



The Tor Project

Our mission is to be the global resource for technology, advocacy, research and education in the ongoing pursuit of freedom of speech, privacy rights online, and censorship circumvention.

What is Tor?

Online anonymity 1) open source software,
2) network, 3) protocol

Community of researchers, developers,
users, and relay operators

Funding from US DoD, Electronic Frontier
Foundation, Voice of America, Google,
NLnet, Human Rights Watch, NSF, US
State Dept, SIDA, Knight Foundation, ...

The Tor Project, Inc.

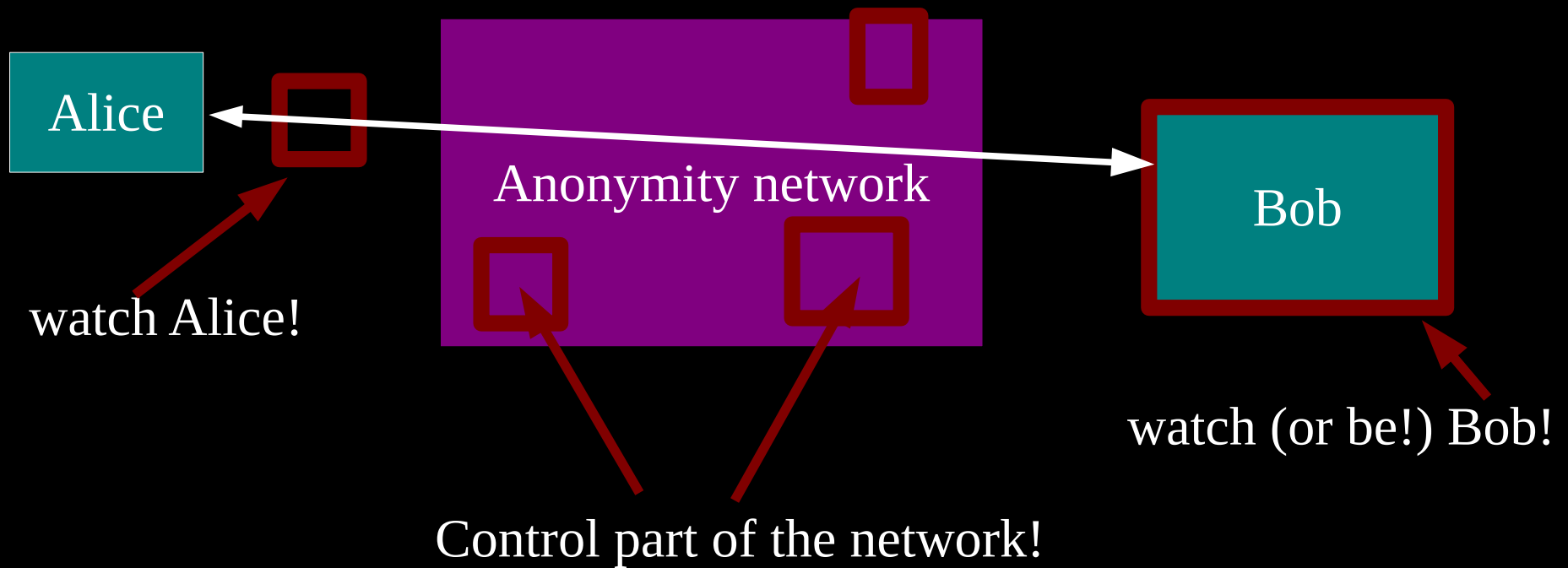


501(c)(3) non-profit organization dedicated to the research and development of tools for online anonymity and privacy

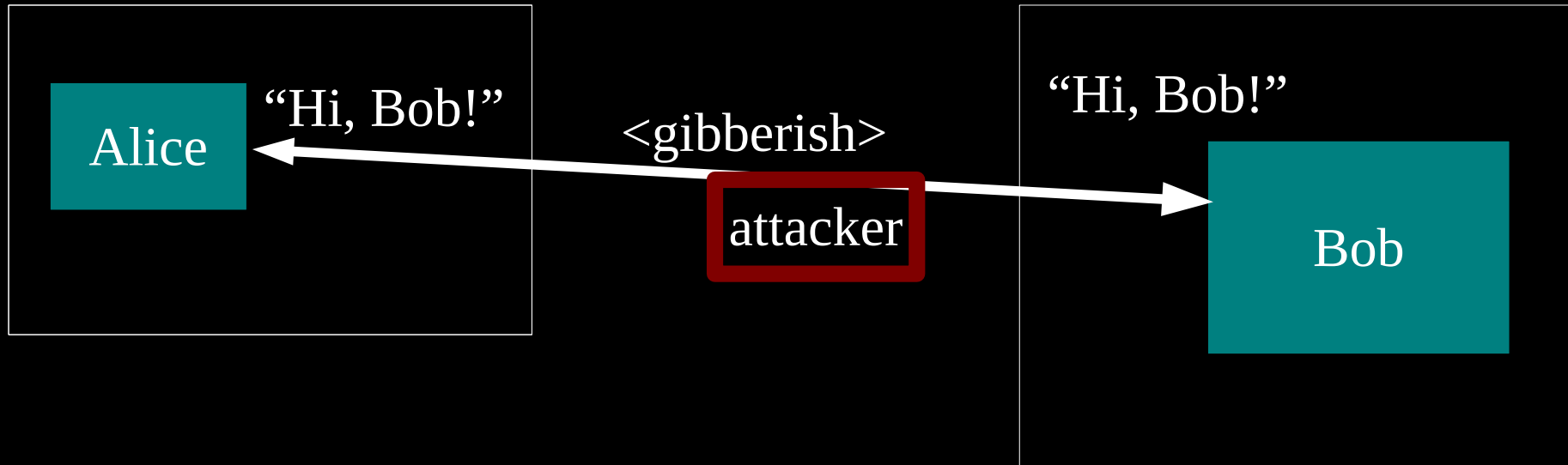


Estimated 2,000,000+
daily Tor users

Threat model: what can the attacker do?



Anonymity isn't encryption: Encryption just protects contents.



Anonymity isn't just wishful thinking...

“You can't prove it was me!”

“Promise you won't look!”

“Promise you won't remember!”

“Promise you won't tell!”

“I didn't write my name on it!”

“Isn't the Internet already anonymous?”

Anonymity serves different interests for different user groups.

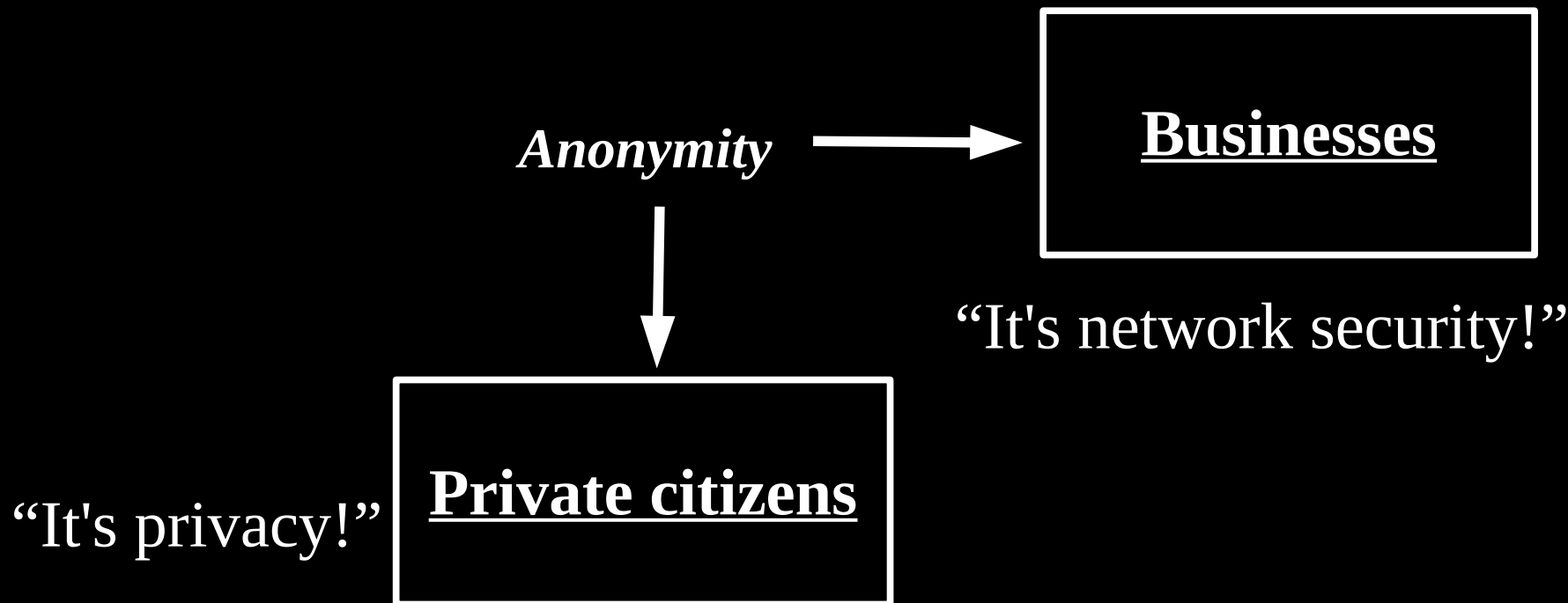
Anonymity



“It's privacy!”

Private citizens

Anonymity serves different interests for different user groups.



Anonymity serves different interests for different user groups.

“It's traffic-analysis resistance!”

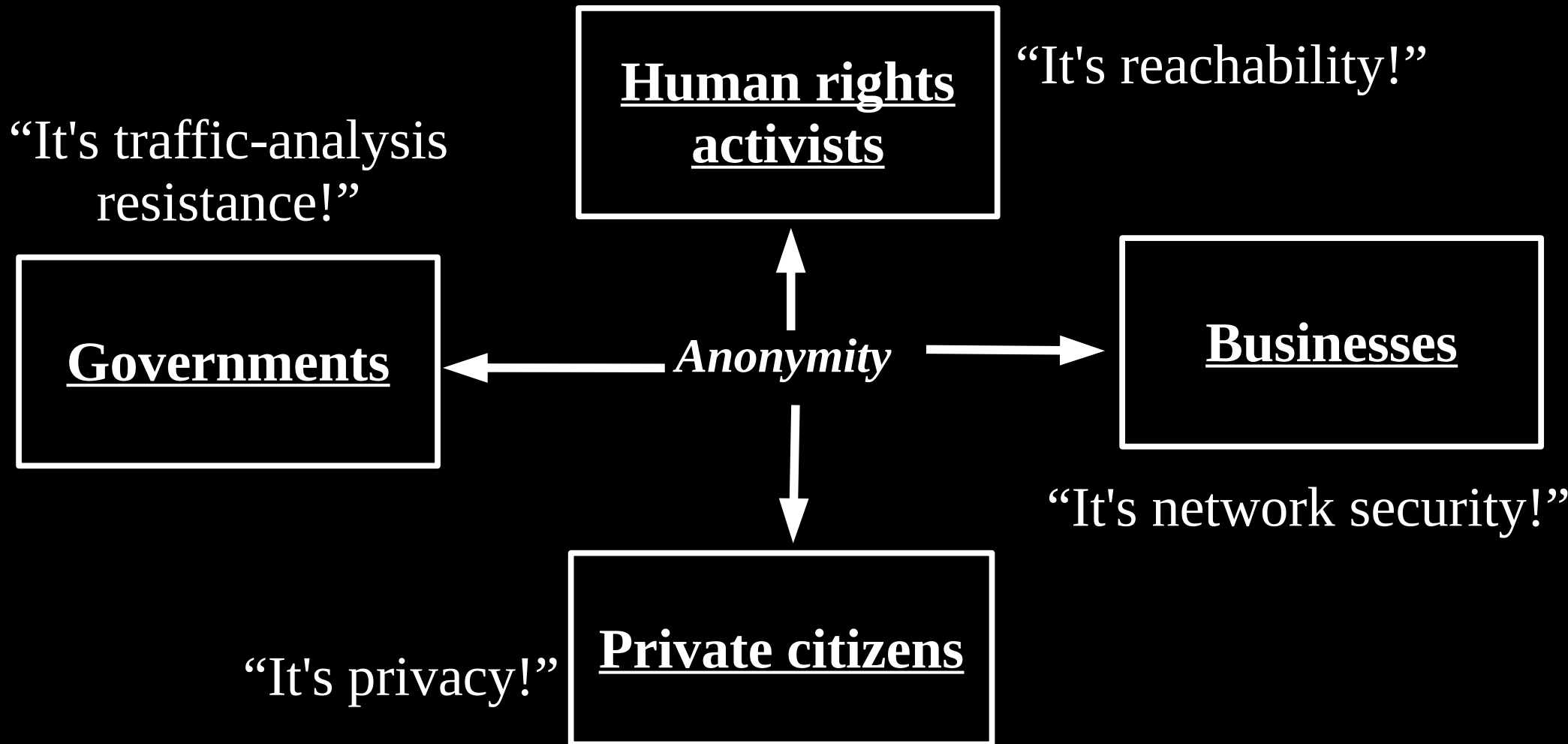


“It's network security!”

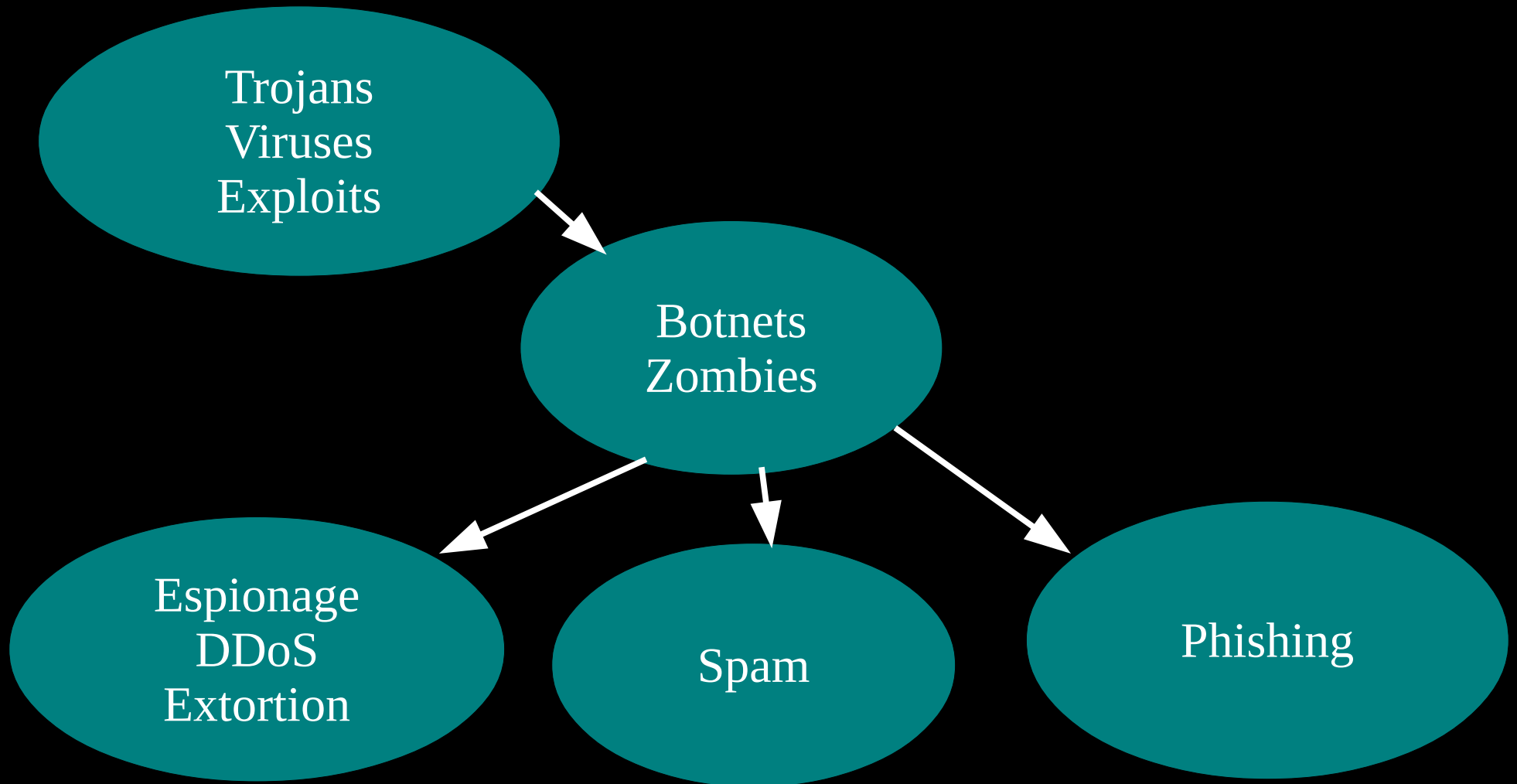
“It's privacy!”



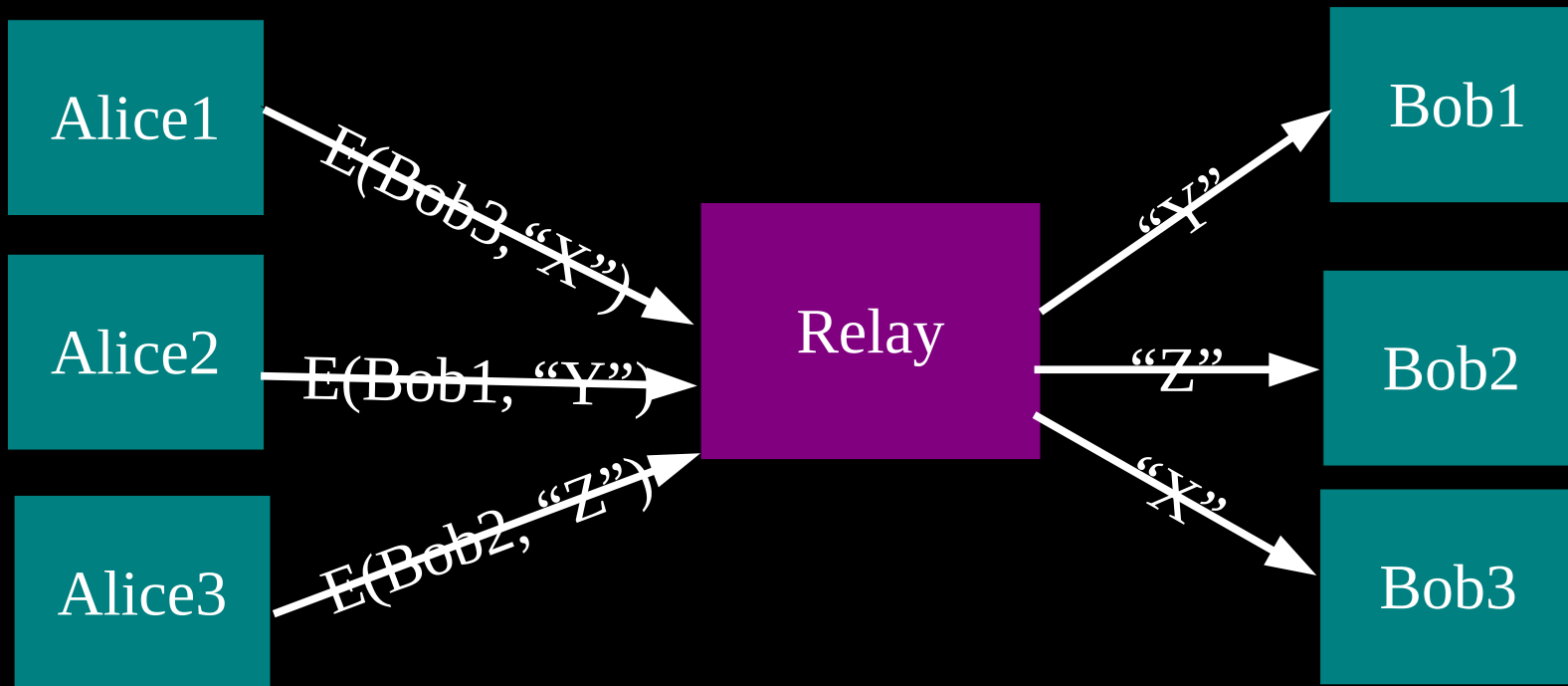
Anonymity serves different interests for different user groups.



Current situation: Bad people on the Internet are doing fine

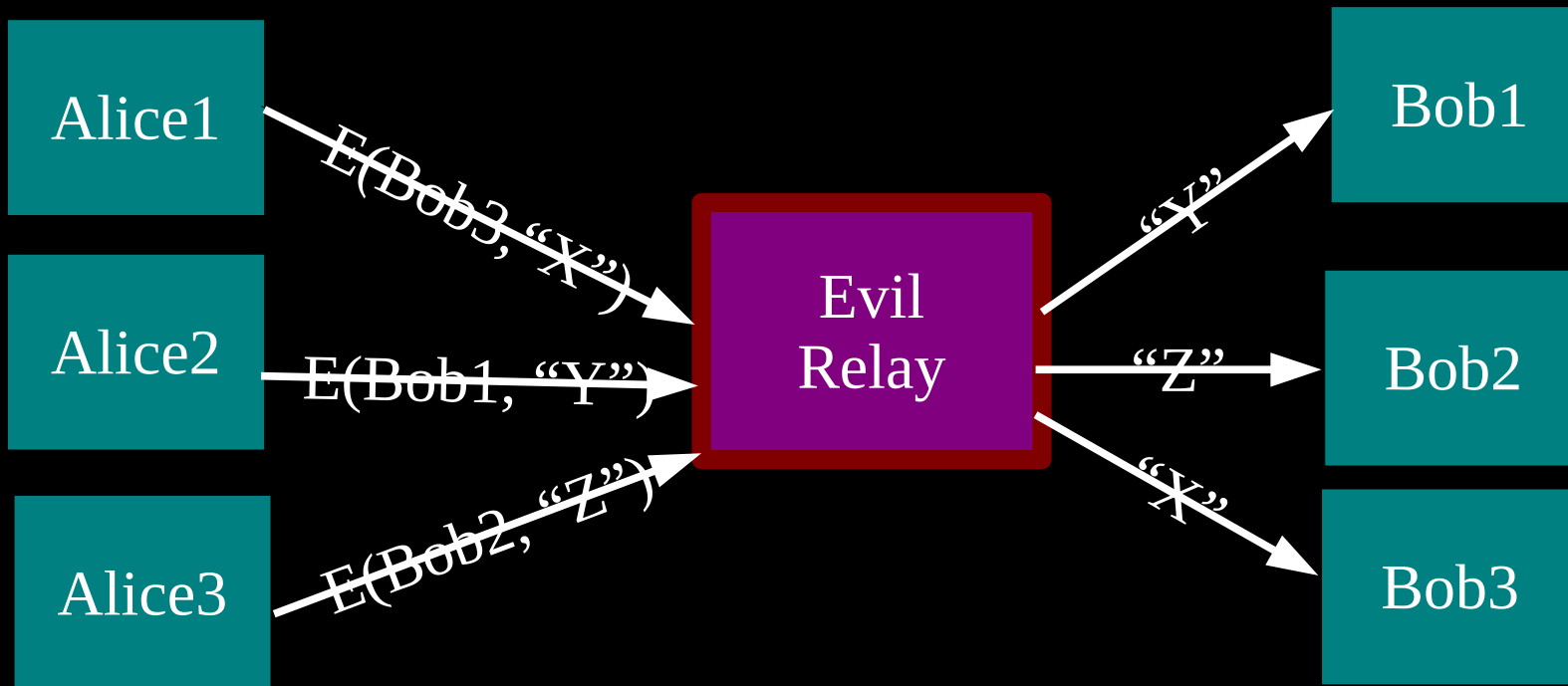


The simplest designs use a single relay to hide connections.

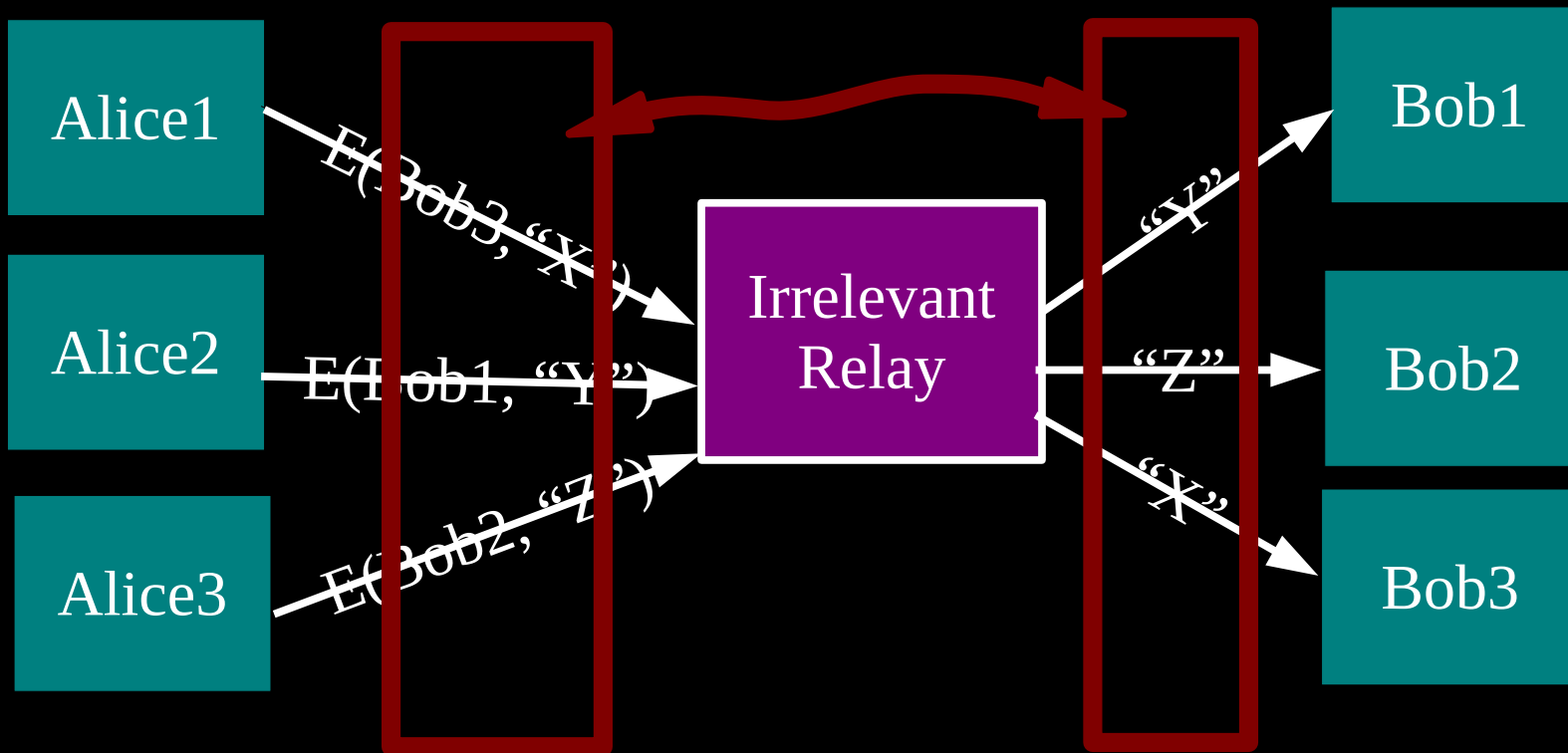


(example: some commercial proxy providers)

**But a single relay (or eavesdropper!)
is a single point of failure.**

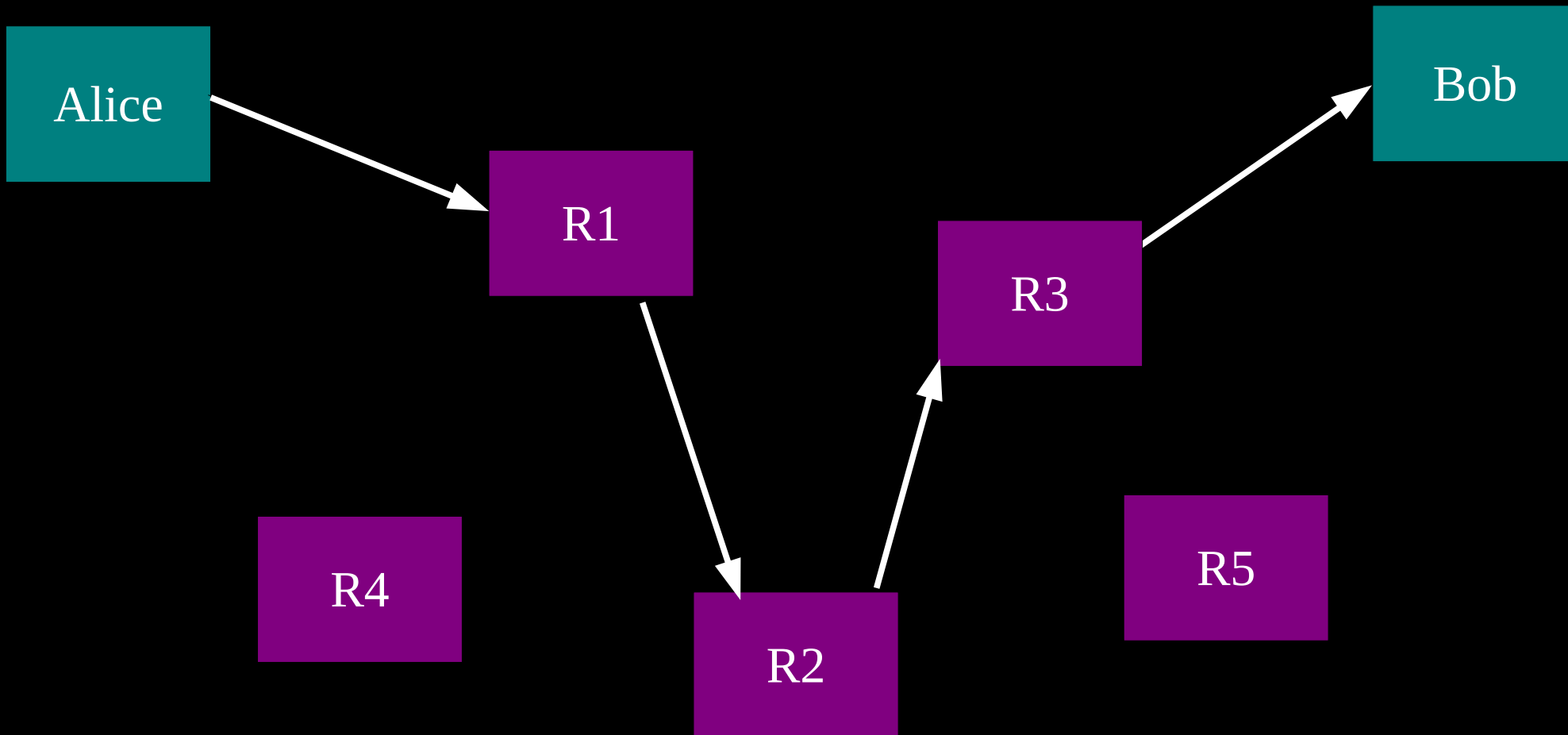


... or a single point of bypass.

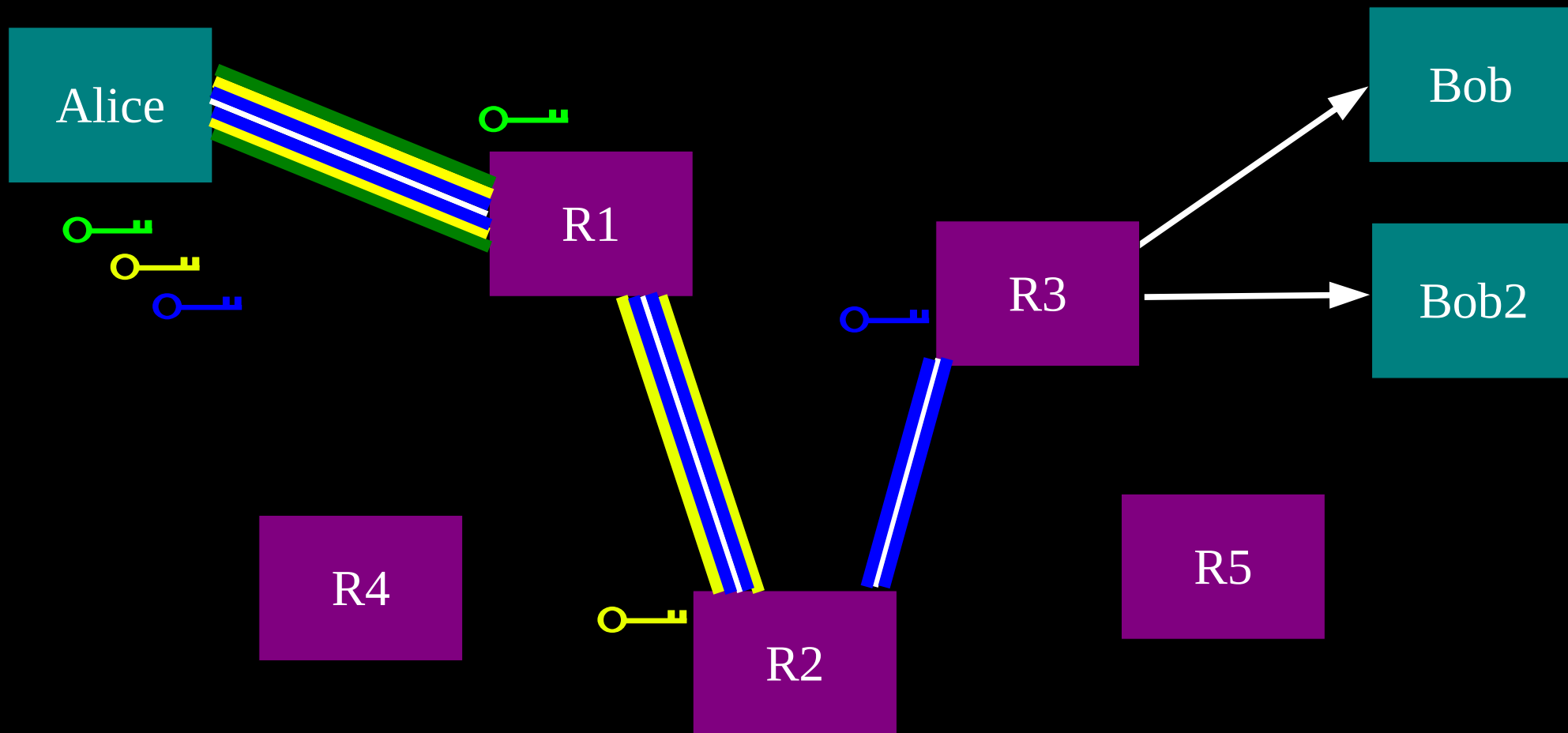


Timing analysis bridges all connections through relay \Rightarrow An attractive fat target

So, add multiple relays so that no single one can betray Alice.

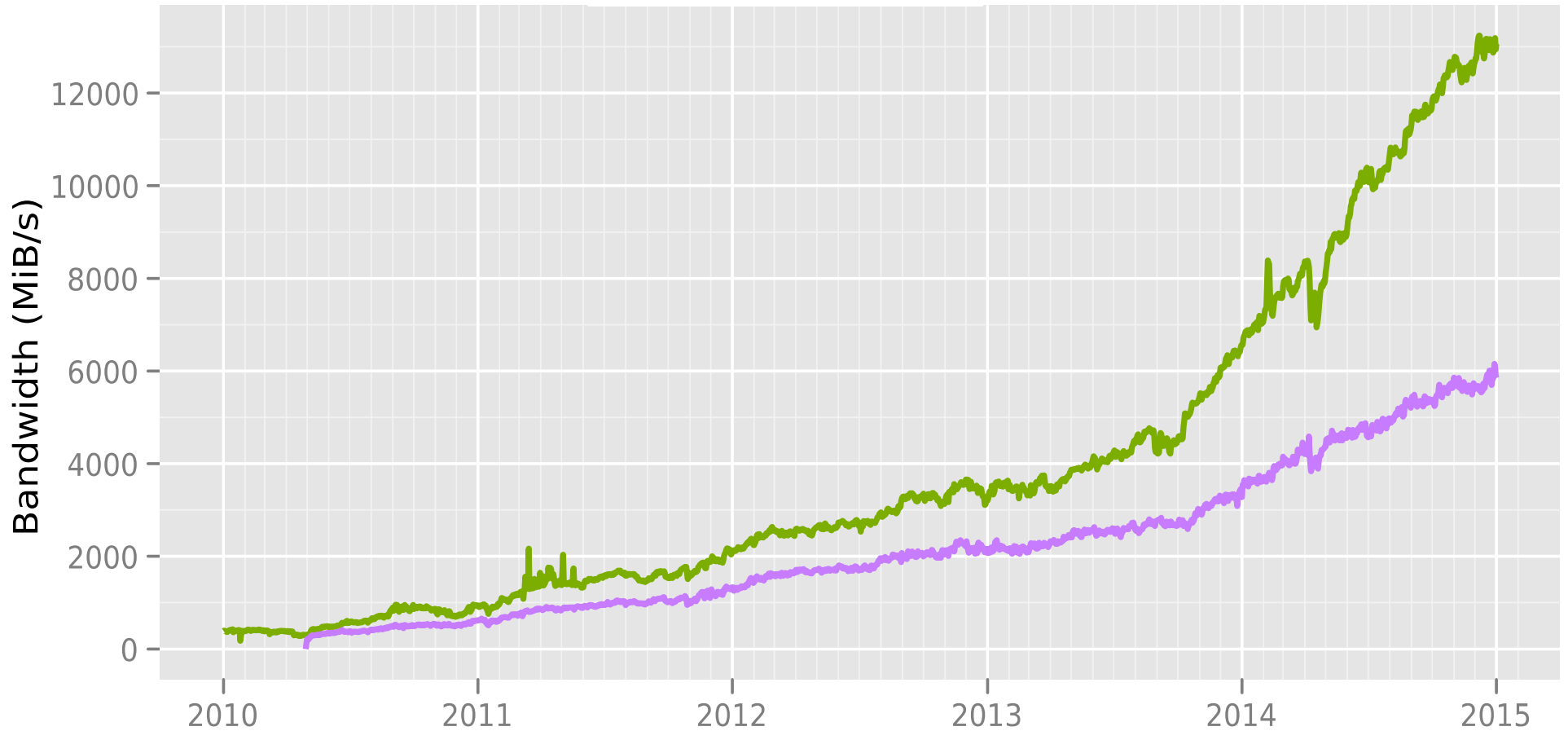


**Alice makes a session key with R1
...And then tunnels to R2...and to R3**



Total relay bandwidth

- Advertised bandwidth
- Bandwidth history



The Tor Project - <https://metrics.torproject.org/>

Tor's safety comes from diversity

- #1: Diversity of relays. The more relays we have and the more diverse they are, the fewer attackers are in a position to do traffic confirmation. (Research problem: measuring diversity over time)
- #2: Diversity of users and reasons to use it. 50000 users in Iran means almost all of them are normal citizens.

- New Identity
- Cookie Protections
- Preferences...
- About Torbutton...
- Open Network Settings...

Congratulations!

This browser is configured to use Tor.
 You are now free to browse the Internet anonymously.
[Test Tor Network Settings](#)

Search securely with Startpage.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

[Tips On Staying Anonymous »](#)

You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- [Run a Tor Relay Node »](#)
- [Volunteer Your Services »](#)
- [Make a Donation »](#)

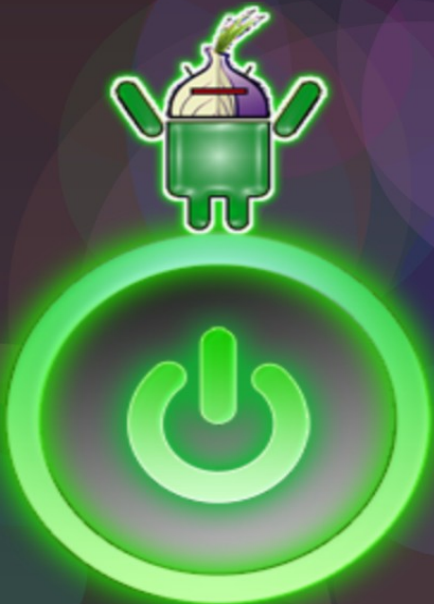
The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. [Learn more about The Tor Project »](#)

Orbot

Connected to the Tor network

Orbot

powered by The Tor Project

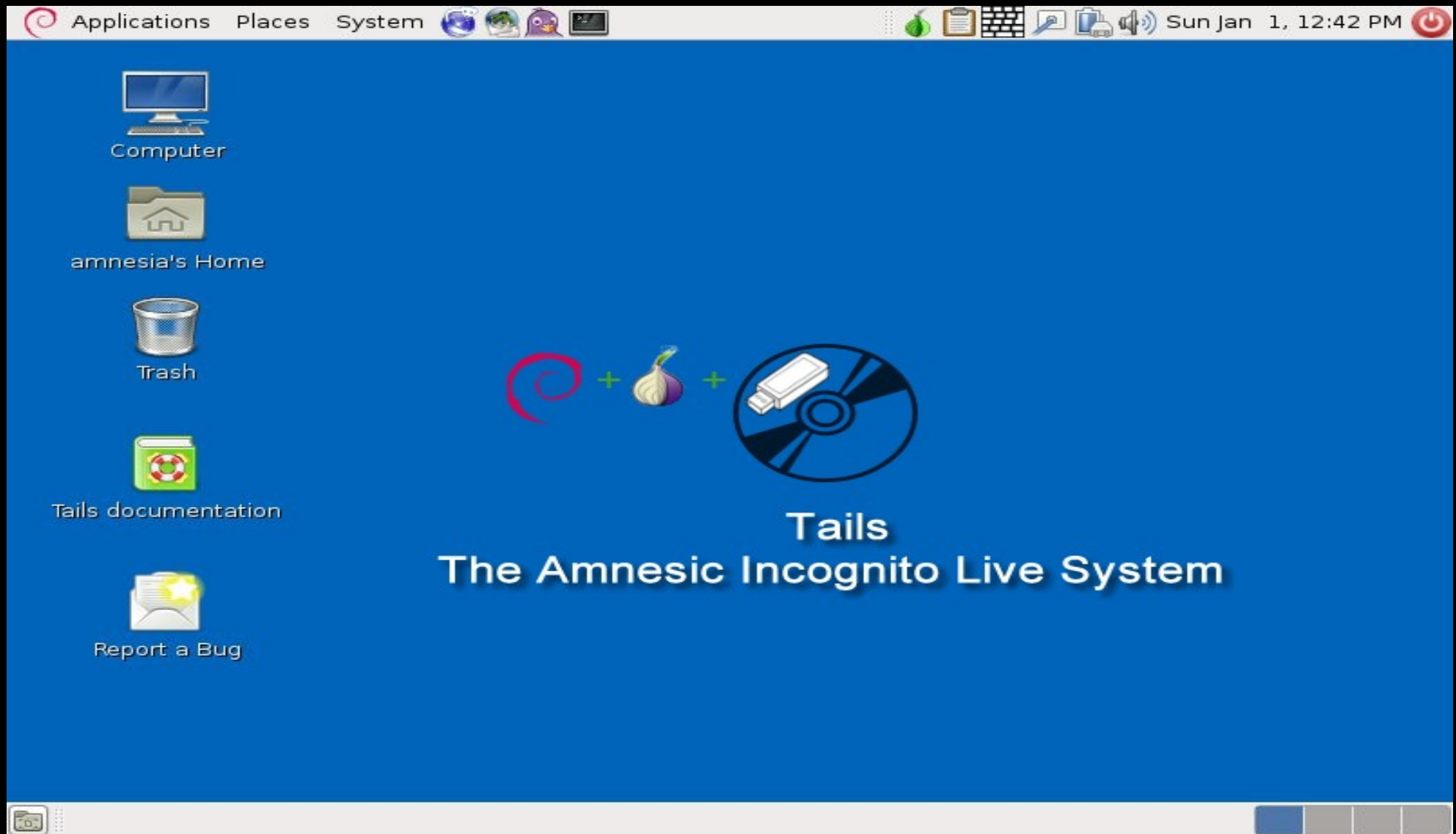


Connected to the Tor network

Download	Log	Upload
98.2kbps / 94.1KB		4.5kbps / 18.4KB

Navigation icons: back, home, recent apps

Tails LiveCD



Deterministic Builds Part Two: Technical Details

View

Edit

Posted October 4th, 2013 by [mikeperry](#) in [cyberpeace](#), [decentralization](#), [deterministic builds](#), [gitian](#), [National Insecurity Agency](#), [security](#)

This is the second post in a two-part series on the build security improvements in the [Tor Browser Bundle 3.0 release cycle](#).

The [first post](#) described why such security is necessary. This post is meant to describe the technical details with respect to how such builds are produced.

We achieve our build security through a reproducible build process that enables anyone to produce byte-for-byte identical binaries to the ones we release. Elsewhere on the Internet, this process is varyingly called "deterministic builds", "reproducible builds", "idempotent builds", and probably a few other terms, too.

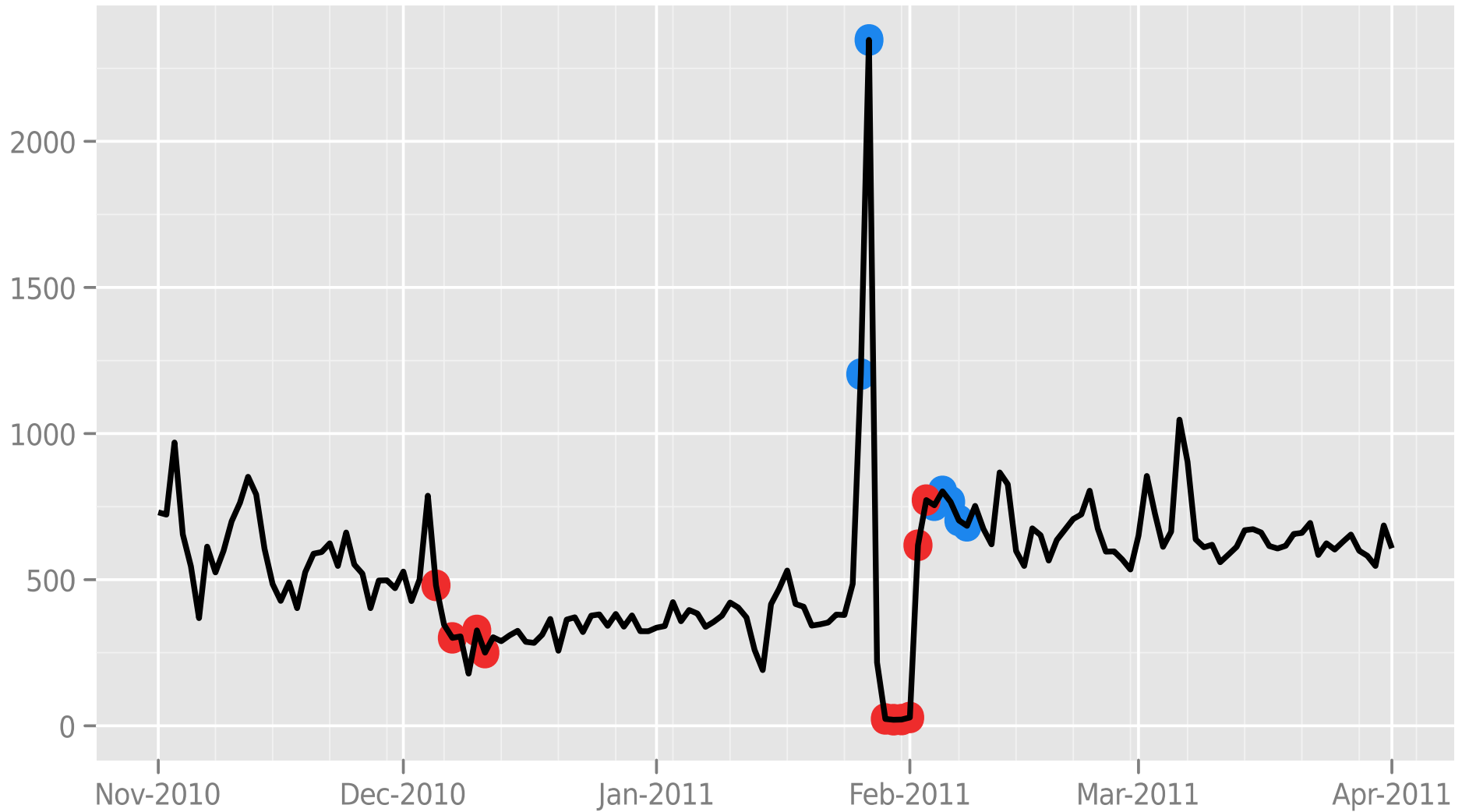
To produce byte-for-byte identical packages, we use [Gitian](#) to build Tor Browser Bundle 3.0 and above, but that isn't the only option for achieving reproducible builds. We will first describe how we use Gitian, and then go on to enumerate the individual issues that Gitian solves for us, and that we had to solve ourselves through either wrapper scripts,

- [Add a New Blog Post](#)
- [Manage Blog](#)
- [Admin Comments](#)
- [Manage Users](#)
- [Add an Event](#)
- [Manage Events](#)
- [Manage Forums](#)

Upcoming events

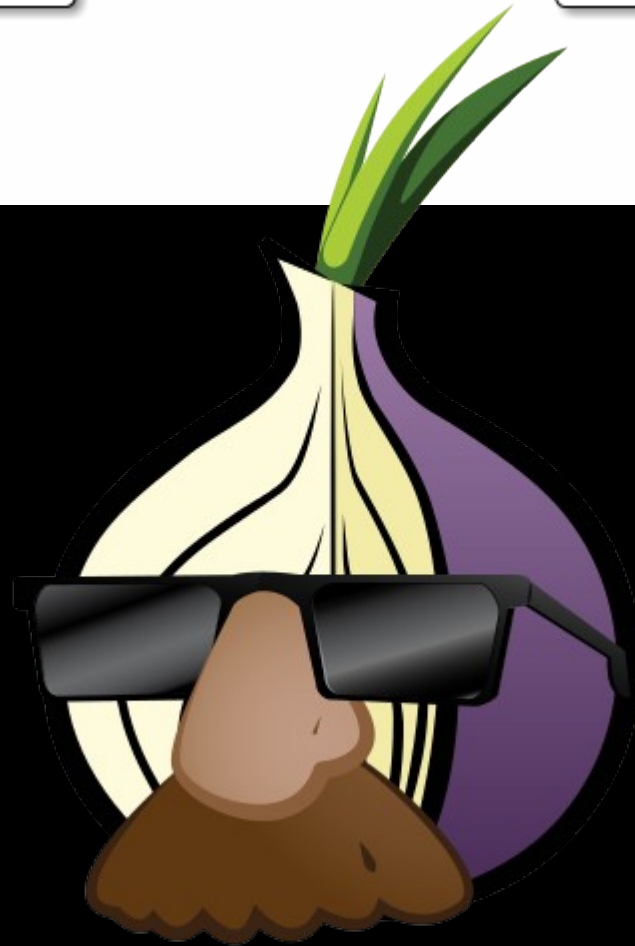
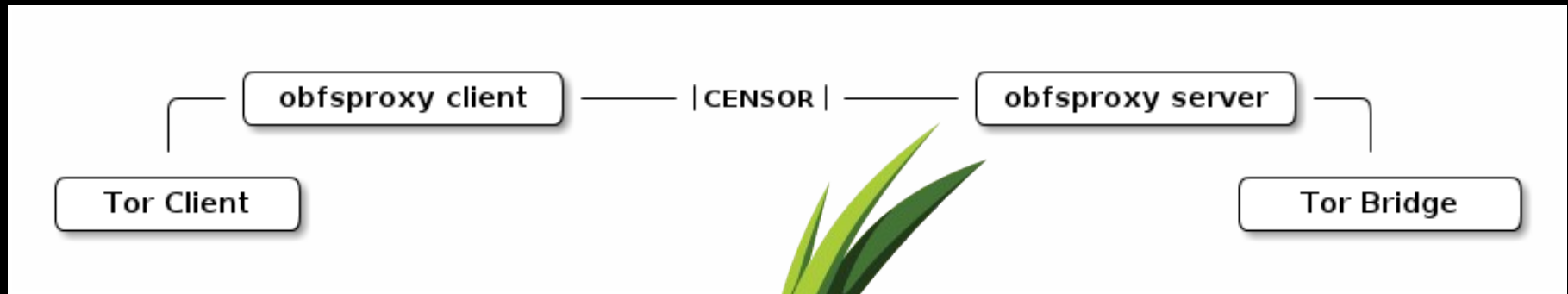
- [Roger, Jake, mar... at 31c3 in Hambu...](#)
(Now o
- [Roger doing invit... Real World Crypt... London](#)
(10 days

Directly connecting users from Egypt



The Tor Project - <https://metrics.torproject.org/>

Pluggable transports







“Still the King of high secure,
low latency Internet Anonymity”

Contenders for the throne:

- None

NSA targets the privacy-conscious

von J. Appelbaum, A. Gibson, J. Goetz, V. Kabisch, L. Kampf, L. Ryge

One of NSA's German targets is 212.212.245.170. The string of numbers is an IP address assigned to Sebastian Hahn, a computer science student at the University of Erlangen. Hahn operates the server out of a grey high-security building a few kilometers from where he lives. Hahn, 28 years old and sporting a red beard, volunteers for the Tor Project in his free time. He is especially trusted by the Tor community, as his server is not just a node, it is a so-called Directory Authority. There are nine of these worldwide, and they are central to the Tor Network, as they contain an index of all Tor nodes. A user's traffic is automatically directed to one of the directory authorities to download the newest list of Tor relays generated each hour.

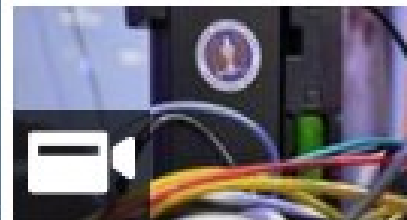
```
1 // MARK: - AUTHORITY
2
3 // Experiment for authoritative directories awaiting the directory protocol.
4
5 #pragma mark - Authentication (for nodes that use it) - Not needed by
6 all (Some directories do not support authentication)
7 // END MARKER
```

Hahn's predecessor named the server Gabelmoo, or Fork Man, the nickname of a local statue of Poseidon. After a look at the NSA source code, Hahn quickly

Nächster Send

Do, 08. 01. 201

WEITERE INFORMA



03.07.14 | 17:15 Uhr

Quellcode entschlü für NSA-Spionage i

Deutsche, die sich m
lung im Internet bes
den gezielt vom US-C
NSA ausgespäht. | m

Only a piece of the puzzle

We hope the users aren't attacked by their hardware and software

No spyware installed, no cameras watching their screens, etc

Users can fetch a genuine copy of Tor?

[HOME](#)[ARCHIVES](#)[ABOUT TOR](#)[DONATE](#)[ADMIN](#)

Tor security advisory: "relay early" traffic confirmation attack

[View](#)[Edit](#)

Posted July 30th, 2014 by [arma](#) in [entry guards](#), [hidden services](#), [research](#), [security advisory](#)

This advisory was posted on the [tor-announce](#) mailing list.

SUMMARY:

On July 4 2014 we found a group of relays that we assume were trying to deanonymize users. They appear to have been targeting people who operate or access Tor hidden services. The attack involved modifying Tor protocol headers to do traffic confirmation attacks.

The attacking relays joined the network on January 30 2014, and we removed them from the network on July 4. While we don't know when they started doing the attack, users who operated or accessed hidden services from early February through July 4 should assume they were affected.

Unfortunately, it's still unclear what "affected" includes. We know the attack looked for

- [Add a New Blog Post](#)
- [Manage Blog](#)
- [Admin Comments](#)
- [Manage Users](#)
- [Add an Event](#)
- [Manage Events](#)
- [Manage Forums](#)

Upcoming events

- [Roger, Jake, many others at 31c3 in Hamburg](#)
(Now on De)
- [Roger doing invited talk at Real World Crypto in London](#)
(10 days on J)

[Article Archive:](#) [Current](#) [1999](#) [2000](#) [2001](#) [2002](#) [2003](#) [2004](#) [2005](#) [2006](#) [2007](#) [2008](#) [2009](#) [2010](#) [2011](#)

Information Warfare: Russia Pays A Reward For A Tor Killer

[Next Article → MURPHY'S LAW: When Is A War A War](#)

August 28, 2014: In July Russia offered a prize of \$111,000 for whoever could deliver, by August 20th, software that would allow Russian security services to identify who was using Tor (The Onion Router), a system that enables users to access the Internet anonymously. On August 22nd Russia announced that an unnamed Russian contractor, with a top security clearance, had received the \$111,000. No other details were provided.

Similar to anonymizer software, Tor was even more untraceable. Unlike anonymizer software, Tor relies on thousands of people running the Tor software, and acting as nodes for email (and attachments) to be sent through so many Tor nodes that it was believed virtually impossible to track down the identity of the sender. Tor was developed as part of an American

[Latest News](#) [Most Read](#) [Most Commented](#)

[INDIA-PAKISTAN: The Generals](#)

[SUPPORT: Better Future Shock](#)

[WARPLANES: China Like The F-22](#)

[SYRIA: Come To ISIS](#)

[AIR TRANSPORTA Contender Flouris](#)

[ELECTRONIC WE Roams The Pacific](#)

[CHINA: Heads Arc Greater Frequency](#)

[WINNING: The Terrorism](#)

[WEAPONS: Too H](#)

[COLOMBIA: The Peace Everyone W](#)

[ELECTRONIC WE](#)

Thursday, October 2, 2014

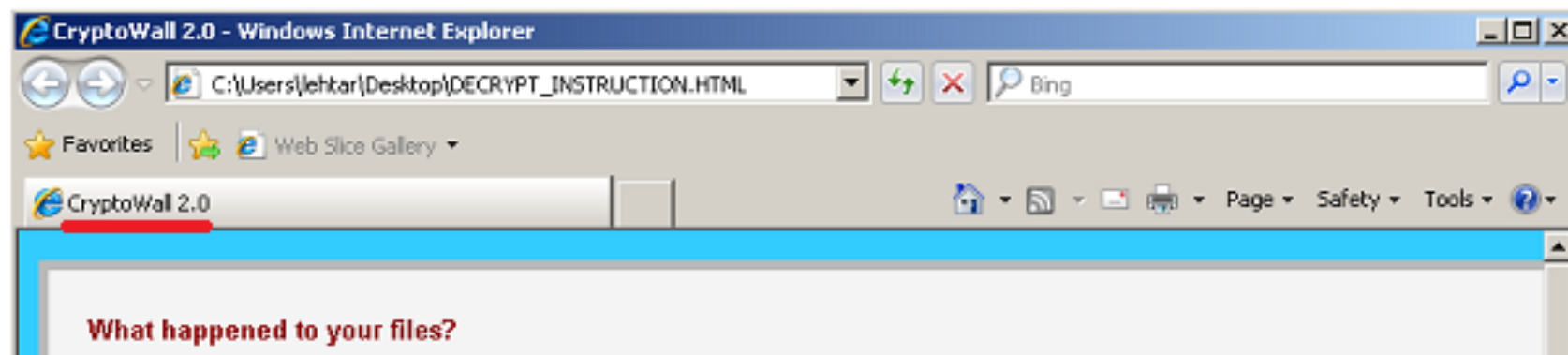
CryptoWall Updated to 2.0

Posted by Artturi @ 1

One of this summer's most followed ransomware families is CryptoWall. Over time CryptoWall has seen minor updates and its core functionality has stayed pretty much the same. Once a machine has been infected, CryptoWall will attempt to encrypt the contents of the victims hard drive and then demand a ransom payment in exchange for the decryption key required to get the files back.

The only major break from this was a few months ago when [we observed a few CryptoWall samples](#) that were using a Tor-component to communicate with their command & control servers. This Tor component was downloaded as an encrypted file from compromised websites. It was then decrypted and used to set up a connection to the Tor network through which the servers could be reached. Interestingly, we only observed a few of these "Torified" versions of CryptoWall. The majority of the samples we have seen have stuck to the original C&C communication method.

That may now have changed. Just yesterday, the first samples of ransomware calling itself "CryptoWall 2.0" [were spotted in the wild](#).



Three ways to destroy Tor

- 1) Legal / policy / media attacks
- 2) Make ISPs hate hosting exit relays
- 3) Make services hate Tor connections
 - Yelp, Wikipedia, Google, Skype, ...
- #3 is getting worse due to centralization (Akamai, Cloudflare) and to outsourcing blacklists



Search Twitter



YOLO Crypto

@yolocrypto



Follow

gonna start silk road 3.0. tor is too hard so
l'm just gonna host it at my home ip address



RETWEETS

122

FAVORITES

101



12:03 PM - 6 Nov 2014

“Threat landscape”

- Application-level threats (Firefox)
- Traffic analysis (observers)
- Possibility of bad relays
- Research is critical (responsibly!)
- Funding diversity