Current events in Tor development.

Roger Dingledine
The Tor Project
https://torproject.org/

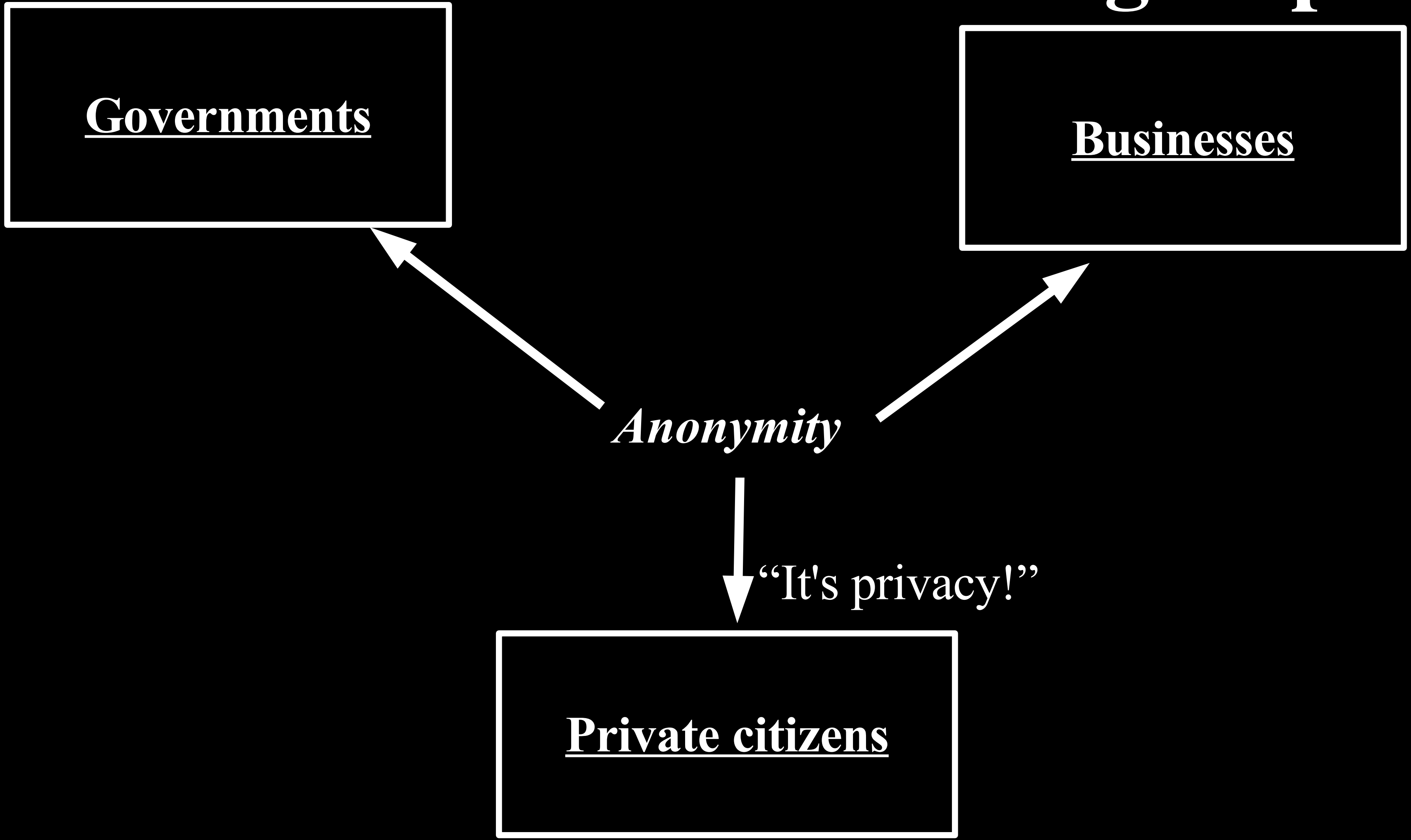
Outline

- Crash course on Tor
- Technical (recent past)
- Policy / law / censorship
- Technical (future)
- Things we need help with

Tor: Big Picture

- Freely available (Open Source), unencumbered.
- Comes with a spec and full documentation: Dresden, Aachen, and Yale groups implemented compatible Java Tor clients; researchers use it to study anonymity.
- 2000 active relays, 200000+ active users, >1Gbit/s.
- Official US 501(c)(3) nonprofit. Three full-time developers, dozens more dedicated volunteers.
- Funding from US DoD, Electronic Frontier Foundation, Voice of America, ...you?

Anonymity serves different interests for different user groups.



Governments

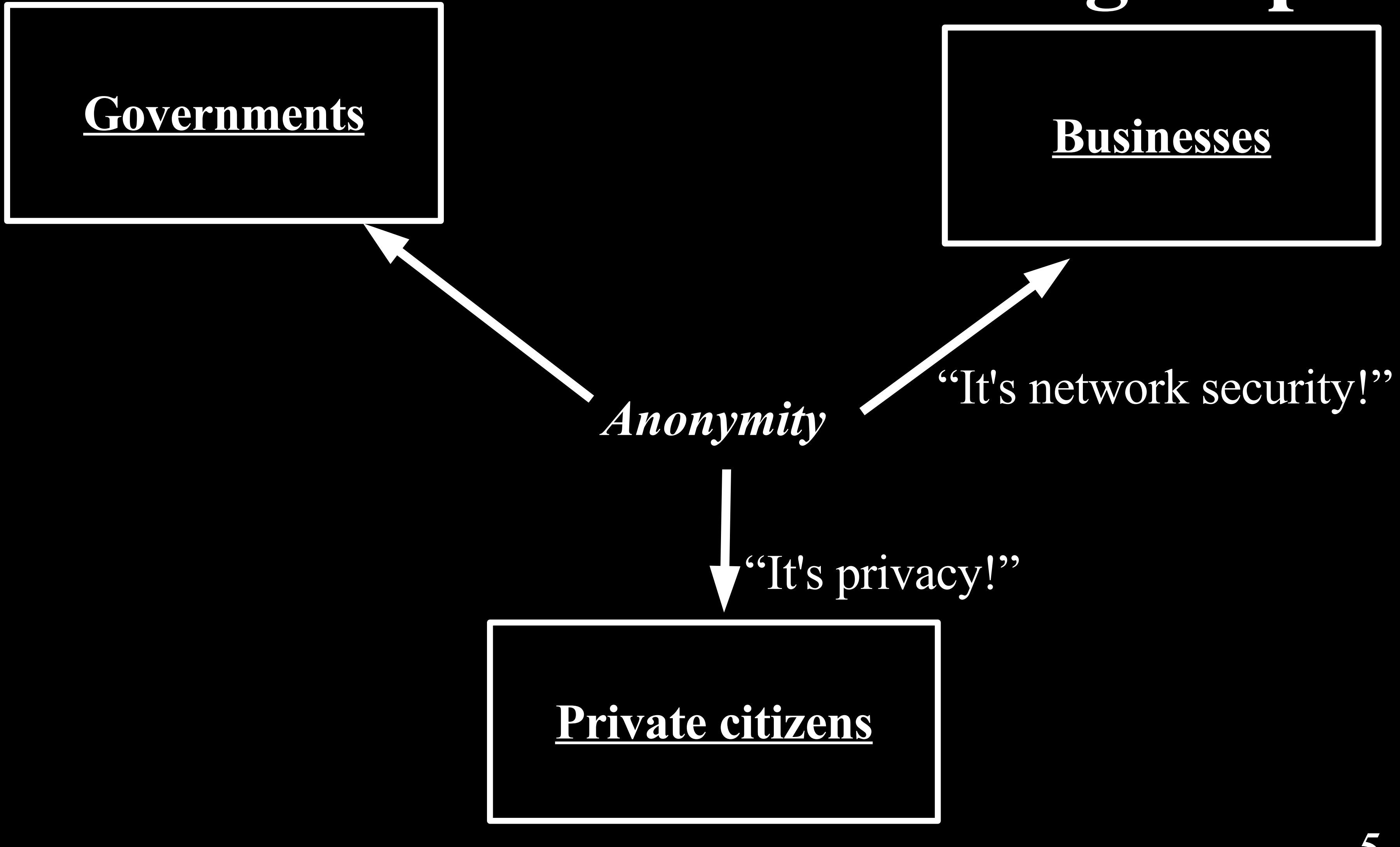
Businesses

Anonymity

“It's privacy!”

Private citizens

Anonymity serves different interests for different user groups.



Governments

Businesses

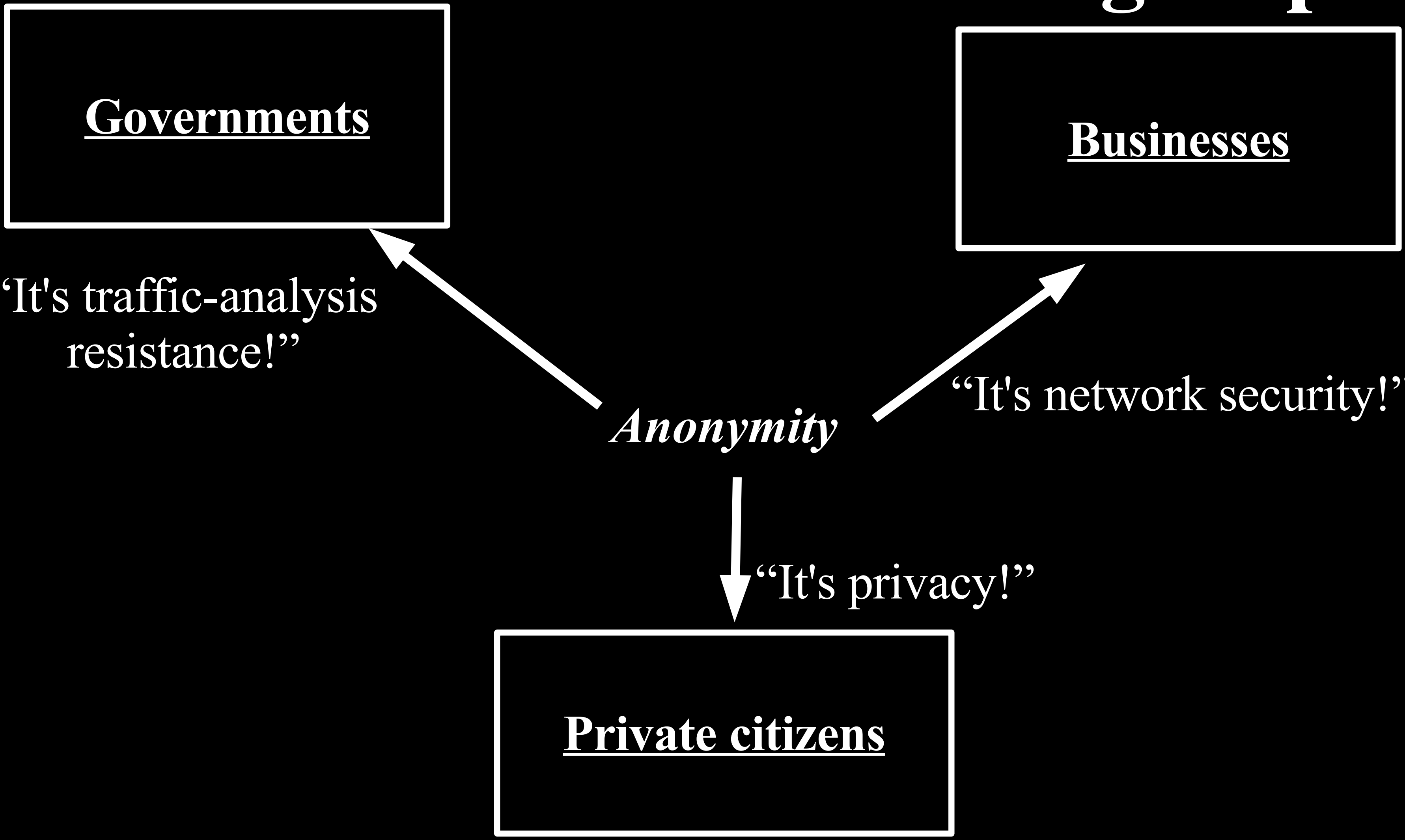
Anonymity

“It's network security!”

“It's privacy!”

Private citizens

Anonymity serves different interests for different user groups.



Governments

“It's traffic-analysis resistance!”

Businesses

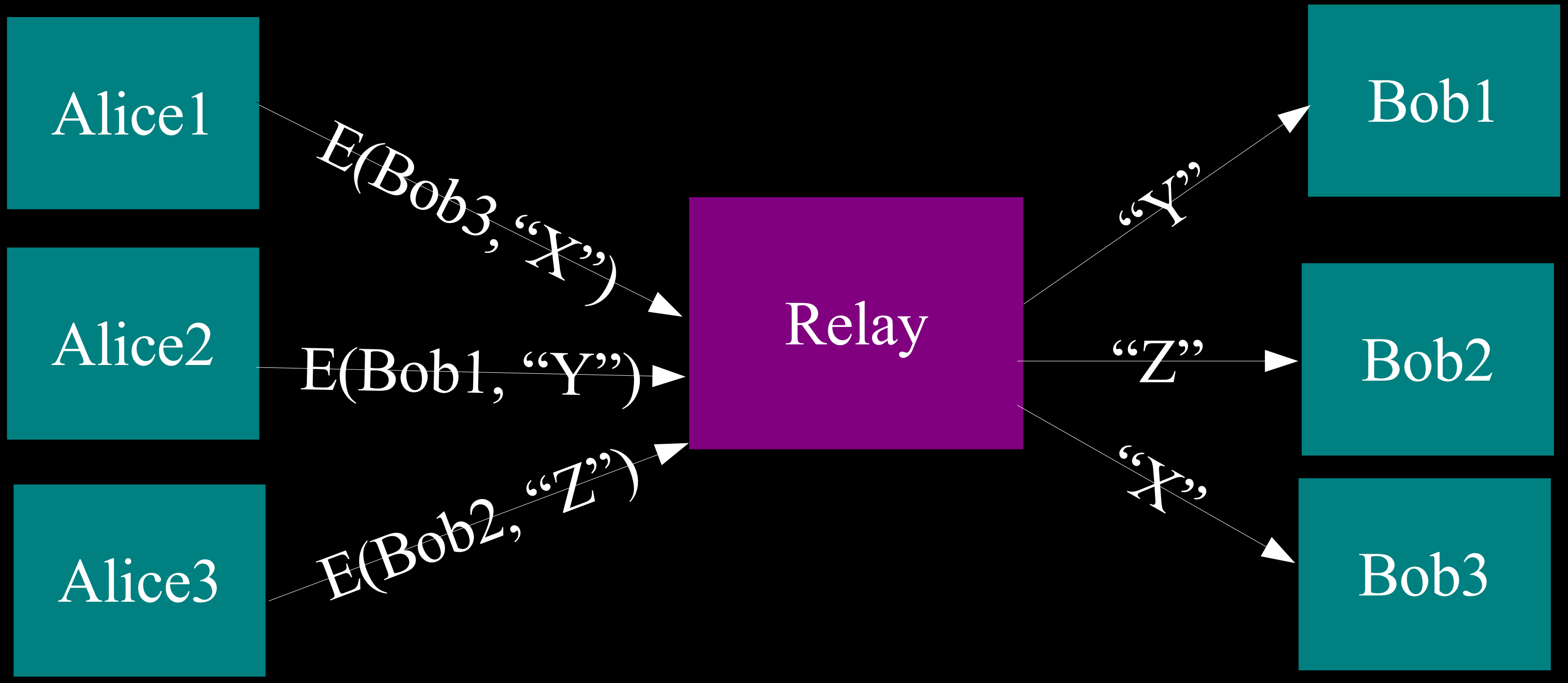
“It's network security!”

Anonymity

“It's privacy!”

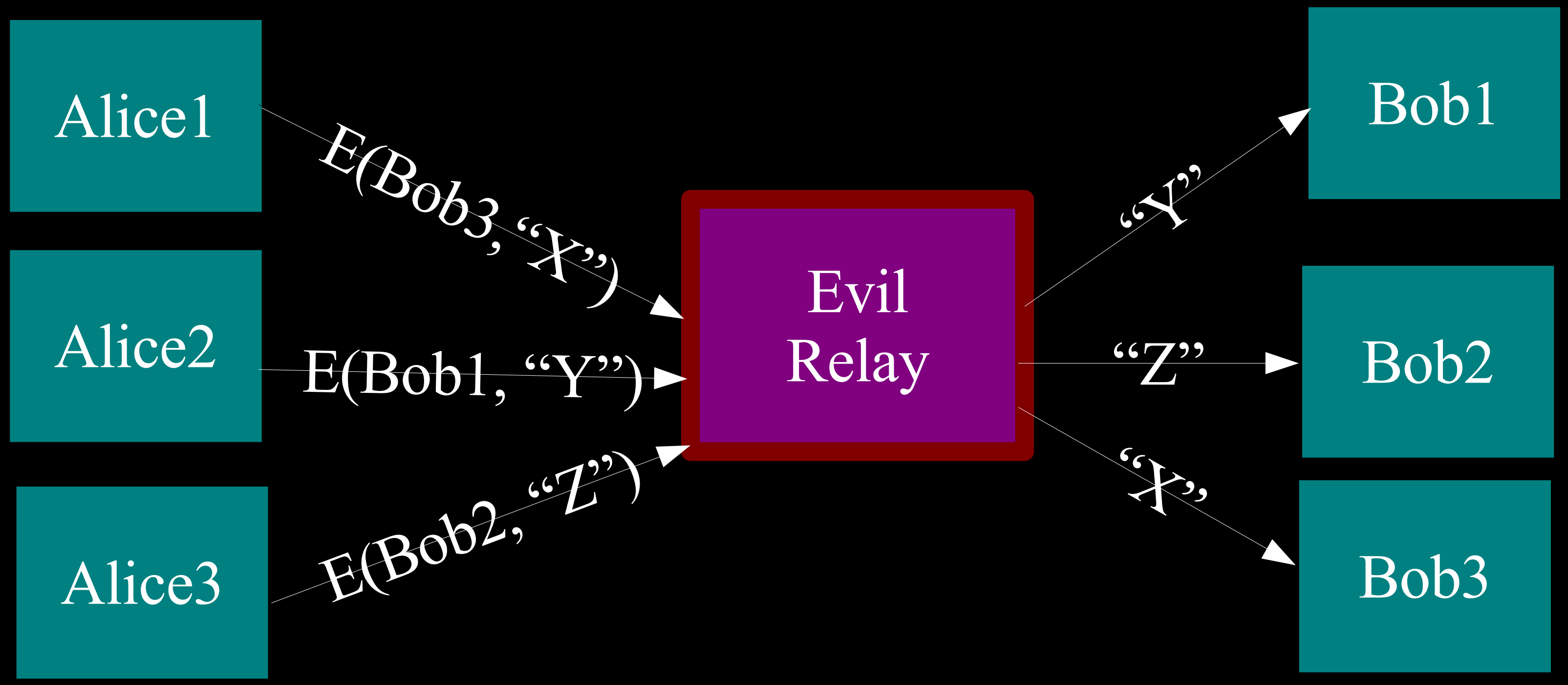
Private citizens

The simplest designs use a single relay to hide connections.



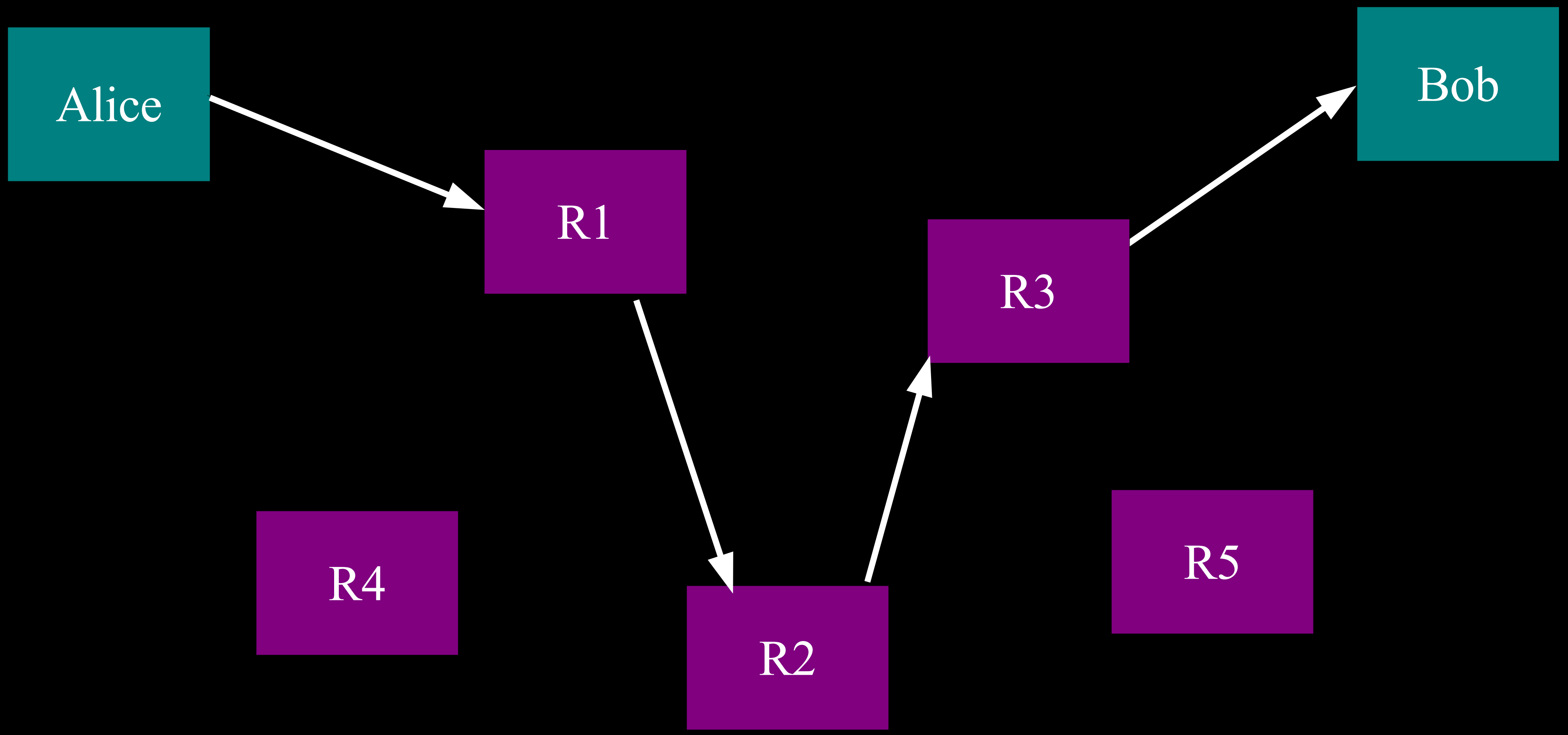
(example: some commercial proxy providers)

But a single relay is a single point of failure.

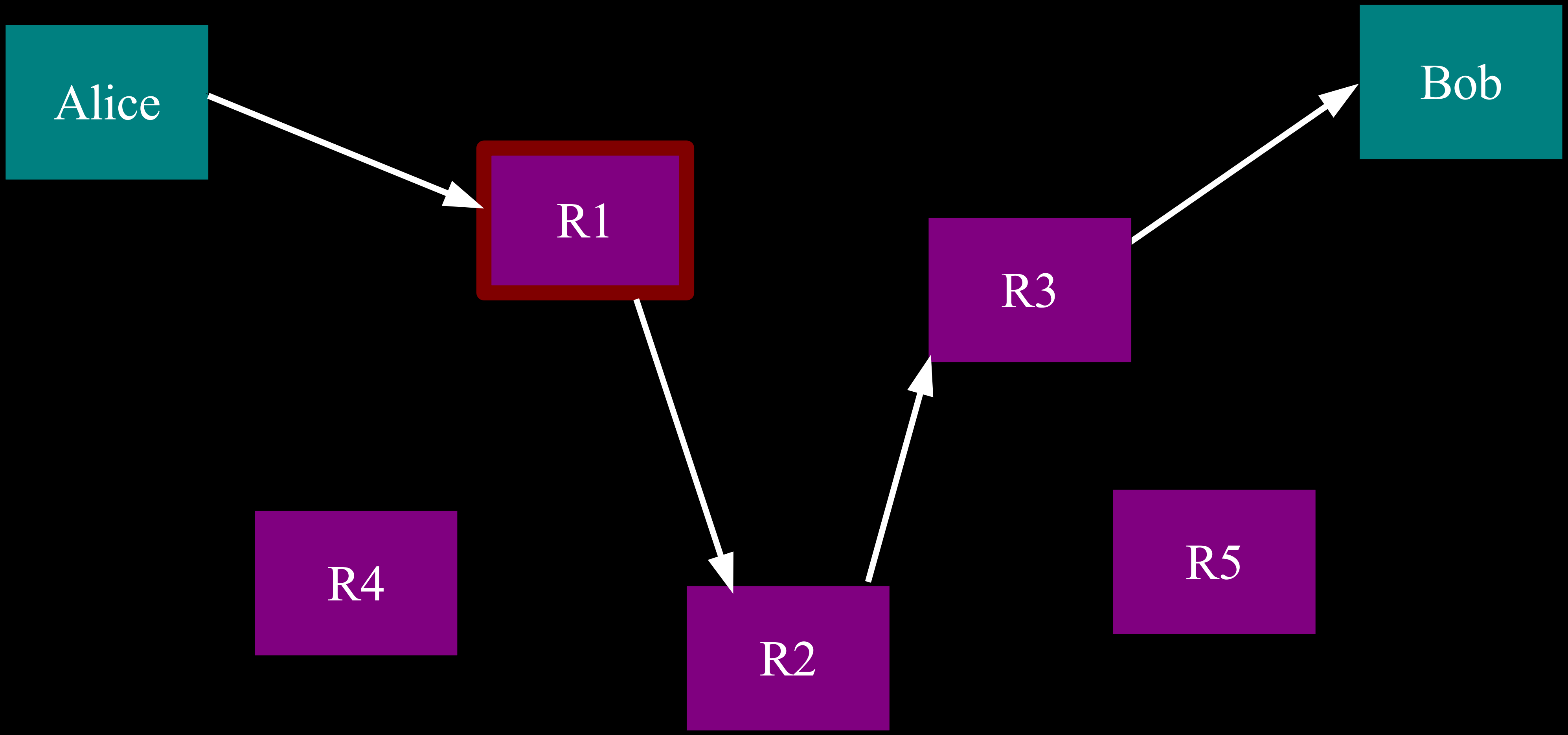


Eavesdropping the relay works too.

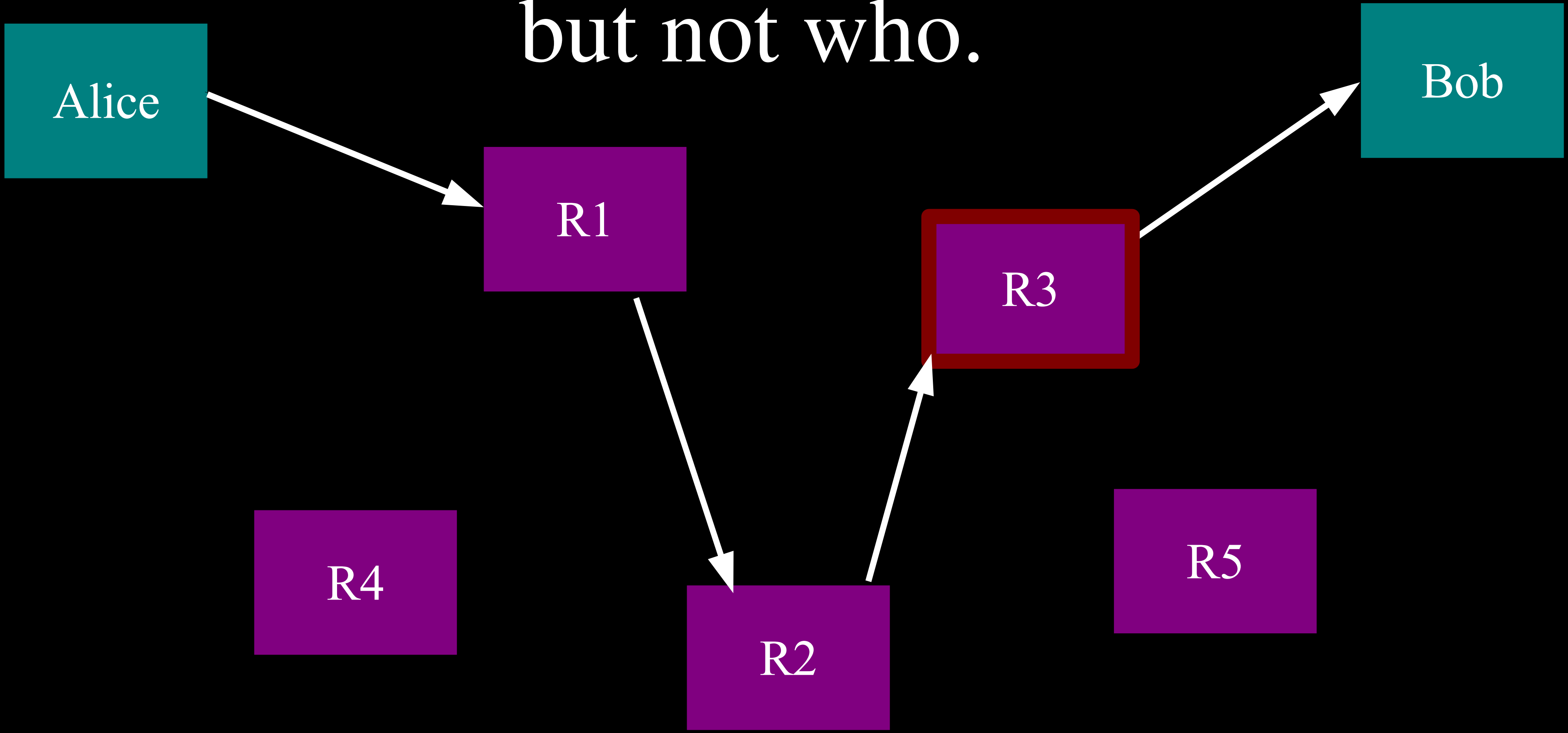
So, add multiple relays so that no single one can betray Alice.



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

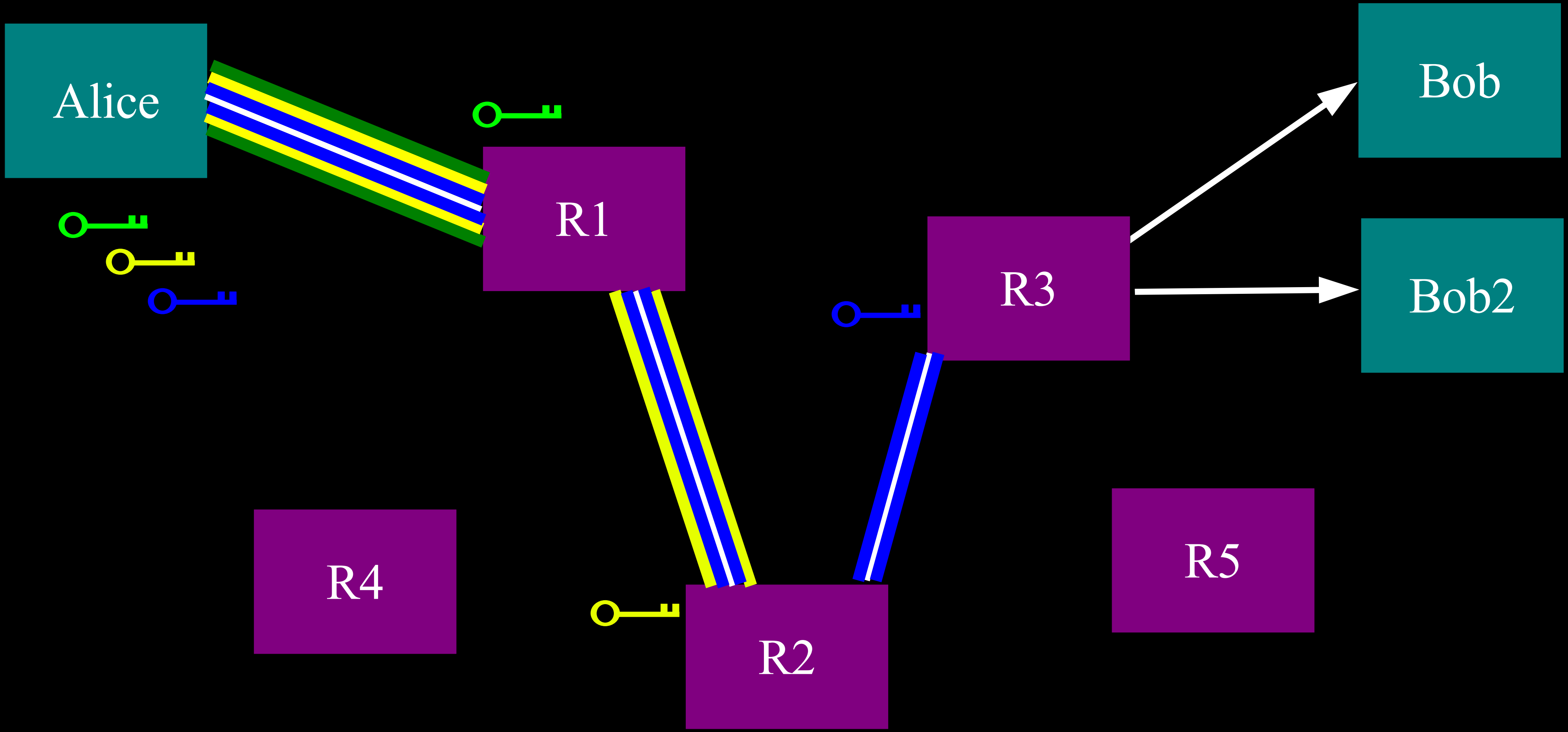


A corrupt final hop can tell that somebody is talking to Bob, but not who.



Alice makes a session key with R1

...And then tunnels to R2...and to R3



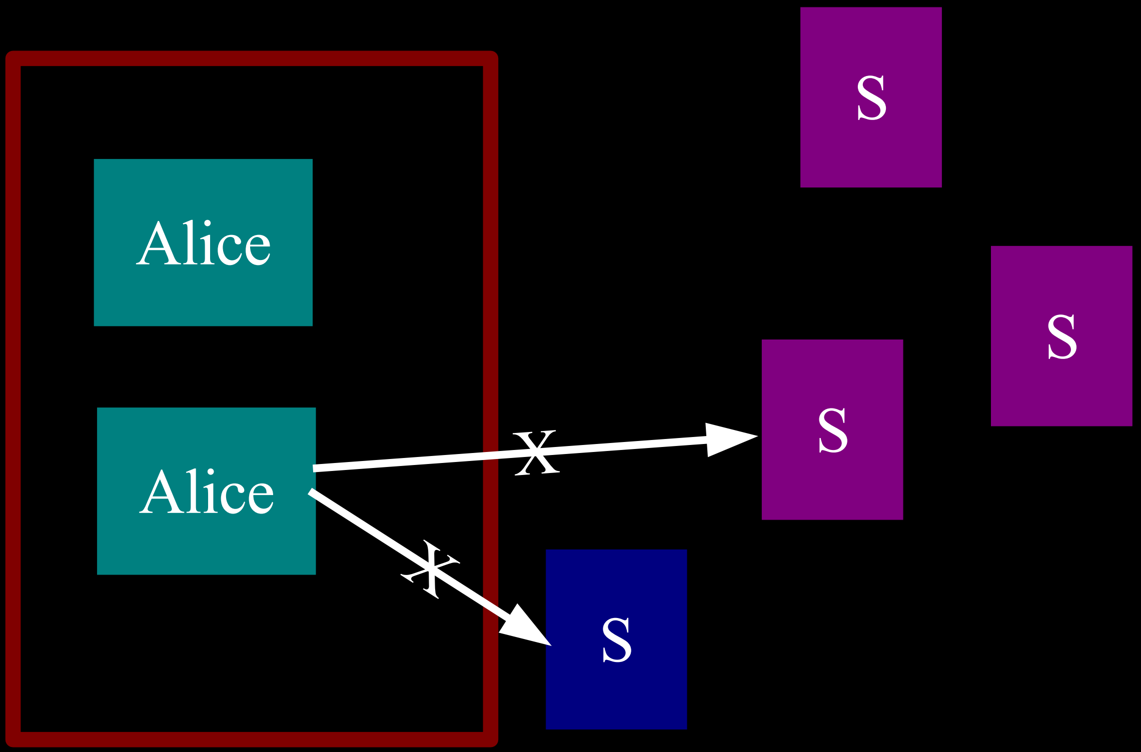
Outline

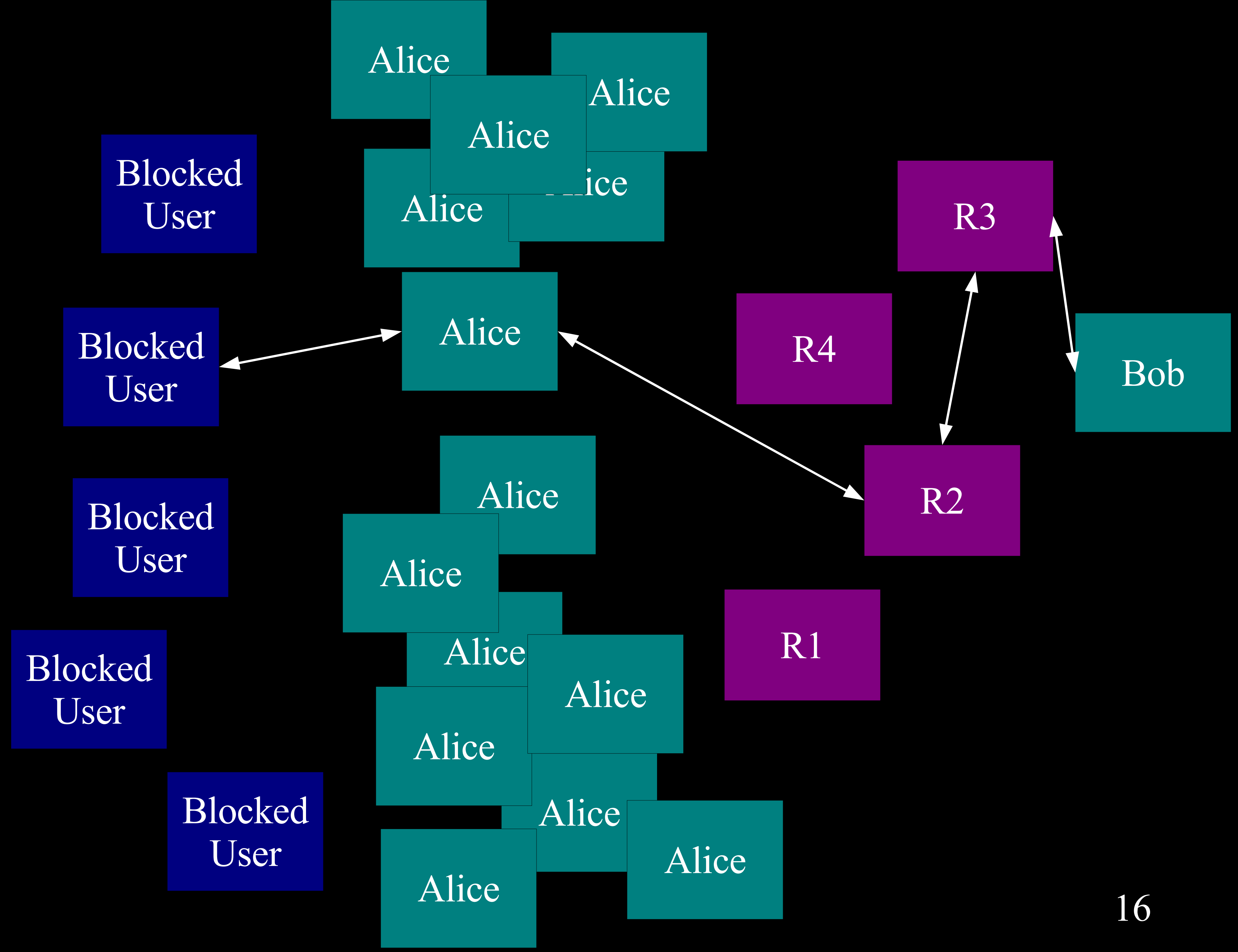
- Crash course in Tor
- *Technical (recent past)*
- Policy / law / censorship
- Technical (future)
- Things we need help with

New v3 directory protocol

- There are two phases of directory information: fetching the network status, and fetching all the descriptors.
- We've changed phase one from fetching 5 network statuses (and computing the majority locally) to fetching just one consensus.
- Still room for optimizing phase two

Governments and other firewalls can just block the whole Tor network.




Alice
Alice
Alice
Alice
Alice
Blocked User
Blocked User
Alice
R3
R4
Bob
R2
Blocked User
Alice
Alice
Alice
Alice
Blocked User
R1
Alice
Alice
Blocked User
Alice
Alice

“Bridge” relays

- Encrypted directory requests (over the same port as other Tor traffic)
- Make Tor's TLS handshake look more like Firefox+Apache
- Integration into Vidalia
- **https://bridges.torproject.org/** or request by unique gmail address

Improved Torbutton

- Torbutton used to just toggle your proxy settings on and off.
- The new version turns off cache, cookies, plugins, doesn't leak your time zone, and blocks many other attacks

Easier for users to be relays

- Rate limit relayed traffic separately from your own traffic
- Automatic IP address detection, bandwidth estimates
- Write limiting as well as read limiting; traffic priorities to make the best use of available bandwidth

Many good research papers in 2007

- Nick Hopper's CCS paper on client latency attacks
- Steven Murdoch's PET paper on sampled traffic analysis at Internet exchanges
- Bauer et al's WPES paper on low-resource Sybil attacks: lying about your bandwidth, uptime, etc
- (Tor's guard nodes are lookingly increasingly good)
- **http://freehaven.net/anonbib/** for many more!

Outline

- Crash course in Tor
- Technical (recent past)
- ***Policy / law / censorship***
- Technical (future)
- Things we need help with

Data retention

- Remember our threat model: even one hop in Germany may be too many
- How many layers of logging are there? If your ISP logs, and *its* ISP logs, ...
- How safe are these logs? Who can access them?
- If nothing is really enforced until 2009, no need to change technical designs immediately. But that means you need to act!

Law enforcement

- Some Tor-induced raids in Germany over the past year(s)
- We really need to teach law enforcement officers more about Tor -- and about Internet security in general.
- Please introduce me to German law enforcement!

Lawyers in Germany

- The US's notion of “legal precedent” makes groups like EFF worthwhile. In Germany, it feels like each case is on its own.
- We need to get more European lawyers involved. Meet them, teach them about Tor. Introduce them to each other.
- Can we make a “German Tor Legal FAQ”?

Snooping on Exit Relays

- Lots of press lately about people watching traffic coming out of Tor. (Ask your lawyer first...)
- Tor hides your location; it doesn't magically encrypt all traffic on the Internet.
- Though Tor *does* protect from your local network.
- Torflow and setting plaintext pop/imap “traps”
- Need to educate users?

File-sharing traffic

- Theory: Tor is slow because a handful of people are running file-sharing apps on it
- We could traffic shape high-volume flows. But: BitTorrent is designed to resist this.
- We could run protocol analysis tools on the exit relays, and snipe bad protocols
- But: liability, neutrality

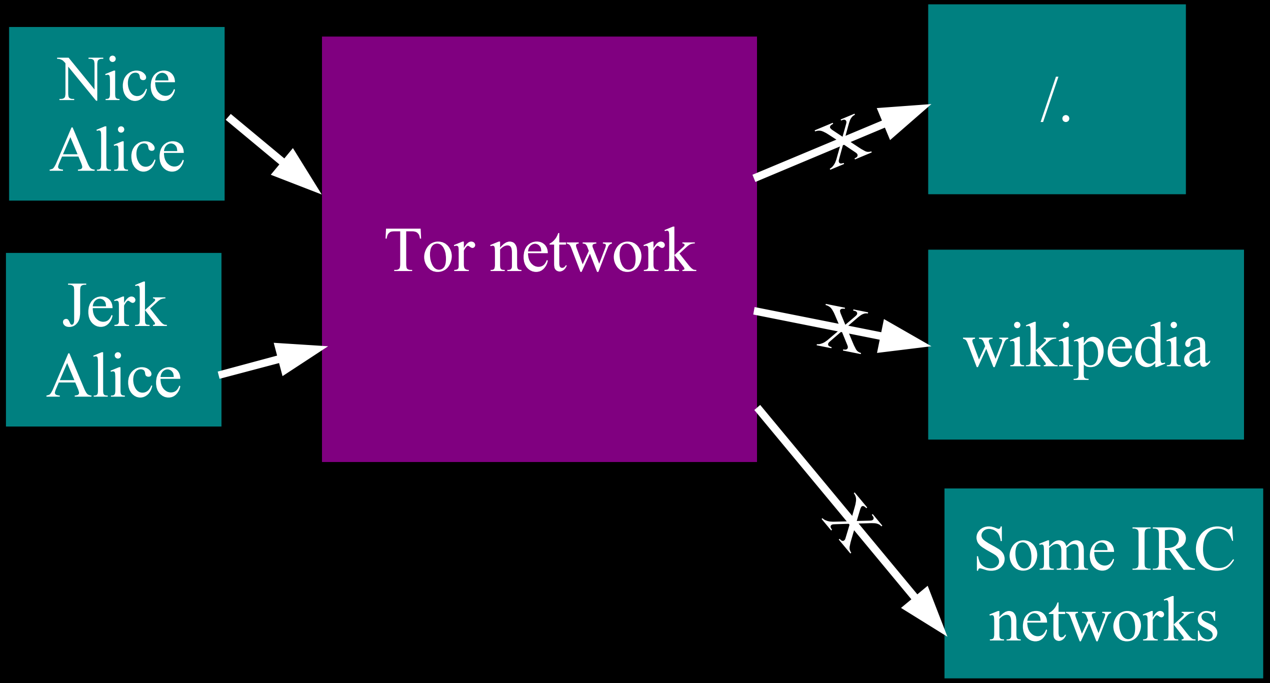
Who runs the relays?

- At the beginning, you needed to know me to have your relay considered“verified”.
- We've automated much of the “is it broken?” checking.
- Still a tension between having lots of relays and knowing all the relay operators

GeoIP reporting?

- We'd really like to get a sense of how many people are using the Tor network, and from where, so we can know what to focus on.
- But it's an anonymity network!
- Directory mirrors can see who asks for info, but we'd like to fix that (“directory guards”)
- Perhaps relays report aggregated daily stats?

Problem: Abusive users get the whole network blocked.



Internet services: blocking (1)

- Many admins think Tor has 6 users. If they see 1 jerk, they conclude that Tor is stupid.
- Right now Wikipedia blocks many many thousands of IP addresses. And they still have problems: AOL, open proxies, Tor, ...

Internet services: blocking (2)

- Wikipedia doesn't want to introduce barriers to contributors. But they could add speedbumps only for IPs they currently block!
- Accounts need to prove that they're worthwhile: manually verify the first few edits, and whitelist after that.
- Should send the abusers back to their open proxies, AOL, neighbor's wireless, etc

Internet services: blocking (3)

- Other options that don't require as many changes to Wikipedia
- Nym (Jason Holt) and Nymble (Dartmouth) make users demonstrate a scarce resource (e.g. an IP address). Then they let websites block further edits from that user without needing to learn his IP address.

Internet services: blocking (4)

- Tor's “DNS exit list” gives an RBL-style interface for looking up whether a given connection is from a Tor exit relay. We want to make it as easy as possible for websites to block accurately; then help them handle Tor.
- Note that blocking connections *from* the Tor network and blocking connections *to* the Tor network are different.

Outline

- Crash course in Tor
- Technical (recent past)
- Policy / law / censorship
- *Technical (future)*
- Things we need help with

Relay by default

- Vidalia should learn how to talk UPNP to routers
- Should auto rate limit so we don't overfill the user's pipe?
- How to scale the network? (Dir info size grows with # of relays; so does # of sockets)
- Windows networking is ... unique.

Incentives to relay

- Give people better performance if they relay?
- Need to be careful – many ways to screw up anonymity
- Let directory authorities do audits and assign gold stars to well-behaving relays in the directory consensus. Circuits from those relays get priority.
- If it adds enough relays, *everybody* benefits.

UDP Transport

- Tor's use of TCP means relays use many many sockets. It also means hop-by-hop congestion recovery. And we can only transport TCP.
- DTLS now exists.
- More research / hacking remains.

Packaging

- Tor browser bundle: Tor, Vidalia, Firefox, Torbutton, Polipo for USB stick
- JanusVM, Xerobank virtual machine
- Incognito LiveCD
- Wireless router images?
- Firefox plugin?

Better load balancing

- Upcoming NDSS paper by Nikita Borisov and Robin Snader on more accurate (and less gameable) bandwidth estimations.
- Mike Perry's measurements from TorFlow
- 3 hops vs 2 hops

Outline

- Crash course in Tor
- Technical (recent past)
- Policy / law / censorship
- Technical (future)
- *Things we need help with*

Things we need help with (1)

- A UPNP lib for Vidalia
- A web-based translation interface for Qt (Vidalia) and our web pages
- Check out our TODO list and the volunteer.html page

Things we need help with (2)

- More relays. More bridges. More funding.
- Introductions to LEO in Berlin / Germany
- Privacy advocates in Germany – and lawyers!
- Best practices docs for using Tor with various applications, and in various contexts
- Google summer-of-code apps in the summer?