Cryptoparty

redshiftzero
jen@redshiftzero.com

Southside Hackerspace: Chicago

August 30, 2014

What are we going to do today?

- Introductions
- Context
- Basic cryptography/security concepts
- Setting up tools: Tor Browser Bundle
- Open time: Q and A, lightning talks, keysigning
- Already use Tor? Please help teach!

Why should we care about privacy?

- Some people have something to hide, but not something the government should have the power to know: e.g. affairs, being in the closet, medical information.
- You may not have anything to hide, but the government may think you do: e.g. bloated terrorist watch lists that are hard to remove oneself from.
- Are you sure you have nothing to hide? There are lots of laws.
- People hide many things even though they're not wrong. e.g. nudity.
- You may not care about hiding it, but you may still be discriminated against because of it. e.g. a company decides that statistically a behavior might suggest you are a poor risk
- Privacy is important for dissidents and democracy. It helps maintain the balance of power between individuals and the state.

Why should we care about privacy?

- Some people have something to hide, but not something the government should have the power to know: e.g. affairs, being in the closet, medical information.
- You may not have anything to hide, but the government may think you do: e.g. bloated terrorist watch lists that are hard to remove oneself from.
- Are you sure you have nothing to hide? There are lots of laws.
- People hide many things even though they're not wrong. e.g. nudity.
- You may not care about hiding it, but you may still be discriminated against because of it. e.g. a company decides that statistically a behavior might suggest you are a poor risk
- Privacy is important for dissidents and democracy. It helps maintain the balance of power between individuals and the state.

Why should we care about privacy?

- Some people have something to hide, but not something the government should have the power to know: e.g. affairs, being in the closet, medical information.
- You may not have anything to hide, but the government may think you do: e.g. bloated terrorist watch lists that are hard to remove oneself from.
- Are you sure you have nothing to hide? There are lots of laws.
- People hide many things even though they're not wrong. e.g. nudity.
- You may not care about hiding it, but you may still be discriminated against because of it. e.g. a company decides that statistically a behavior might suggest you are a poor risk
- Privacy is important for dissidents and democracy. It helps maintain the balance of power between individuals and the state.

Why should we care about privacy?

- Some people have something to hide, but not something the government should have the power to know: e.g. affairs, being in the closet, medical information.
- You may not have anything to hide, but the government may think you do: e.g. bloated terrorist watch lists that are hard to remove oneself from.
- Are you sure you have nothing to hide? There are lots of laws.
- People hide many things even though they're not wrong. e.g. nudity.
- You may not care about hiding it, but you may still be discriminated against because of it. e.g. a company decides that statistically a behavior might suggest you are a poor risk
- Privacy is important for dissidents and democracy. It helps maintain the balance of power between individuals and the state.

Why should we care about privacy?

- Some people have something to hide, but not something the government should have the power to know: e.g. affairs, being in the closet, medical information.
- You may not have anything to hide, but the government may think you do: e.g. bloated terrorist watch lists that are hard to remove oneself from.
- Are you sure you have nothing to hide? There are lots of laws.
- People hide many things even though they're not wrong. e.g. nudity.
- You may not care about hiding it, but you may still be discriminated against because of it. e.g. a company decides that statistically a behavior might suggest you are a poor risk
- Privacy is important for dissidents and democracy. It helps maintain the balance of power between individuals and the state.

Why should we care about privacy?

- Some people have something to hide, but not something the government should have the power to know: e.g. affairs, being in the closet, medical information.
- You may not have anything to hide, but the government may think you do: e.g. bloated terrorist watch lists that are hard to remove oneself from.
- Are you sure you have nothing to hide? There are lots of laws.
- People hide many things even though they're not wrong. e.g. nudity.
- You may not care about hiding it, but you may still be discriminated against because of it. e.g. a company decides that statistically a behavior might suggest you are a poor risk
- Privacy is important for dissidents and democracy. It helps maintain the balance of power between individuals and the state.

Lessons from Snowden

- The NSA is grabbing up lots of data. Their motivation is to collect every communication that exists, everywhere.
- "Properly implemented strong cryptosystems are one of the few things we can rely on"
- But endpoint security is an issue.
- If the government and corporations don't care about protecting our privacy, we can do it for ourselves.

Security Mindset

There's no such thing as absolute security. Consider your home.

You're balancing risk and security. You want to exert just more effort than your adversary is willing to commit.

Consider your threat model:

- What do you want to keep private? e.g. your .porn directory, your stolen government documents, the fact that you have cancer, your sexuality
- Who wants to know? e.g. Your employer? Nosy kids in coffee shops? Criminals? Police? FBI? NSA?
- What can they do to find out? e.g. Dragnet surveillance vs. targeted surveillance
- What happens if they succeed? e.g. embarassment to death, imprisonment

Then you make a security plan.

How can we communicate securely in the presence of third parties? Cryptography!

How can we communicate securely in the presence of third parties? Cryptography!

General Computer Security Advice

- Keep your system (both your OS and applications) up to date with security updates.
- Don't run code from people or organizations you don't trust: Email attachments!
- Free and open source software is better for security: Linux!
- Don't reuse passwords if possible, use long passwords, and use two-factor authentication if available. Use a password manager if that helps (e.g. Keepass).
- Use HTTPS as much as possible: Install **HTTPS Everywhere**, a browser extension.

General Computer Security Advice

- Keep your system (both your OS and applications) up to date with security updates.
- Don't run code from people or organizations you don't trust: Email attachments!
- Free and open source software is better for security: Linux!
- Don't reuse passwords if possible, use long passwords, and use two-factor authentication if available. Use a password manager if that helps (e.g. Keepass).
- Use HTTPS as much as possible: Install **HTTPS Everywhere**, a browser extension.

General Computer Security Advice

- Keep your system (both your OS and applications) up to date with security updates.
- Don't run code from people or organizations you don't trust: Email attachments!
- Free and open source software is better for security: Linux!
- Don't reuse passwords if possible, use long passwords, and use two-factor authentication if available. Use a password manager if that helps (e.g. Keepass).
- Use HTTPS as much as possible: Install **HTTPS Everywhere**, a browser extension.

General Computer Security Advice

- Keep your system (both your OS and applications) up to date with security updates.
- Don't run code from people or organizations you don't trust: Email attachments!
- Free and open source software is better for security: Linux!
- Don't reuse passwords if possible, use long passwords, and use two-factor authentication if available. Use a password manager if that helps (e.g. Keepass).
- Use HTTPS as much as possible: Install **HTTPS Everywhere**, a browser extension.

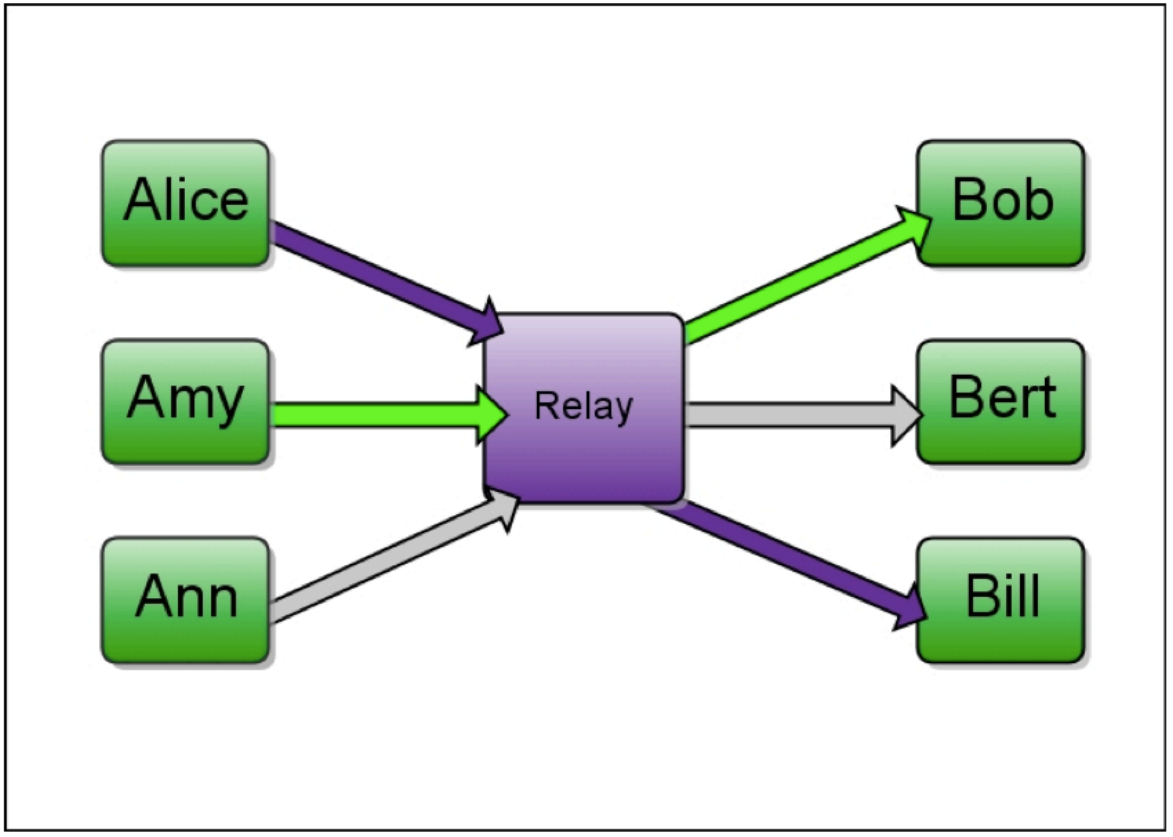
General Computer Security Advice

- Keep your system (both your OS and applications) up to date with security updates.
- Don't run code from people or organizations you don't trust: Email attachments!
- Free and open source software is better for security: Linux!
- Don't reuse passwords if possible, use long passwords, and use two-factor authentication if available. Use a password manager if that helps (e.g. Keepass).
- Use HTTPS as much as possible: Install **HTTPS Everywhere**, a browser extension.

Anonymity Systems

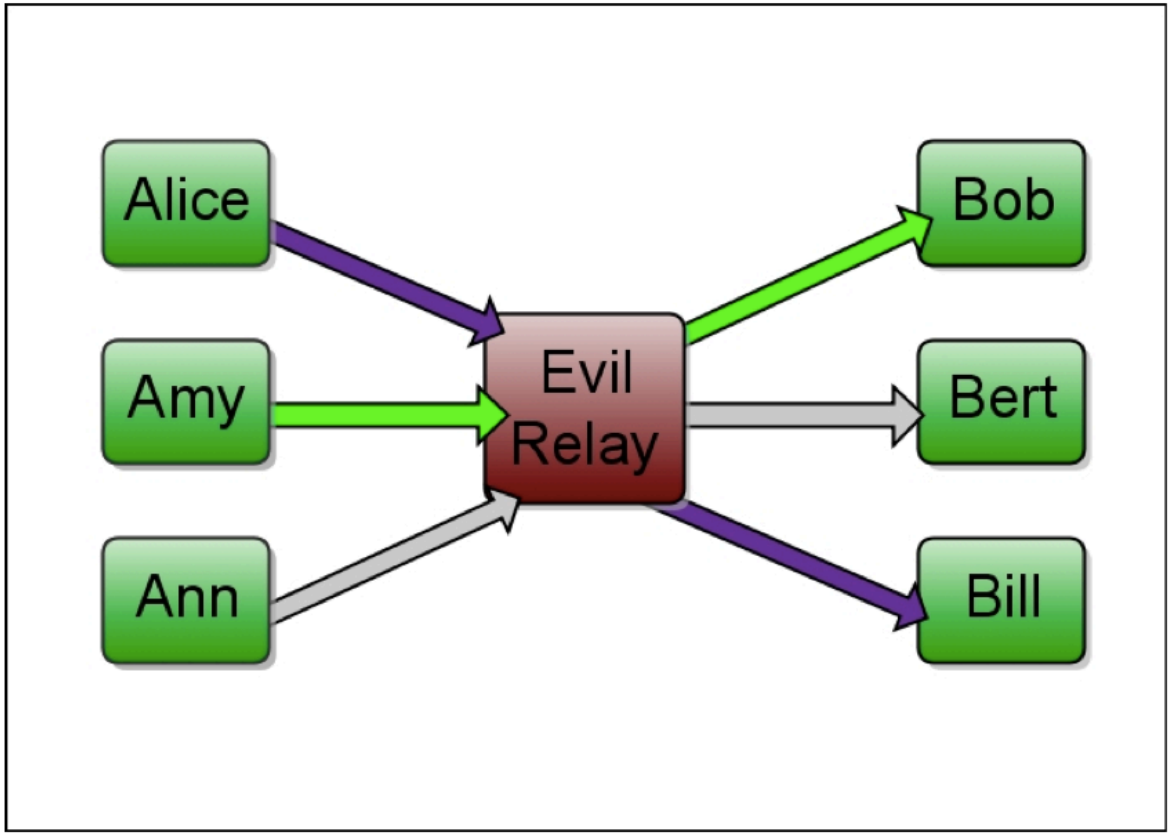
Anonymity means you can't tell who did what. **This isn't just crypto.**

One solution: Use a VPN (Virtual Private Network).



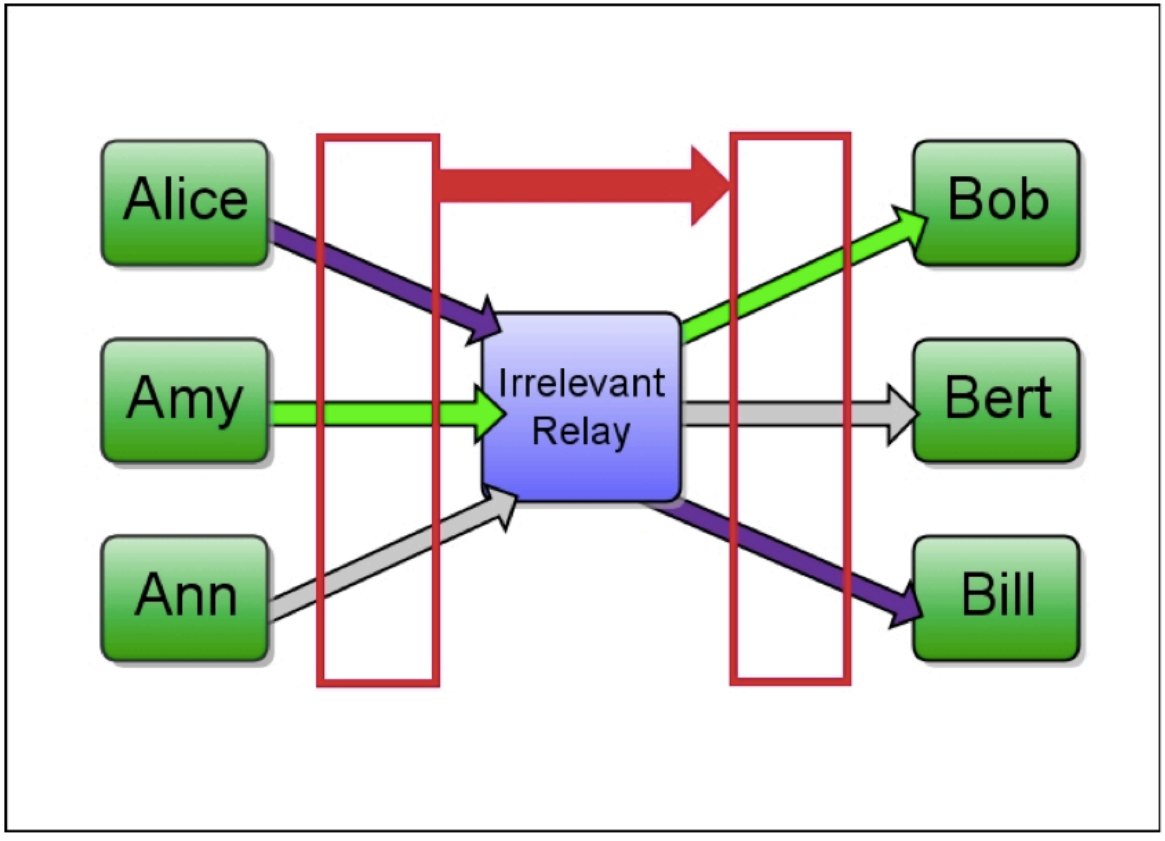
Anonymity Systems

Issues arise if the VPN provider cooperates with the adversary or is compromised.

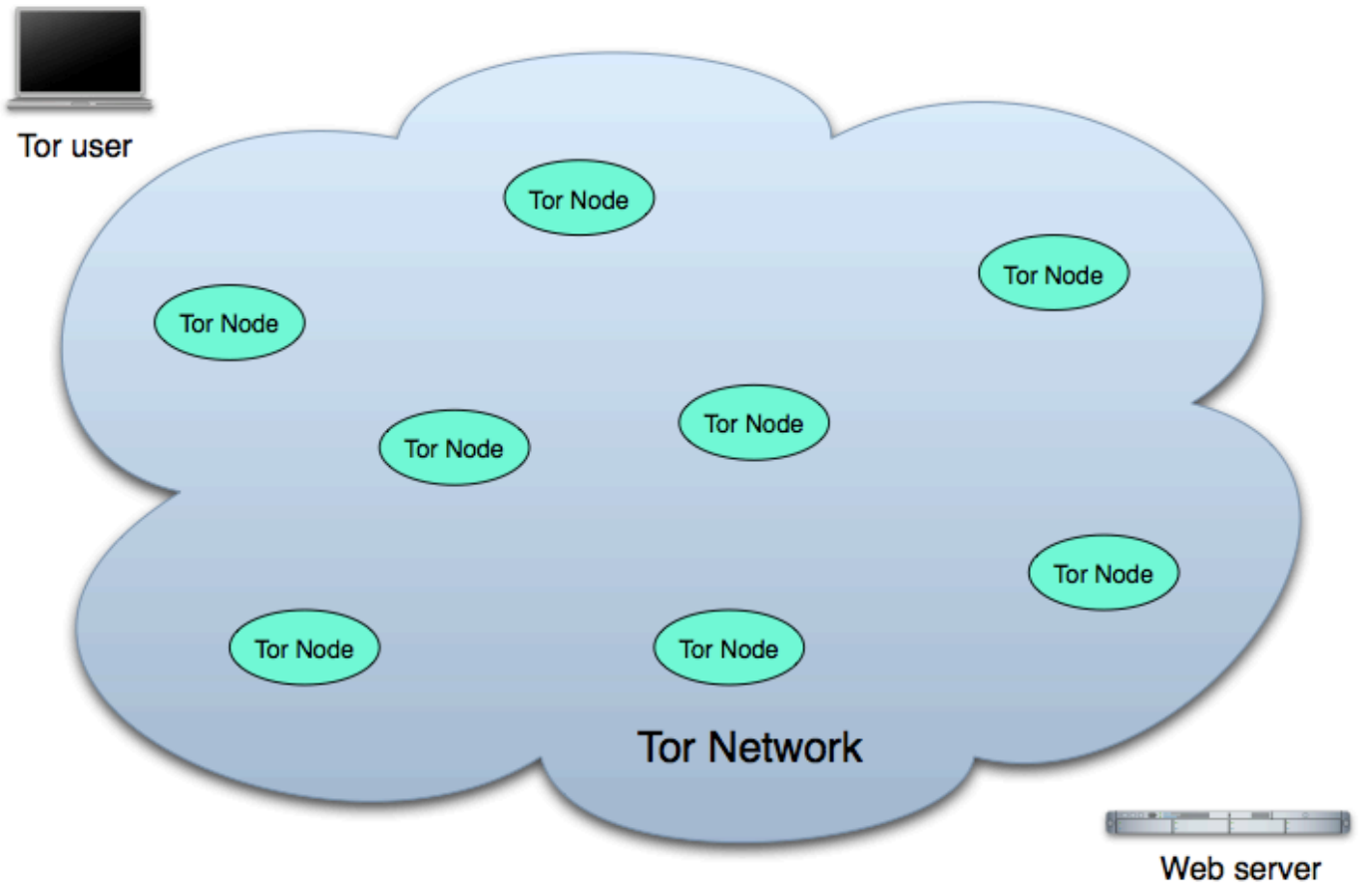


Anonymity Systems

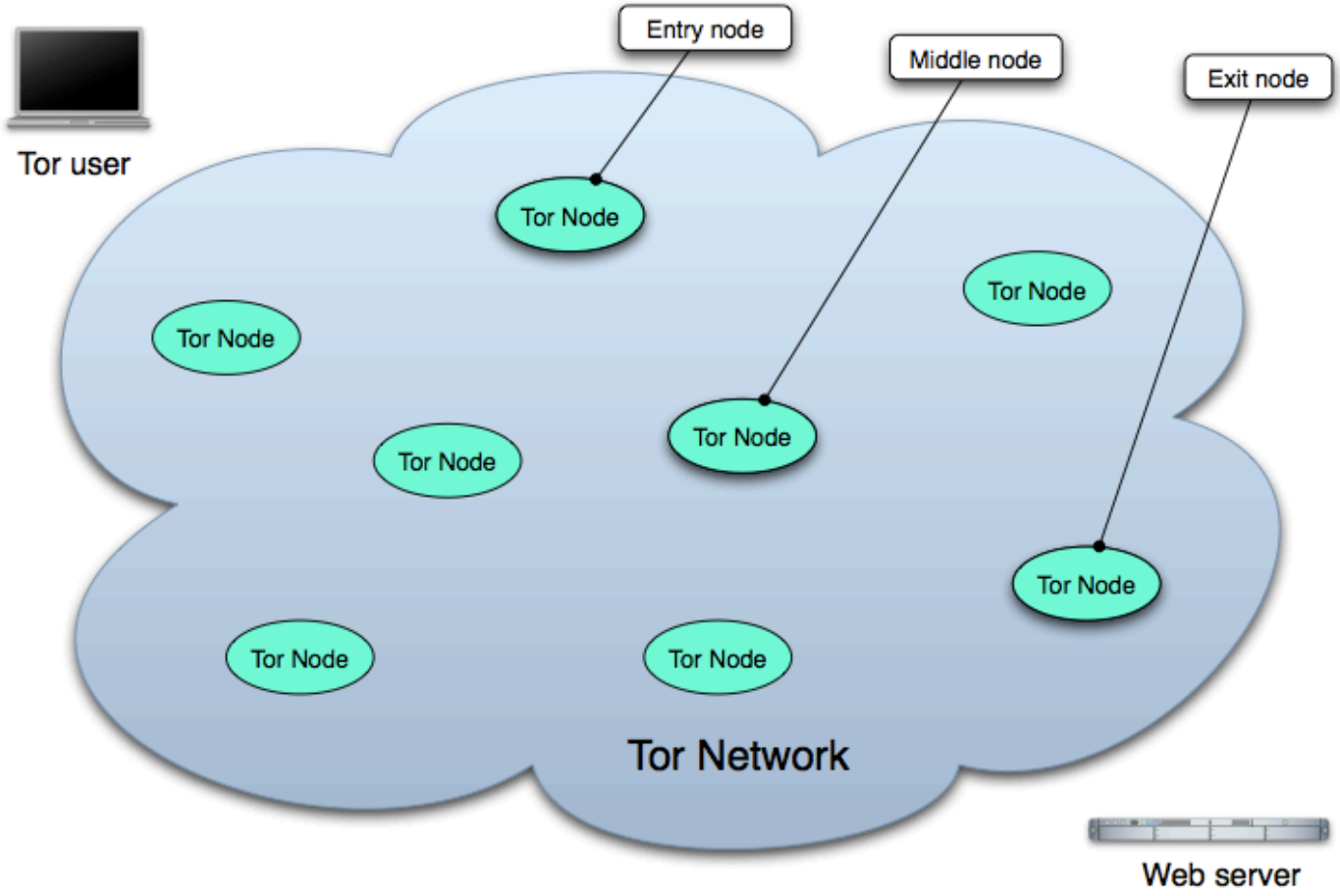
Even if the VPN provider does not cooperate, an adversary watching all the inputs and outputs to this single server could potentially deanonymize users.



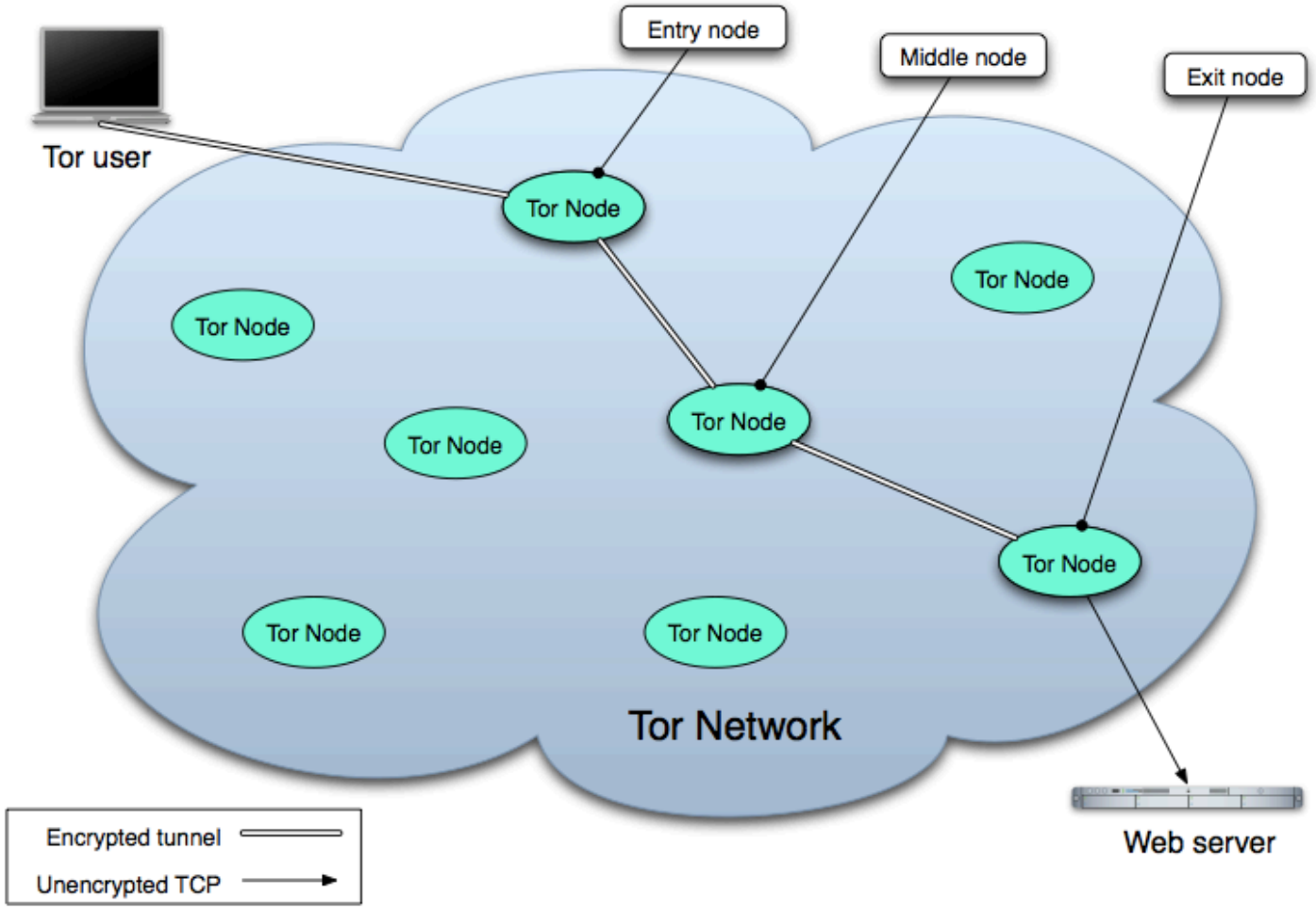
So what to do?


Tor user
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Network
Web server

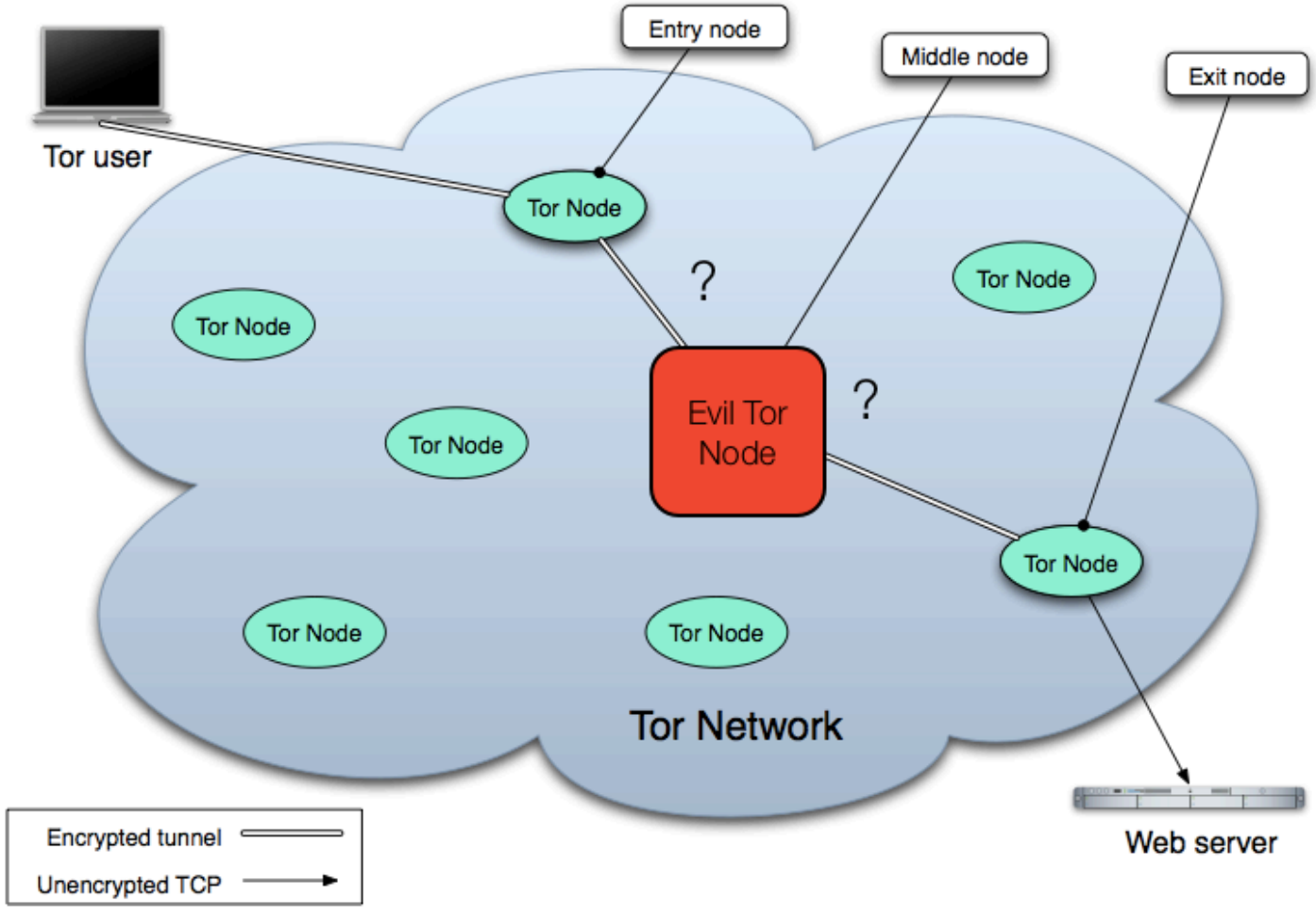
So what to do?


Entry node
Middle node
Exit node
Tor user
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Network
Web server

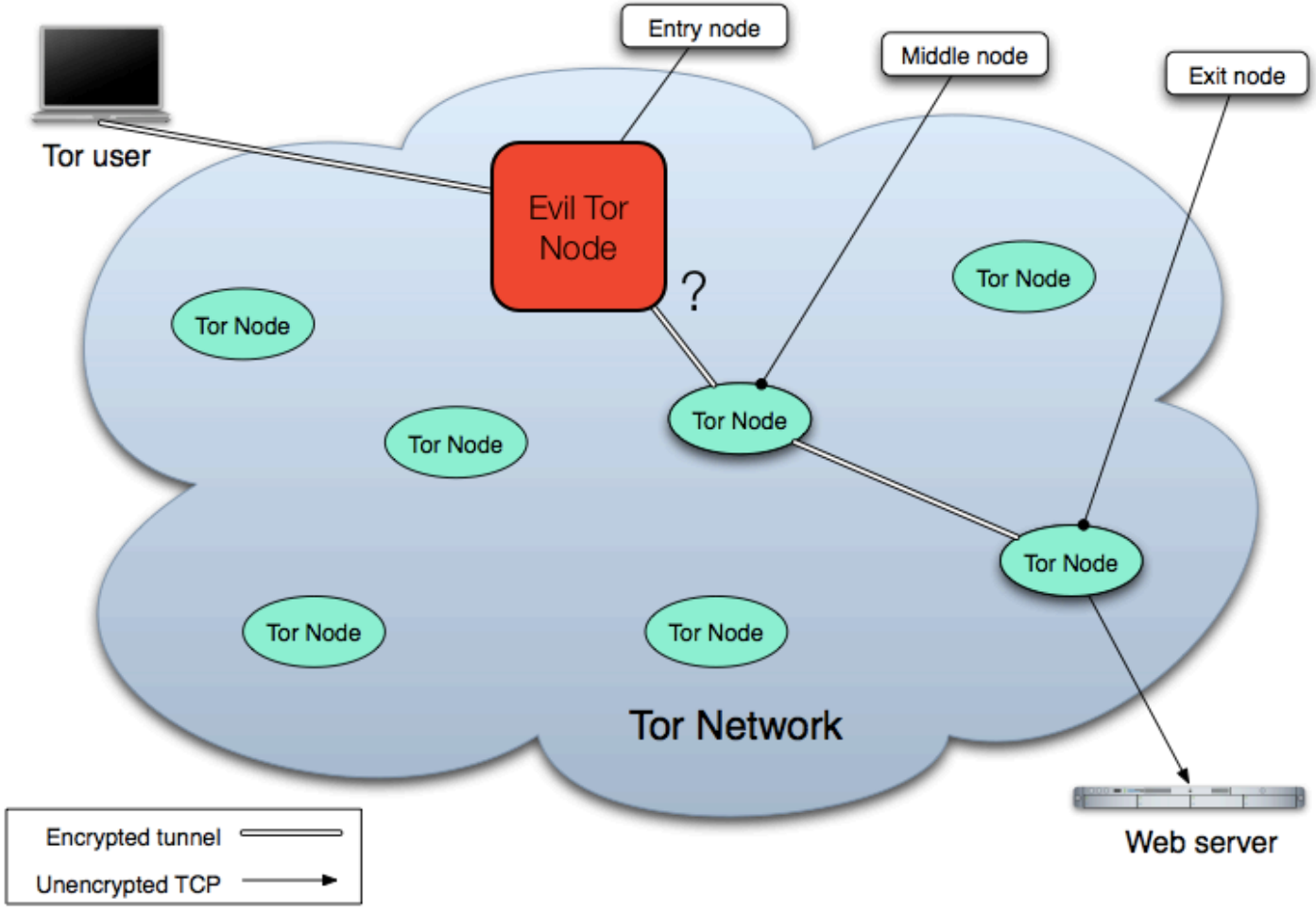
So what to do?


Entry node
Middle node
Exit node
Tor user
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Network
Web server
Encrypted tunnel
Unencrypted TCP

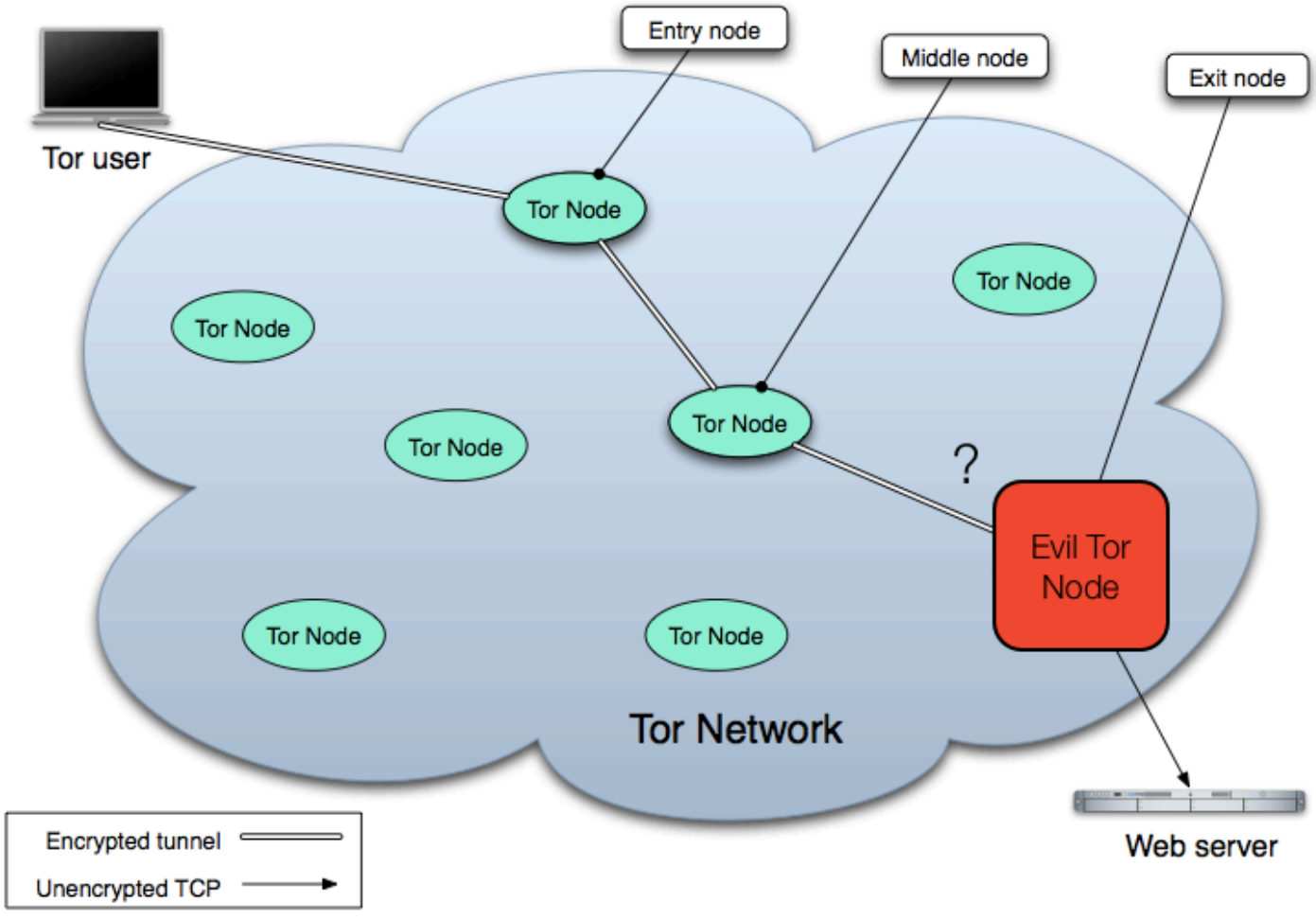
So what to do?


Entry node
Middle node
Exit node
Tor user
Tor Node
?
Tor Node
Tor Node
Evil Tor Node
?
Tor Node
Tor Node
Tor Node
Tor Node
Tor Network
Web server
Encrypted tunnel
Unencrypted TCP

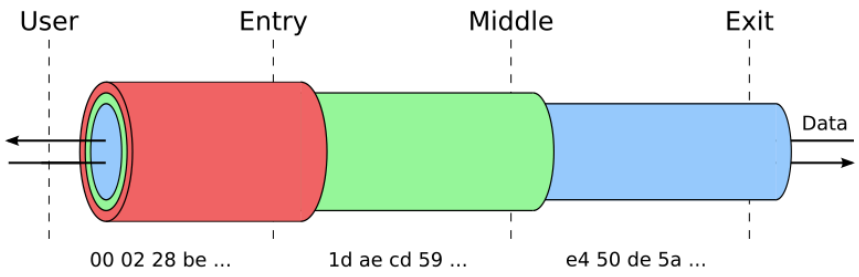
So what to do?


Entry node
Middle node
Exit node
Tor user
Evil Tor Node
?
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
Tor Network
Web server
Encrypted tunnel
Unencrypted TCP

So what to do?


Entry node
Middle node
Exit node
Tor user
Tor Node
Tor Node
Tor Node
Tor Node
Tor Node
?
Evil Tor Node
Tor Node
Tor Node
Tor Network
Web server
Encrypted tunnel
Unencrypted TCP

Tor



Relays data through ∼6000 volunteer relays. Encrypted connections between the client and Tor relays.
Slower than a VPN, but provides more anonymity (but VPNs can still be useful).

The Tor Project is a 501c3 non-profit dedicated to the development of anonymity tools. They write the Tor Browser Bundle, which is software that enables one to use the Tor network.

Tor

Low latency: Tor doesn't put in delays between relays (not intentionally at least). Makes it usable, but potentially vulnerable to end-to-end correlation attacks (traffic analysis).

While these traffic analysis attacks are possible, the NSA's own documents reveal they have a very difficult time de-anonymizing Tor users:

> *We will never be able to de-anonymize all Tor users all the time. . . with manual analysis we can de-anonymize a very small fraction of Tor users. . . no success de-anonmizing a user on demand*

[1]

[1] Full details here: theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document

Tor: Usability Issues 1

- Keep Tor Browser Bundle (like all software) updated. TBB will load check.torproject.org and verify you are using the latest version. PAY ATTENTION TO THIS.
- The exit nodes see your unencrypted traffic unless you are using end-to-end encryption. TBB includes HTTPS everywhere.
- Flash is disabled for privacy reasons. Use HTML5 video.

Tor: Usability Issues 1

- Keep Tor Browser Bundle (like all software) updated. TBB will load check.torproject.org and verify you are using the latest version. PAY ATTENTION TO THIS.
- The exit nodes see your unencrypted traffic unless you are using end-to-end encryption. TBB includes HTTPS everywhere.
- Flash is disabled for privacy reasons. Use HTML5 video.

Tor: Usability Issues 1

- Keep Tor Browser Bundle (like all software) updated. TBB will load check.torproject.org and verify you are using the latest version. PAY ATTENTION TO THIS.
- The exit nodes see your unencrypted traffic unless you are using end-to-end encryption. TBB includes HTTPS everywhere.
- Flash is disabled for privacy reasons. Use HTML5 video.

Tor: Usability Issues 2

- Be careful opening documents downloaded through Tor. Do it offline or while using Tails. TBB will warn you about this.
- Don't torrent: You might be deanonymizing yourself in the torrent tracker and you are slowing down the network/causing abuse violations for exit node operators.

Tor: Usability Issues 2

- Be careful opening documents downloaded through Tor. Do it offline or while using Tails. TBB will warn you about this.
- Don't torrent: You might be deanonymizing yourself in the torrent tracker and you are slowing down the network/causing abuse violations for exit node operators.

Evading censorship

If you suspect your use of Tor is being monitored or blocked:

- Use a bridge: A relay not listed in the main Tor directory.
- Use pluggable transports to evade Deep Packet Inspection. To use pluggable transports, you should hit "Yes" when Tor asks you "Does your ISP block or otherwise censor connections to the Tor Network?". This will by default use a protocol called obfs3, which is right now the most developed anti-DPI measure.

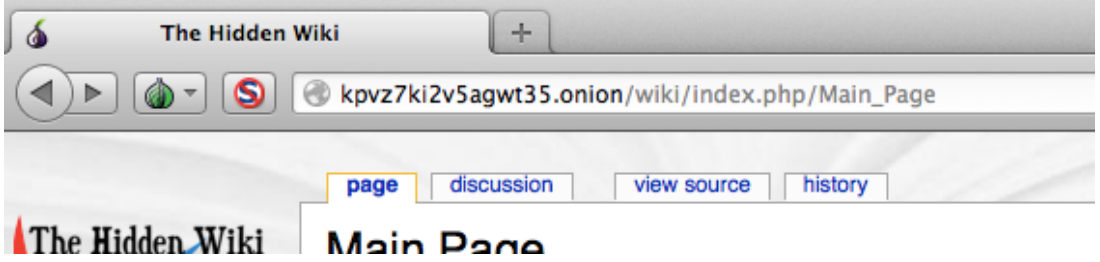
Evading censorship

If you suspect your use of Tor is being monitored or blocked:

- Use a bridge: A relay not listed in the main Tor directory.
- Use pluggable transports to evade Deep Packet Inspection. To use pluggable transports, you should hit "Yes" when Tor asks you "Does your ISP block or otherwise censor connections to the Tor Network?". This will by default use a protocol called obfs3, which is right now the most developed anti-DPI measure.

Hidden Services

Can also use Tor to anonymize a server (as well as just the client).



[16 characters derived from the hidden service's public key].onion

You only can access these *.onion sites if you through Tor

Tor: Download

Download:

- Download Tor Browser Bundle: https://www.torproject.org/download/download-easy.html.en
- For Android: Orfox

Tails: a live Linux distro that transparently routes your traffic through Tor: https://tails.boum.org

- Based on Debian Stable
- Live DVD or Live USB

Securely downloading and installing TBB

- Step 0: GPG (GnuPG) download:
  - Download GPG (Mac: GPGtools.org, Linux: it's installed, Windows: gpg4win.org)
  - Verify the SHA1 sum matches: (Mac: `openssl sha1 filename`, Linux: `sha1sum filename`, Windows: "Microsoft File Checksum Integrity Verifier")
- Step 1: Download Erinn Clark's PGP key (she signs TBB)
  - `gpg --keyserver x-hkp://keys.gnupg.net --recv-keys 0x63FEE659`
- Step 2: Verify the fingerprint
  - `gpg --fingerprint 0x63FEE659`
  - Should be: 8738 A680 B84B 3031 A630 F2DB 416F 0610 63FE E659
- Step 3: Download and check the TorBrowserBundle
  - Download TBB (*.zip file) and the signature (*.asc file) from torproject.org
  - `gpg --verify Tor-*.asc Tor*.zip`
- Step 4: Now you can unzip TorBrowserBundle*.zip and install!

Example

```
$ gpg --keyserver x-hkp://keys.gnupg.net --recv-keys 0x63FEE659
gpg: requesting key 63FEE659 from hkp server keys.gnupg.net
gpg: key 63FEE659: "Erinn Clark <erinn@torproject.org>" not changed
gpg: Total number processed: 1
gpg:              unchanged: 1
$ gpg --fingerprint 0x63FEE659
pub   2048R/63FEE659 2003-10-16
      Key fingerprint = 8738 A680 B84B 3031 A630  F2DB 416F 0610 63FE E659
uid                  Erinn Clark <erinn@torproject.org>
uid                  Erinn Clark <erinn@debian.org>
uid                  Erinn Clark <erinn@double-helix.org>
sub   2048R/EB399FD7 2003-10-16

$ vi TorBrowserBundle-3.5.4-osx32_en-US.zip.asc
$ cp Downloads/TorBrowserBundle-3.5.4-osx32_en-US.zip .
$ gpg --verify TorBrowserBundle-3.5.4-osx32_en-US.zip.asc TorBrowserBundle-3.5.4-osx32_en-US.zip
gpg: Signature made Tue Apr  8 16:08:46 2014 CDT using RSA key ID 63FEE659
gpg: Good signature from "Erinn Clark <erinn@torproject.org>"
gpg:                 aka "Erinn Clark <erinn@debian.org>"
gpg:                 aka "Erinn Clark <erinn@double-helix.org>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 8738 A680 B84B 3031 A630  F2DB 416F 0610 63FE E659
$
```