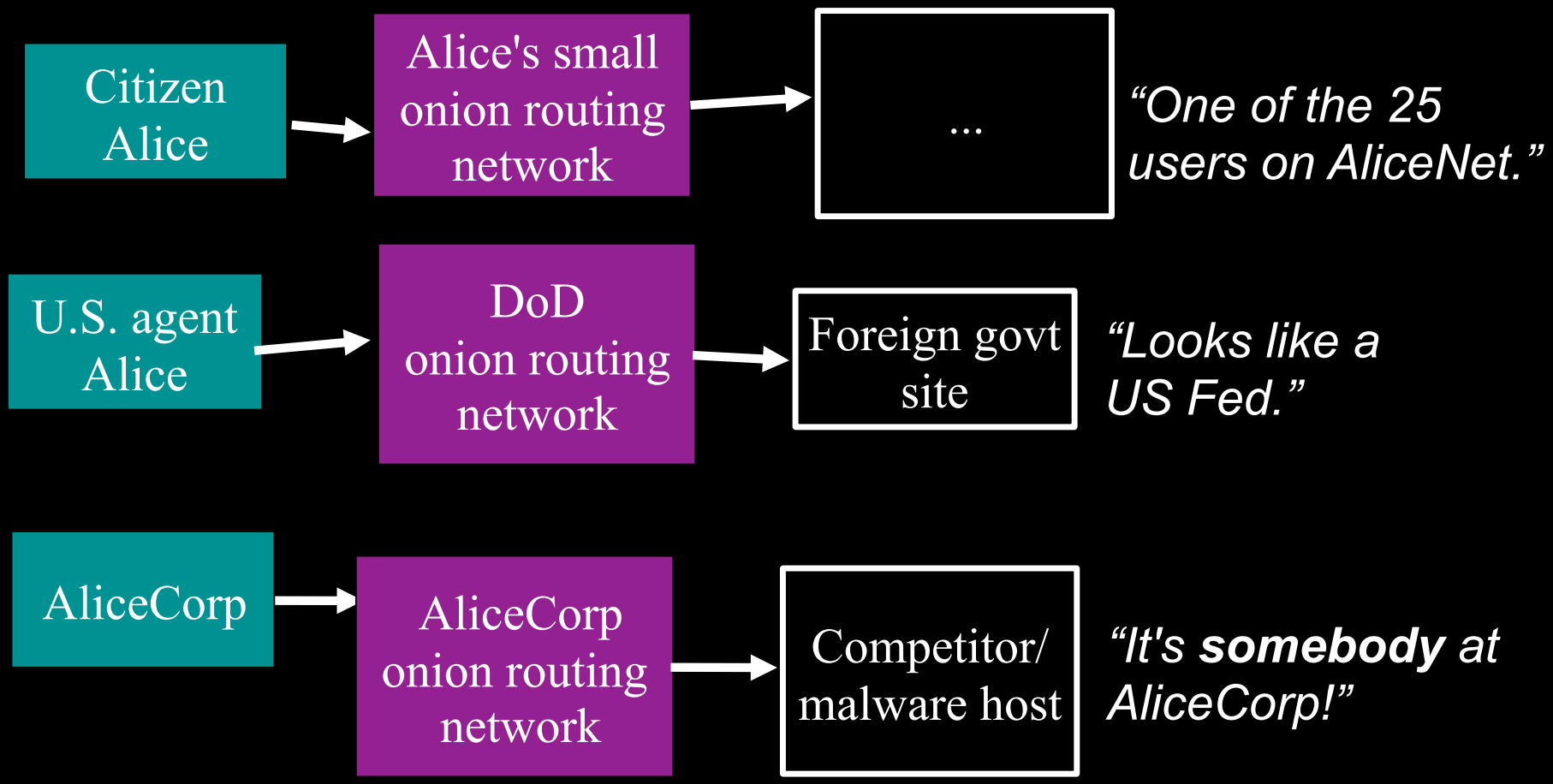
"Wanna buy a list of Alice's suppliers? What about her customers? What about her engineering department's favorite search terms?"

"We attack Alice's customers with malware, and watch for when she notices us."

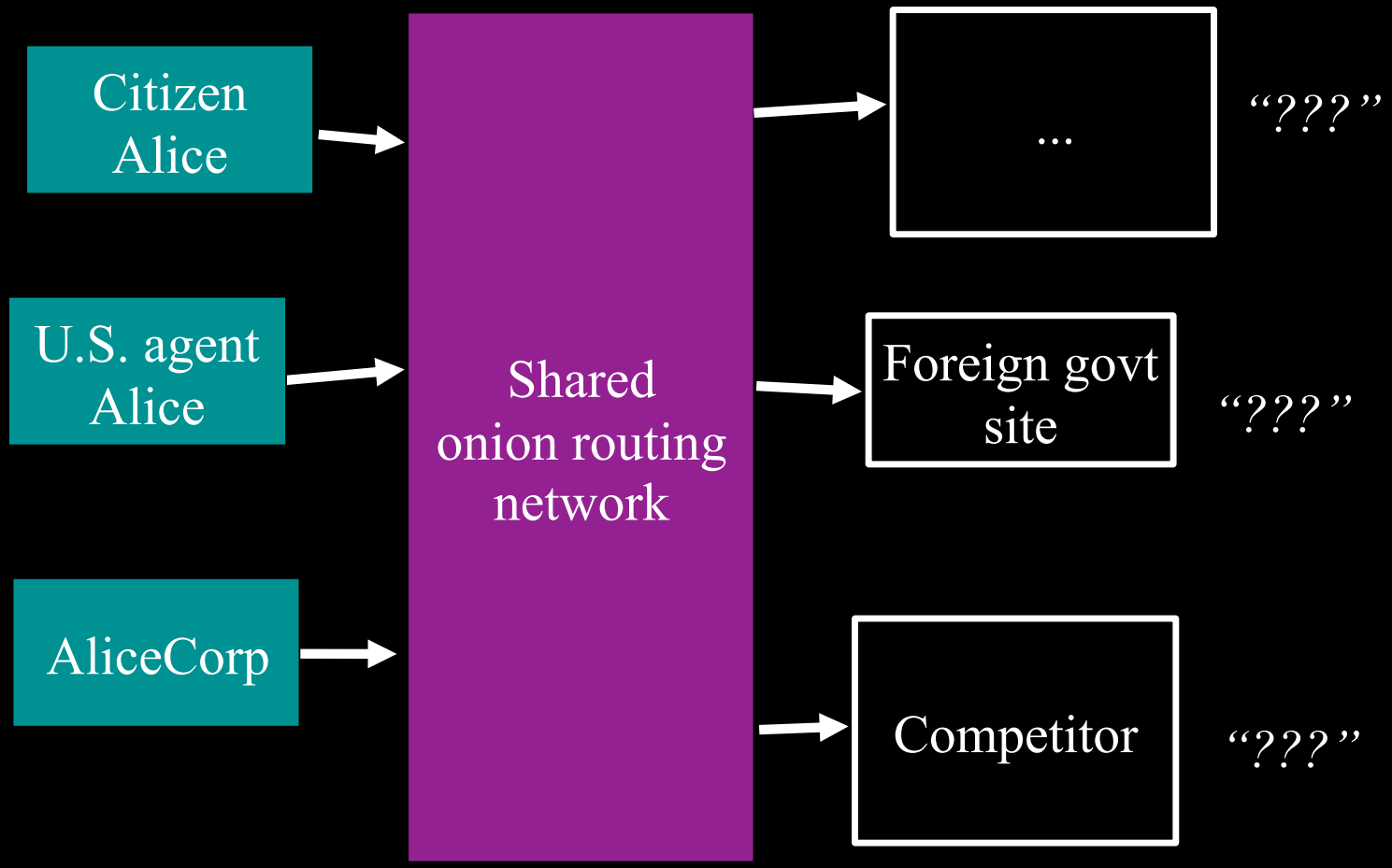
You can't be anonymous by yourself: private solutions are ineffective...



You can't be anonymous by yourself: private solutions are ineffective...



... so, anonymity loves company



Tor

Tor's Onion Routing

The NRL project begun in 2001

Also a separate entity, the Tor Project, incorporated as 501(c)3 in 2006

Also refers to the large public network: currently c. 3000 servers worldwide with .5 to 1 million concurrent users

- Self organized independent of NRL and Tor Project

Also refers to the Tor software run by users or network operators

EDITION: U.S. | INTERNATIONAL | MÉXICO

Set edition preference

CNN Tech

Home | Video | NewsPulse | U.S. | World | Politics | Justice | Entertainment | Tech | Health | Livi

Sports ›

Starting a revolution with technology

By **Gabe LaMonica** and **Taryn Fixel**, CNN

June 17, 2011 9:24 a.m. EDT | Filed under: Innovation

Faces of an 'iRevolution'

The CNN documentary "iRevolution" profiles citizen journalists who have played a key role in the protests shaking the Arab world. These Internet activists have braved jail, torture and death threats to help bring about reform.

STORY HIGHLIGHTS

- The Internet played a key role in the political revolutions in Egypt

CNN's "iRevolution: Online Warriors of the Arab Spring," premieres Sunday, June 19, 8 p.m. ET & PT. It will re-air Saturday, June 25, at 8 p.m. and 11p.m.

EDITION: U.S. | INTERNATIONAL | MÉXICO

Set edition preference

CNN Tech

Home | Video | NewsPulse | U.S. | World | Politics | Justice | Entertainment | Tech | Health | Livi

Sports ›

Starting a revolution with technology

By **Gabe LaMonica** and **Taryn Fixel**, CNN

June 17, 2011 9:24 a.m. EDT | Filed under: Innovation

ent shut it down.

Faces of an 'iRevolution'

The CNN documentary "iRevolution" profiles citizen journalists who have played a k the Arab world. These Internet activists have braved jail, torture and death threats t

authorities tracking their Internet activities.

Activists in Tunisia, Egypt and Bahrain told CNN about five technologies that have been most useful in getting around government-imposed blockades:

1. Tor

Tor is a circumvention tool that allows users to access censored information online, by bouncing communications among a network of users around the world, ultimately enabling its users to maintain anonymity online.

Slim Amamou, a "hacktivist" based in Tunisia, describes Tor as a program that enables you to "circumvent the central service of censorship by using a computer from someone else in the world."

It played a crucial role, he says, because social media pages sharing information about the protests were "systematically censored so you could not access them without censorship circumvention tools.

"So [Tor] was vital to get information and share it."

STORY HIGHLIGHTS

- The Internet played a key role in the political revolutions in Egypt

CNN's "iRevolution: Online Warriors of the Arab Spring," premieres Sunday, June 19, 8 p.m. ET & PT. It will re-air Saturday, June 25, at 8 p.m. and 11p.m.

Tor and circumvention

Connecting through Tor shows a Tor node IP address to censor rather than true destination

Tor and circumvention

Connecting through Tor shows a Tor node IP address to censor rather than true destination

But there are only about 3000 nodes: could an adversary simply block access to the network?

Blocking and bridges

- Tor nodes are listed in public directories
  - so the clients can discover them and build routes
  - to be a good netizen (your server can refuse connections from Tor if you want)
  - but facilitating blocks from public Tor network -> facilitating blocks ***to*** the public Tor network, so
- Bridges: Nodes that just provide connection to Tor network
  - not publicly listed -> harder to discover/block
- Not the only way to block: DPI tricks on handshake etc.


Politics Business National Local Culture Libya Opinion Who's Who Press Headlines
MASTER OF ARTS IN DIPLOMACY
A unique blend of an online Global Affairs curriculum with a concentration in your field of expertise.
International Terrorism
International Conflict Management
International Commerce
You are here: Home » Culture » Arab Bloggers Meeting: Energizing the Blogosphere Through the Arab Revolutions
Arab Bloggers Meeting: Energizing the Blogosphere Through the Arab Revolutions
Houda Mzioudet | 06 October 2011 | 1 Comment
The Arab Bloggers Meeting kicked off its second day on October 4th with a BarCamp, a series of user-generated conferences and open participatory workshops whose content was provided by attendees and which addressed different techniques that could be of use to bloggers. The workshops took place in six rooms in the Golden Tulip Hotel in Ganmarth, and in each room was a trainer who coached bloggers on the usage of Photoshop, video editing, translations, and editorials. Moreover, bloggers suggested particular issues that might come up during the elections and brainstormed ways to cover them.

Arab Bloggers Meeting: Energ Blogosphere Through the Arab

Houda Mzioudet | 06 October 2011 | 1 Comment

The Arab Bloggers Meeting kicked off its second day on October 4t generated conferences and open participatory workshops whose c which addressed different techniques that could be of use to blogg in the Golden Tulip Hotel in Ganmarth, and in each room was a trai Photoshop, video editing, translations, and editorials. Moreover, b might come up during the elections and brainstormed ways to co

The issue of censorship was, and will continue to be, the greatest challenge of bloggers. During the conference, Marek Tuszynsk suggested tools to circumvent censorship, as well as how to use proxies — such as those used by bloggers during the Internet blackout period throughout the Arab revolutions, when social media networks were blocked by authoritarian regimes. According to Marek, the "Tor Project" is the most effective way to circumvent censorship, although many regimes in the Middle East have blocked access to the "Tor Project."

Mexico cartels lash out against 'Internet snitches'

By CHRIS BRONK

Published 07:05 p.m., Friday, September 30, 2011

After Iraq, Mexico is the most dangerous place on the planet for working journalists. Since 2000, some 58 reporters, photographers and editors targeted by narcotics cartels have been killed in drug-related violence that has taken more than 40,000 lives. As a result, news coverage by Mexican journalists on the narco-insurgency has plummeted, and a grossly violent spree of lawlessness in contemporary Mexico has gone unreported. Following the deaths of two staff members last year, the editors of Ciudad Juarez's El Diario asked the cartels, "What do you want from us?" in a lead editorial.

With traditional media on the sidelines, the Internet has filled the breach. Blog and social media discussions on security in Mexico are not merely a fascination with crime but rather, practical guidance. With so much violence, being in the wrong place at the wrong time is a common occurrence.

In stark contrast to the rosy use of social media for organizing and directing protests in the revolutions of the Arab Spring, the New York Times' Damien Cave observed, "In Mexico, Twitter, Facebook and other tools are instead deployed for local survival." Twitter provides a forecast on the spasms of violence in once safe cities like Monterrey, Veracruz and San Luis Potosi for digitally connected Mexicans.

For some time, the Internet provided an unobstructed channel for public safety information and anonymous

Mexico cartels lash out against 'Internet snitches'

By CHRIS BRONK
Published 07:05 p.m., Friday, September 30, 2011

After Iraq, Mexico is the most dangerous place on the planet for working journalists. Since 2000, some 58 reporters, photographers and editors targeted by narcotics cartels have been killed in drug-related violence that has taken more than 40,000 lives. As a result, news coverage by Mexican journalists on the n
spree of
unrepor
asked th

With tra
on sec
violenc

In stark
Arab Sp
instead
like Mor

For som

If the Zetas are able to tie digital and physical identities, it represents a new leap in its ability to monitor signals and develop cyber intelligence. This likely means the Zetas have gained the capacity to see inside the network operations of the country's major Internet and telecommunications providers. Yet another institution of the Mexican state has been manipulated and corrupted by the forces battling to control the narcotics still demanded by the U.S. market.

So how can more Mexicans do what Laredo Girl has done while avoiding recriminations from Mexican gangs? Probably the best technology for this is Tor (torproject.org), used daily around the world to allow people to connect to the Internet without others listening in. Tor has notably been in a battle with the government of Iran, which has twice tried to block Tor traffic from getting out of the country. Each time, within a day, Tor identified the attack and found a way to get back online.

Tor, or other systems like it, guarantees that an electronic eavesdropper learns nothing. However, public posting to social media must still be protected by a pseudonym. Discussion aside, social media - with or without effective anonymity - cannot be expected to magically restore law and order south of the border.

However, by giving a voice to the problem, perhaps there will be more pressure to act.

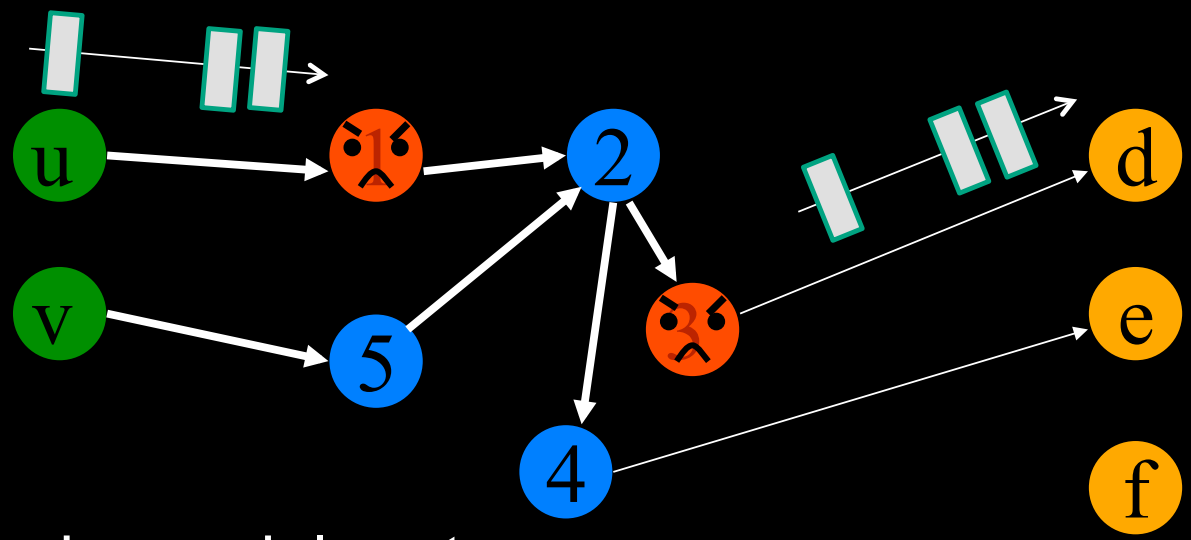
A Tor Feature and Bug

Anybody can run a node in the network

A significant adversary could own much of the network

How can we route securely even if our adversary owns 30% of the network?

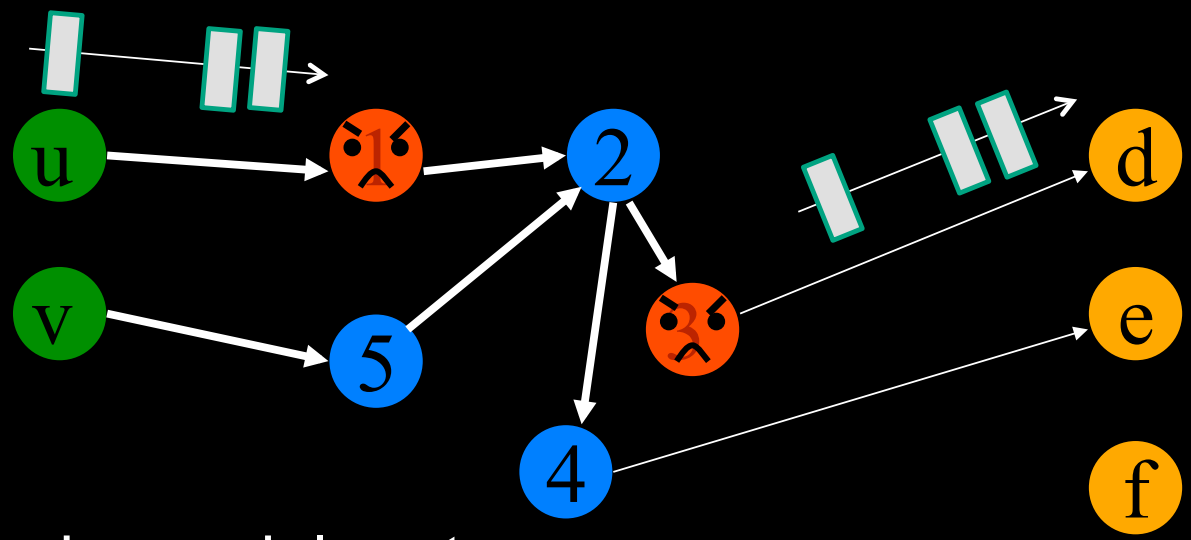
Risk of end-to-end correlation attack



Some adversarial routers

User doesn't know where the adversary is.

Use trust to minimize risk of end-to-end correlation attack



Some adversarial routers

User doesn't know where the adversary is.

User may have some idea of which routers are likely to be adversarial.

Adding trust to onion routing

Assume that nodes are trusted to different degrees.

Simplest question to ask first: How can we choose the first and last node in an onion routing circuit to minimize the chance of a correlation attack?

- i.e. minimize the chance that they are both compromised

Adding trust in links, association of a user with the nodes he trust... can come later, but are pointless if we cannot handle this most basic question.

Model of Trust

Router r_i has **trust** t_i. An attempt to compromise a router succeeds with probability $c_i = 1\text{-}t_i$.

User will choose circuits using a known distribution.

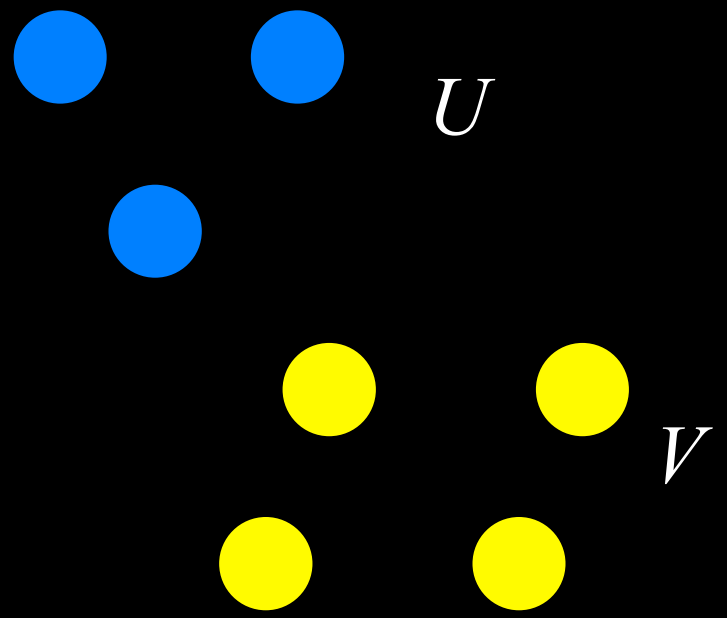
Adversary attempts to compromise at most k routers, $K \subseteq R$.

After attempts, users actually choose circuits.

Trust Model

Two trust levels: $t_1 \geq t_2$

U = $\{r_i \mid t_i = t_1\}$, V = $\{r_i \mid t_i = t_2\}$

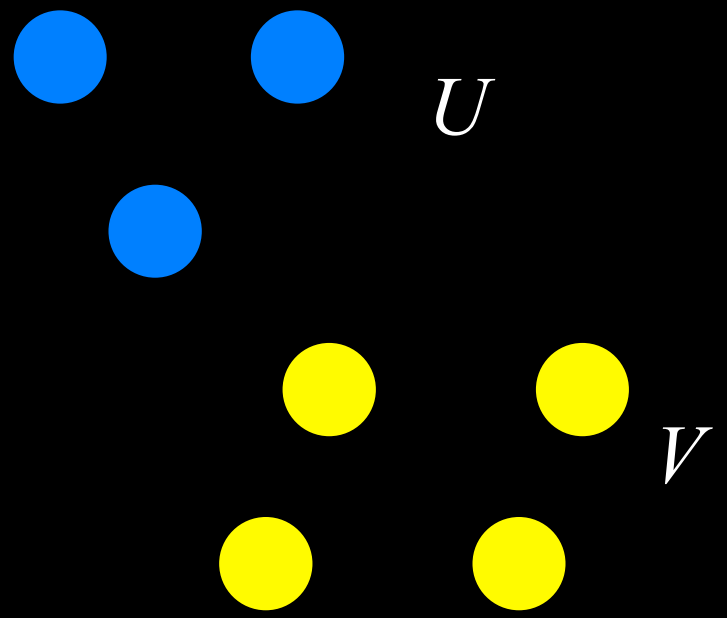


Trust Model

Two trust levels: $t_1 \geq t_2$

U = $\{r_i \mid t_i = t_1\}$, V = $\{r_i \mid t_i = t_2\}$

Theorem: Three distributions can be optimal:



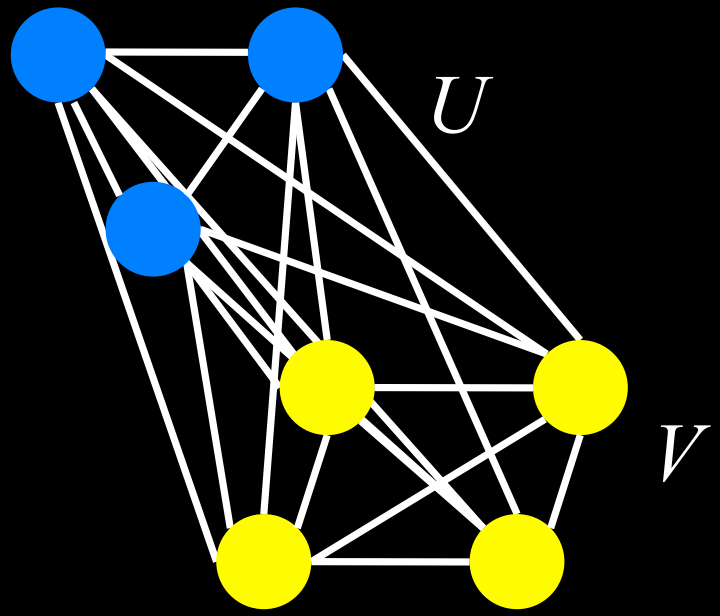
Trust Model

Two trust levels: $t_1 \geq t_2$

U = $\{r_i \mid t_i=t_1\}$, V = $\{r_i \mid t_i=t_2\}$

Theorem: Three distributions can be optimal:

1. $p(r,s) \propto c_r c_s$ for $r,s \in R$



Trust Model

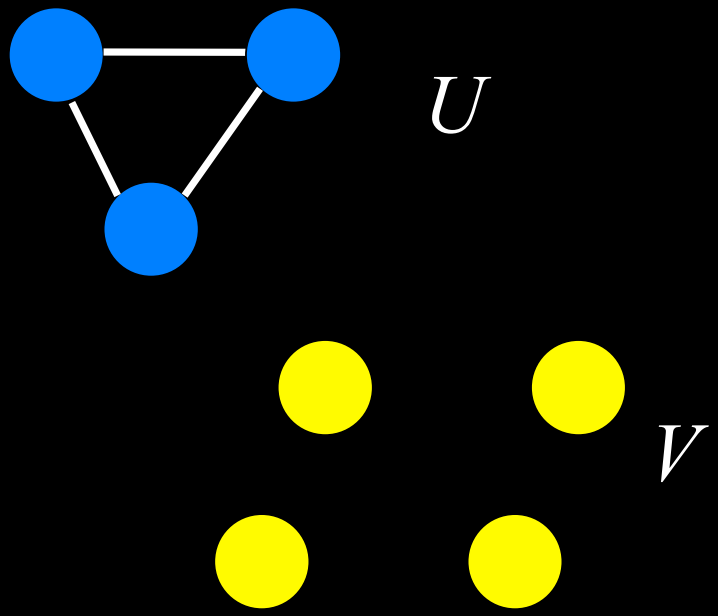
Two trust levels: $t_1 \geq t_2$

U = $\{r_i \mid t_i=t_1\}$, V = $\{r_i \mid t_i=t_2\}$

Theorem: Three distributions can be optimal:

1. $p(r,s) \propto c_r c_s$ for $r,s \in R$

2. $p(r,s) \propto \begin{cases} c_1^2 & \text{if } r,s \in U \\ 0 & \text{otherwise} \end{cases}$



Trust Model

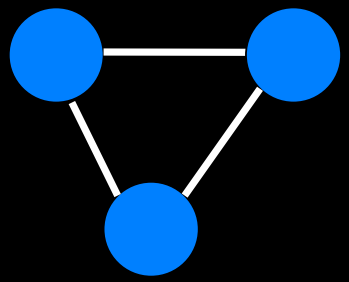
Two trust levels: $t_1 \geq t_2$

U = $\{r_i \mid t_i=t_1\}$, V = $\{r_i \mid t_i=t_2\}$

Theorem: Three distributions can be optimal:

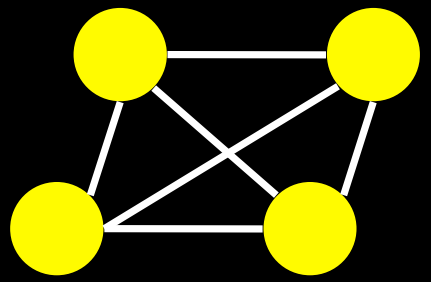
1. $p(r,s) \propto c_r c_s$ for $r,s \in R$

2. $p(r,s) \propto \begin{cases} c_1^2 & \text{if } r,s \in U \\ 0 & \text{otherwise} \end{cases}$



U

3. $p(r,s) \propto \begin{cases} c_1^2(n(n\text{-}1)\text{-}v_0(v_0\text{-}1)) & \text{if } r,s \in U \\ c_2^2(m(m\text{-}1)\text{-}v_1(v_1\text{-}1)) & \text{if } r,s \in V \\ 0 & \text{otherwise} \end{cases}$



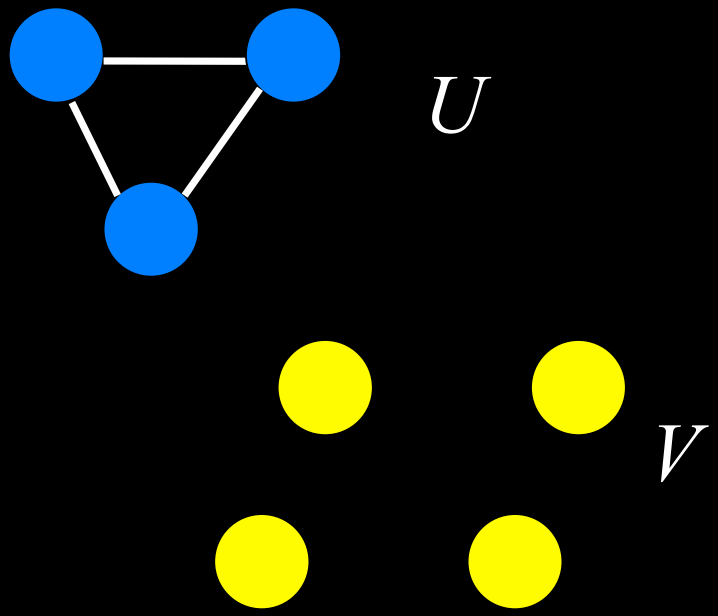
V

More general adversary

Analysis assumes only nodes are compromised:

What if you are visiting a hostile website?

What if the link to the destination is observed?



Downhill algorithm

Pick from most trusted nodes for first hop

Then pick from a broader set for each successive hop in the route

Each hop may include nodes less trusted by you, but also less likely to be associated with you

Table 1: Examples of optimal thresholds

(a) Small trusted and untrusted sets, for example when the user has information about a few good routers and a few bad routers, and has little information for the rest.

# Routers	5	1000	10
Prob. of compromise	0.01	0.1	0.9
Optimal thresholds	0.01	0.1	0.9

	Downhill	Trusted	Random	Lower bnd.
$E[Y]$	0.0274	0.2519	0.1088	0.01

(b) Small trusted, medium semi-trusted, large untrusted sets, for example when the adversary is strong, but the user and her friends run some routers.

# Routers	5	50	1000
Prob. of compromise	.001	0.05	0.5
Optimal thresholds	0.05	0.5	

	Downhill	Trusted	Random	Lower bnd.
E[Y]	0.0550	0.1751	0.4763	0.001