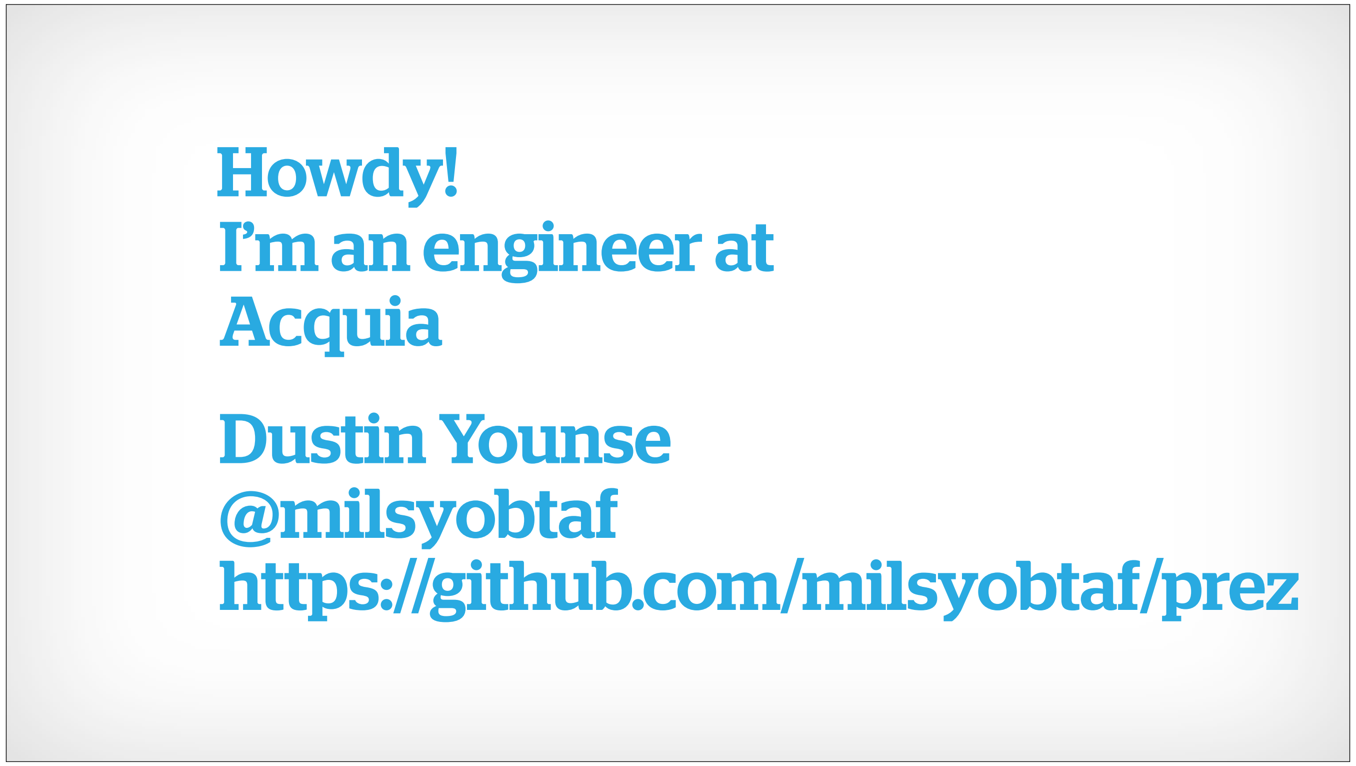
The Digital Speakeasy: Secure and Anonymous Access to Your Website

NERD Summit 3/19/17



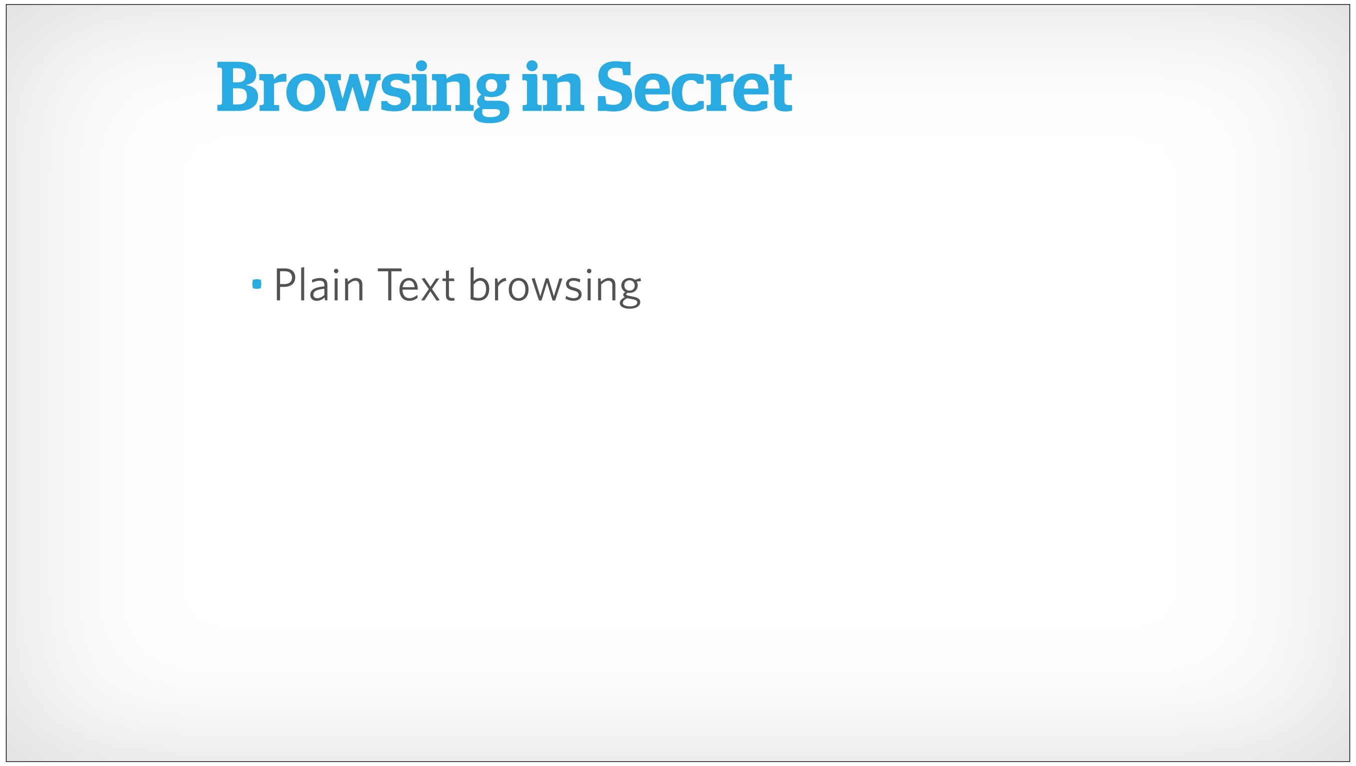
Howdy!
I’m an engineer at
Acquia

Dustin Younse
@milsyobtaf
https://github.com/milsyobtaf/prez

We’re a small hosting company based out of Boston - maybe you’ve heard of us? In a previous life, I headed the support team at Four Kitchens, based out of Austin, TX, which means I did a lot of somewhat repetitive work, but every once in a while a client asks us to do something particularly cool, which is what I’m here to talk about.

What Is The Digital Speakeasy?

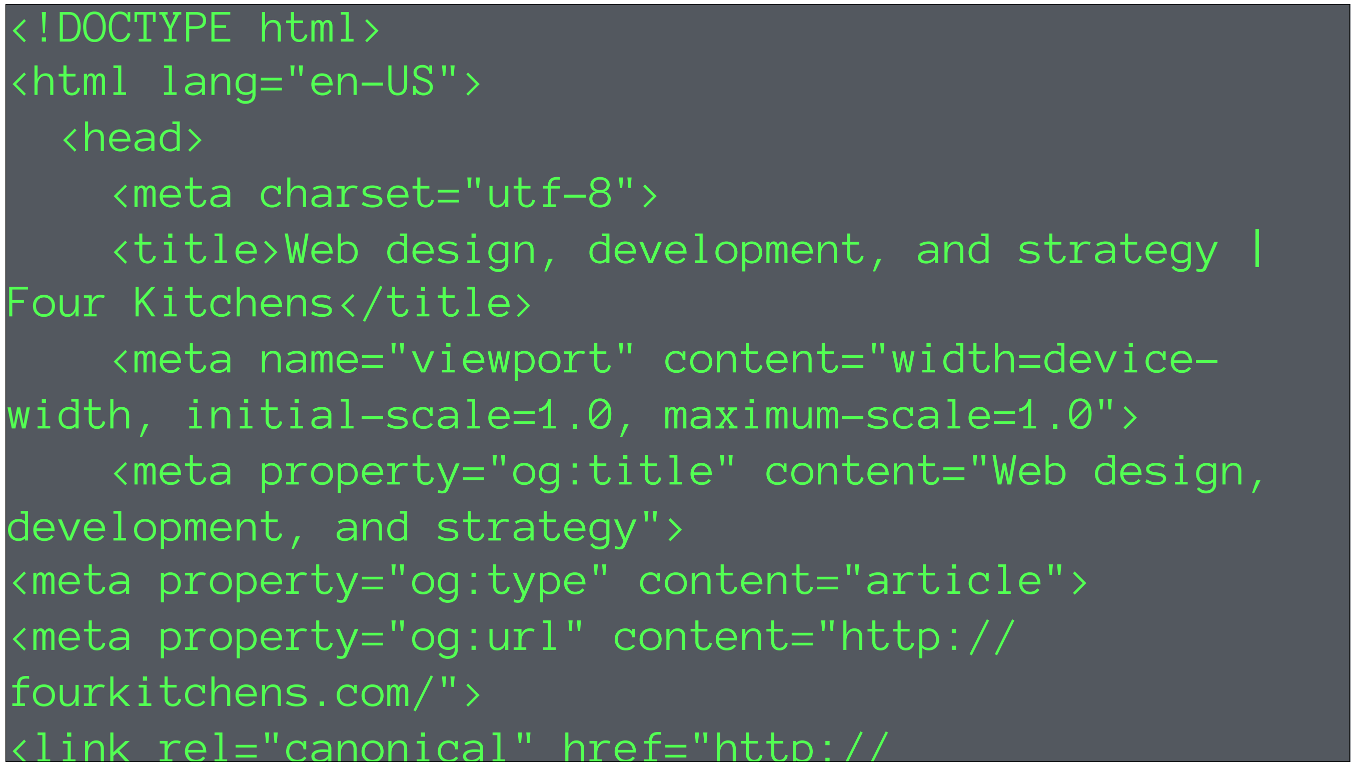
What is the digital speakeasy?



Browsing in Secret

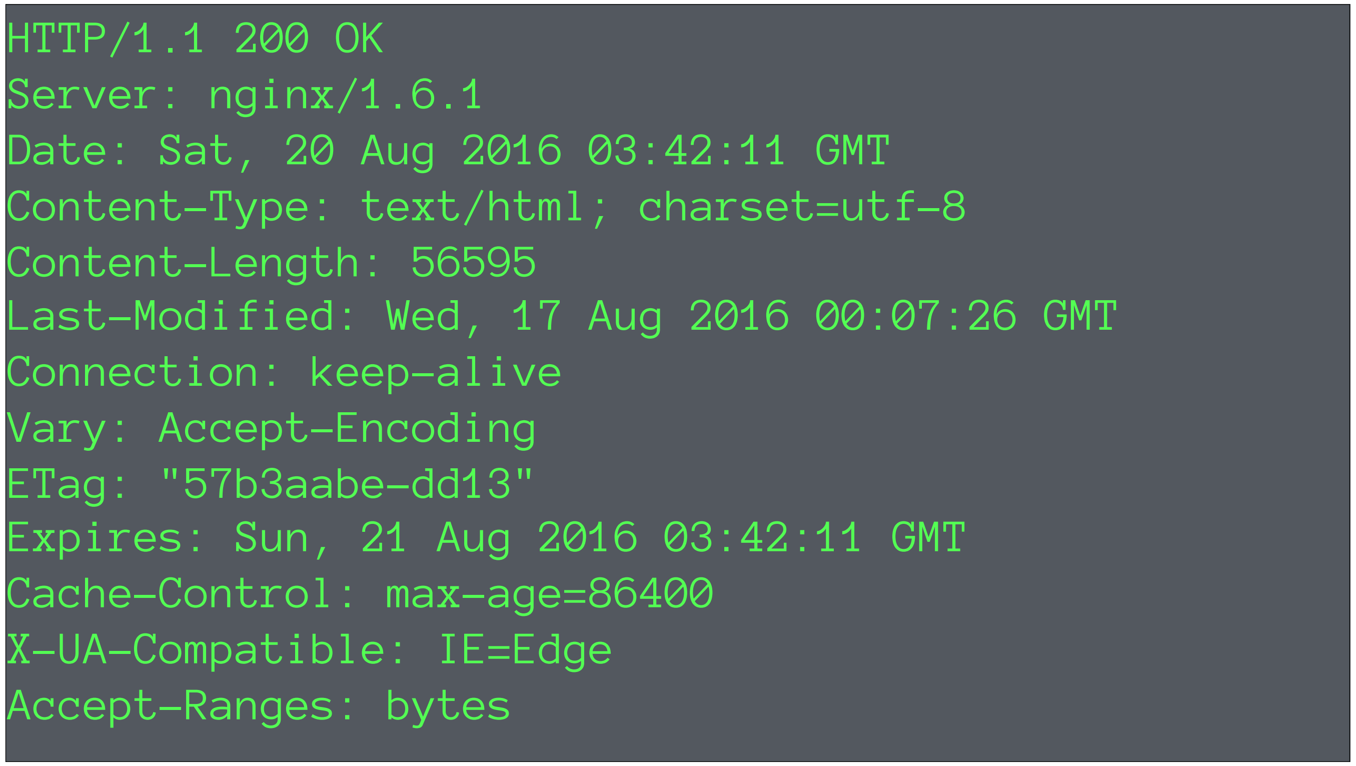
- Plain Text browsing

At it’s core, the web is just a bunch of text files and images flying back and forth, which anyone can read. Whether you’re using wireless or an ethernet cable, there are always places where people can listen in on your traffic. Text looks like text, images look like images, credit card numbers look like credit card numbers.



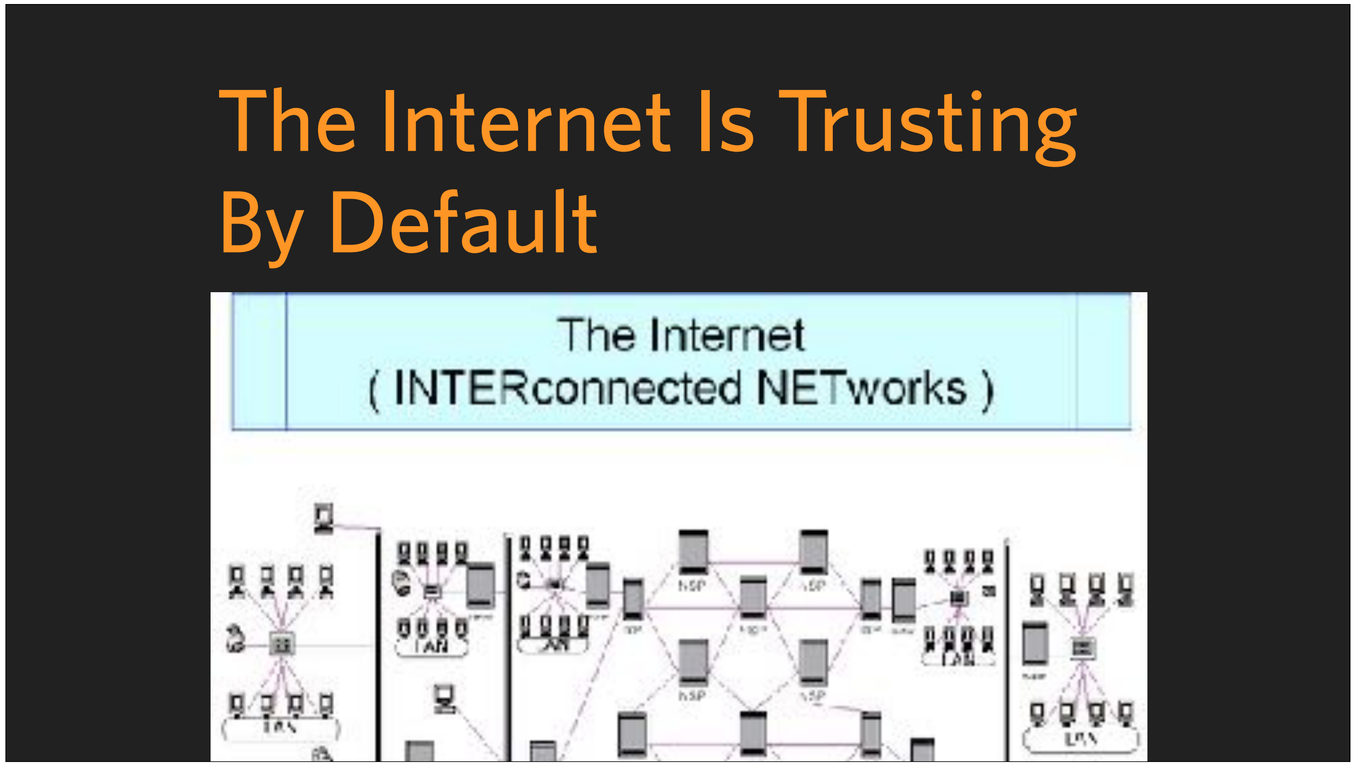
```
<!DOCTYPE html>
<html lang="en-US">
  <head>
    <meta charset="utf-8">
    <title>Web design, development, and strategy |
Four Kitchens</title>
    <meta name="viewport" content="width=device-
width, initial-scale=1.0, maximum-scale=1.0">
    <meta property="og:title" content="Web design,
development, and strategy">
<meta property="og:type" content="article">
<meta property="og:url" content="http://
fourkitchens.com/">
<link rel="canonical" href="http://
```

You get the web content, of course



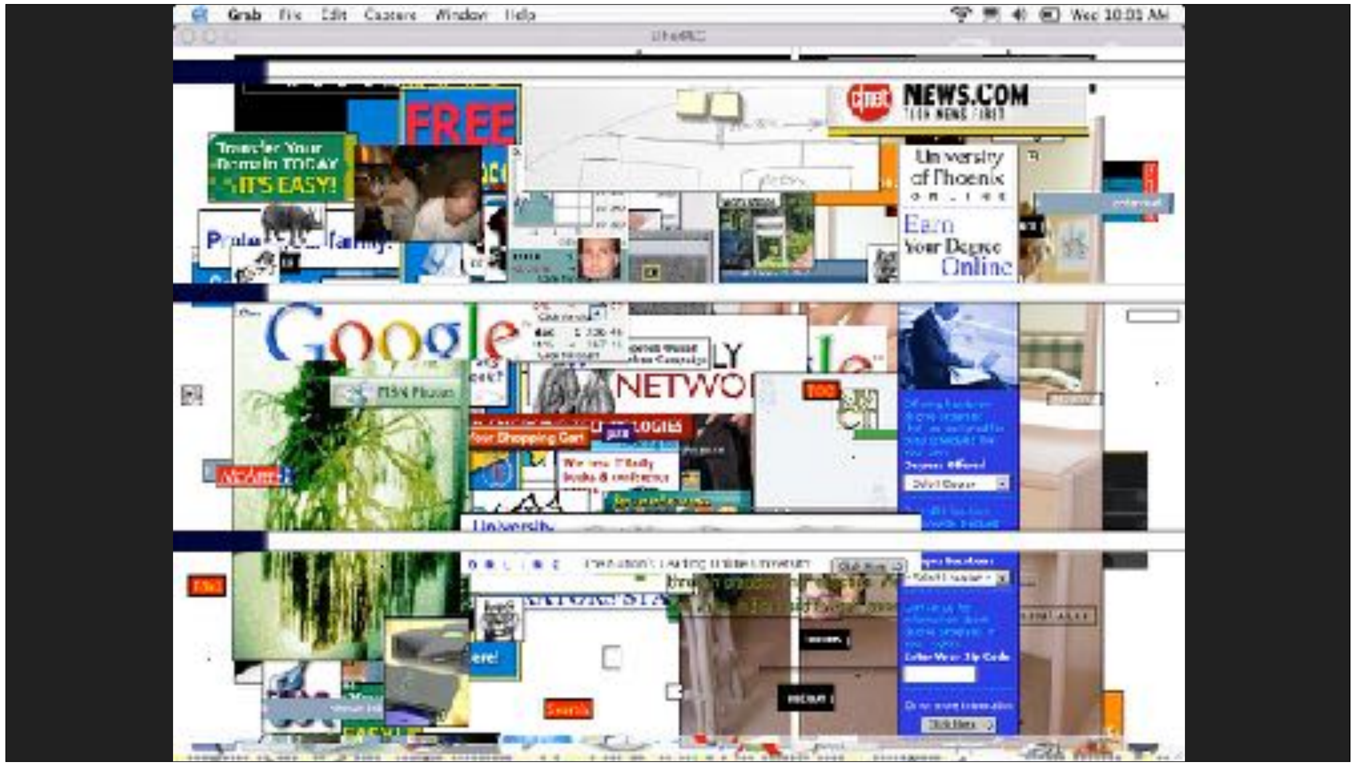
```
HTTP/1.1 200 OK
Server: nginx/1.6.1
Date: Sat, 20 Aug 2016 03:42:11 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 56595
Last-Modified: Wed, 17 Aug 2016 00:07:26 GMT
Connection: keep-alive
Vary: Accept-Encoding
ETag: "57b3aabe-dd13"
Expires: Sun, 21 Aug 2016 03:42:11 GMT
Cache-Control: max-age=86400
X-UA-Compatible: IE=Edge
Accept-Ranges: bytes
```

But you also get the metadata

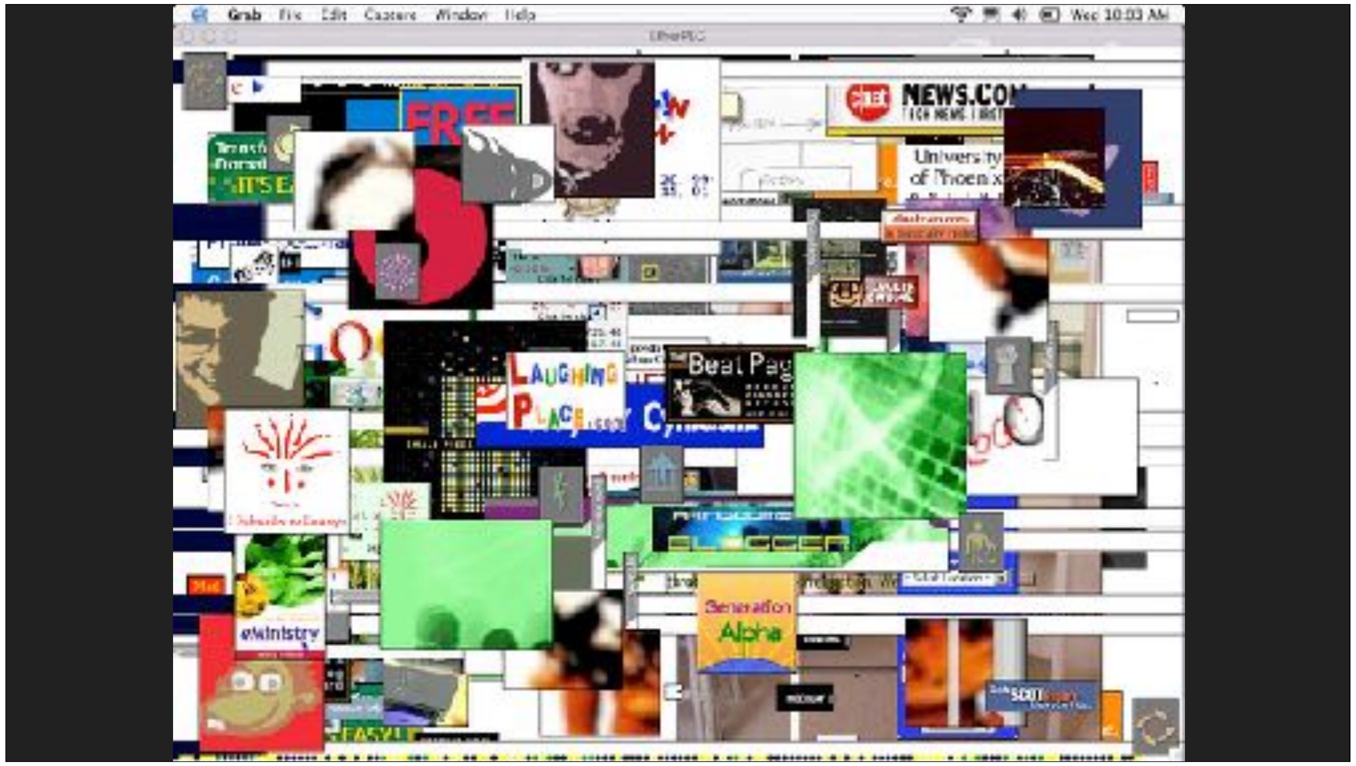


The Internet Is Trusting By Default

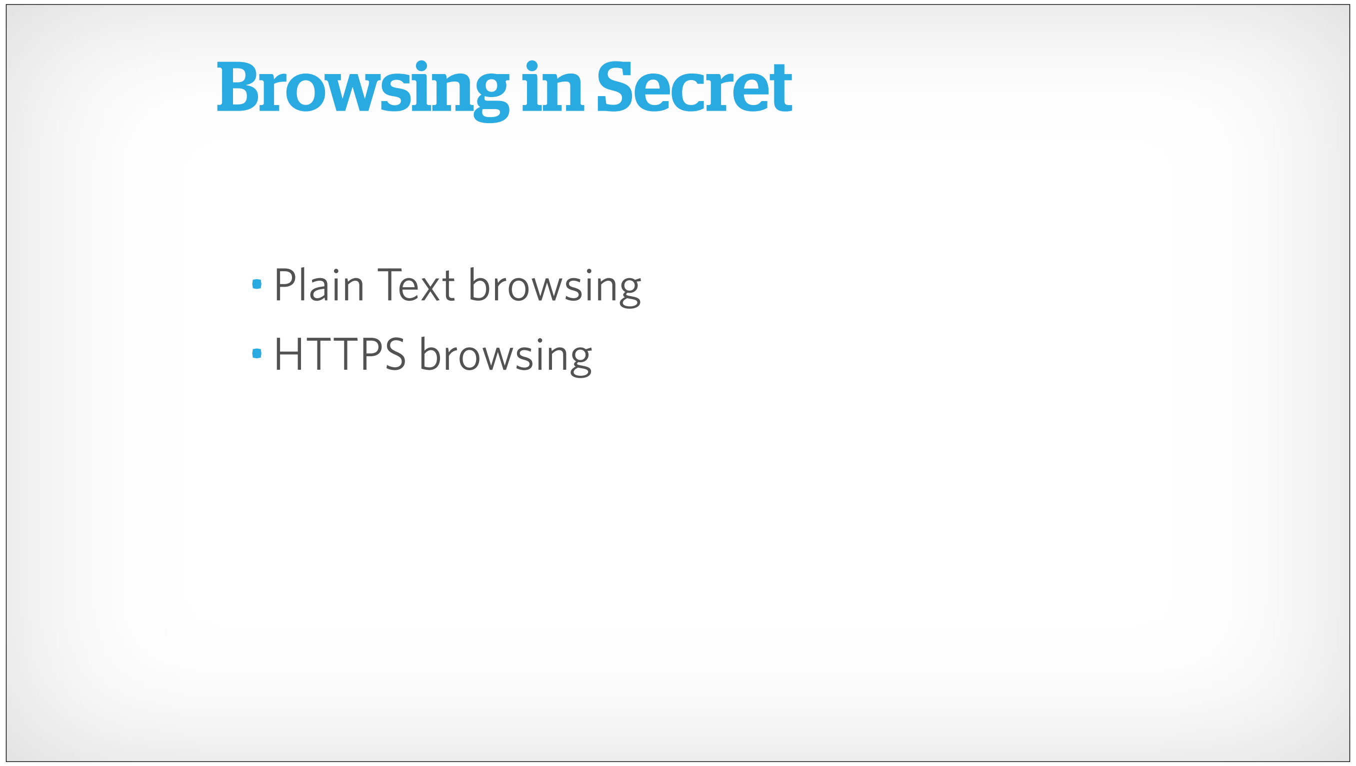
The internet was designed to be open. It’s trusting by default. Every computer on a given network segment has access to all of the data on that entire network segment. With the right knowhow you can do things like this.



In 2005 I got my first computer with wireless, a G4 iBook. I discovered a little program called EtherPEG that did exactly one thing – it let you literally snatch the images on the wireless network out of thin air.


Grab File Edit Capture Window Help
Wed 10:03 AM
FREE
NEWS.COM
University of Phoenix
LAUGHING PLACE.com
Beat Page
Generation Alpha
eMinistry
EASYLI

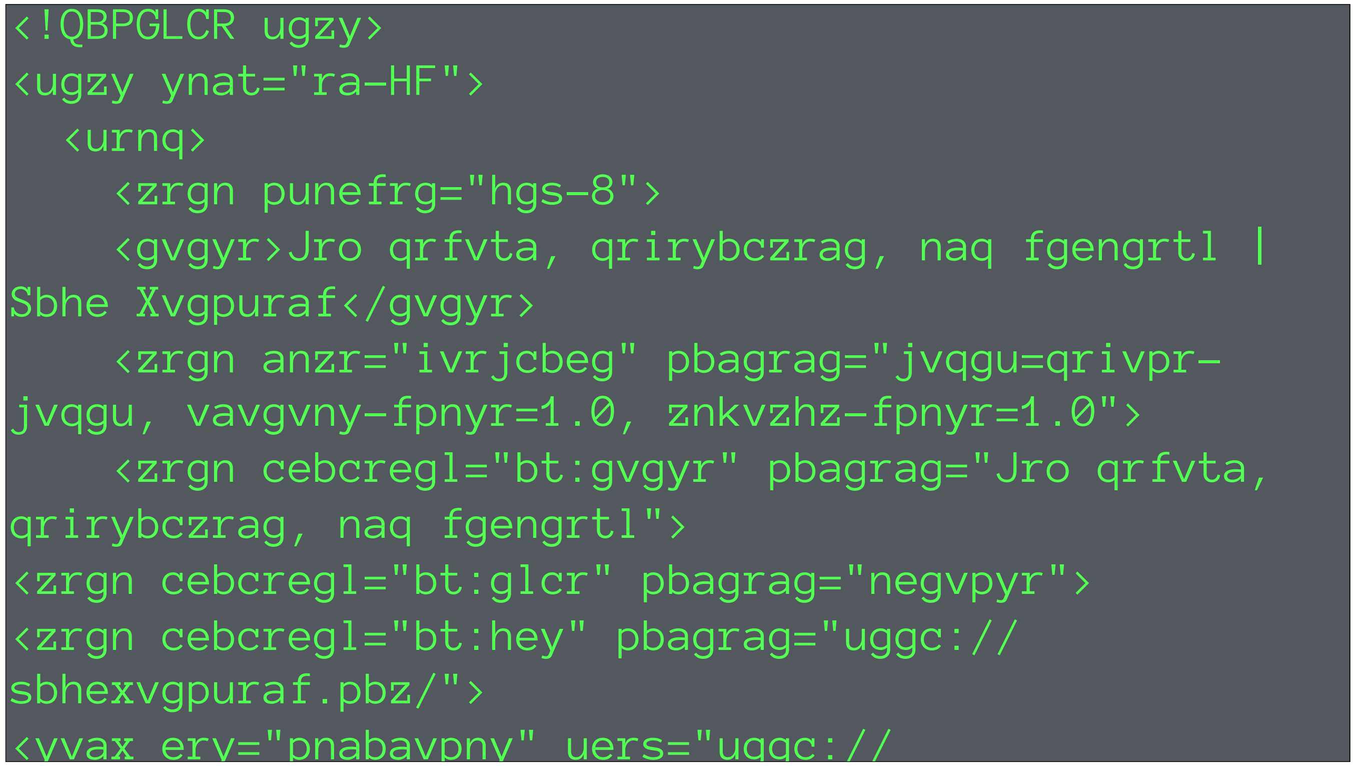
These kinds of things are still _very possible_, with a bit more work.



Browsing in Secret

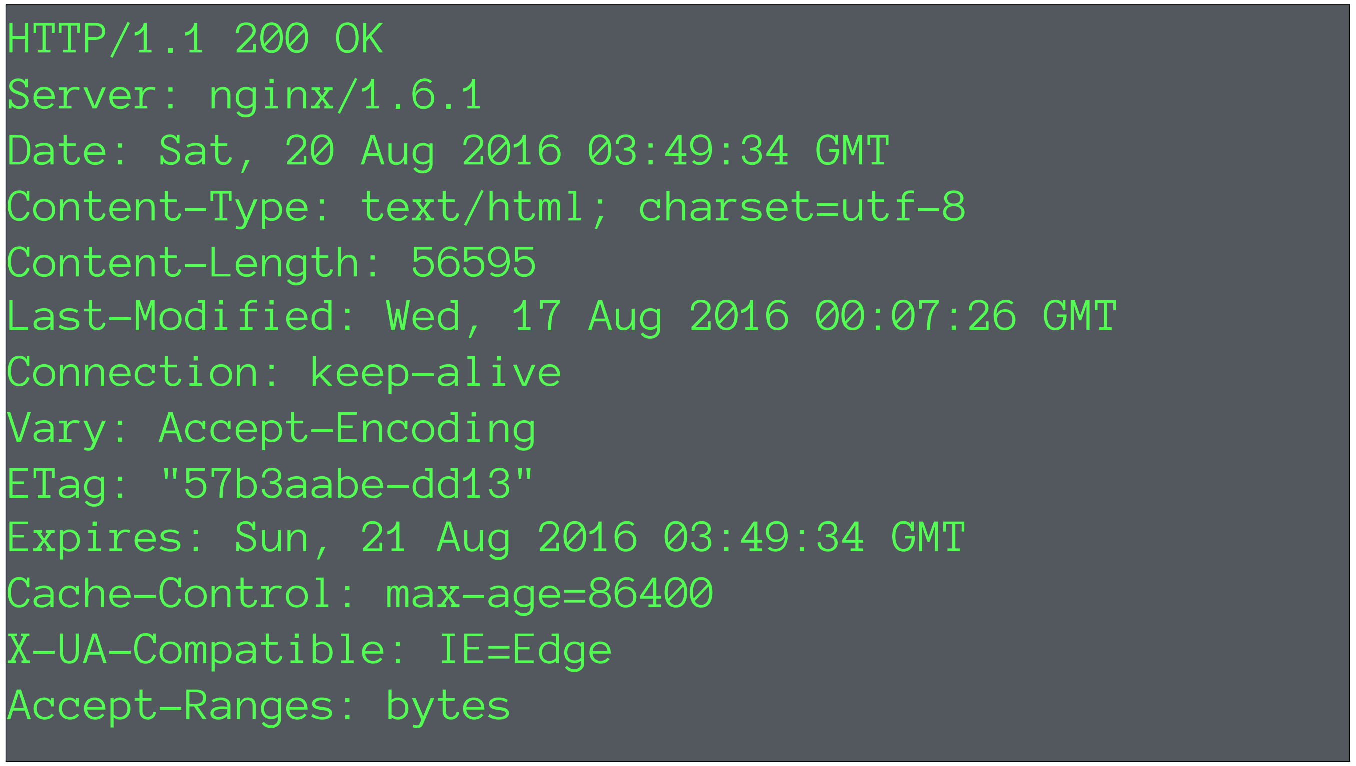
- Plain Text browsing
- HTTPS browsing

HTTPS is a step up, encrypting your connection from point to point



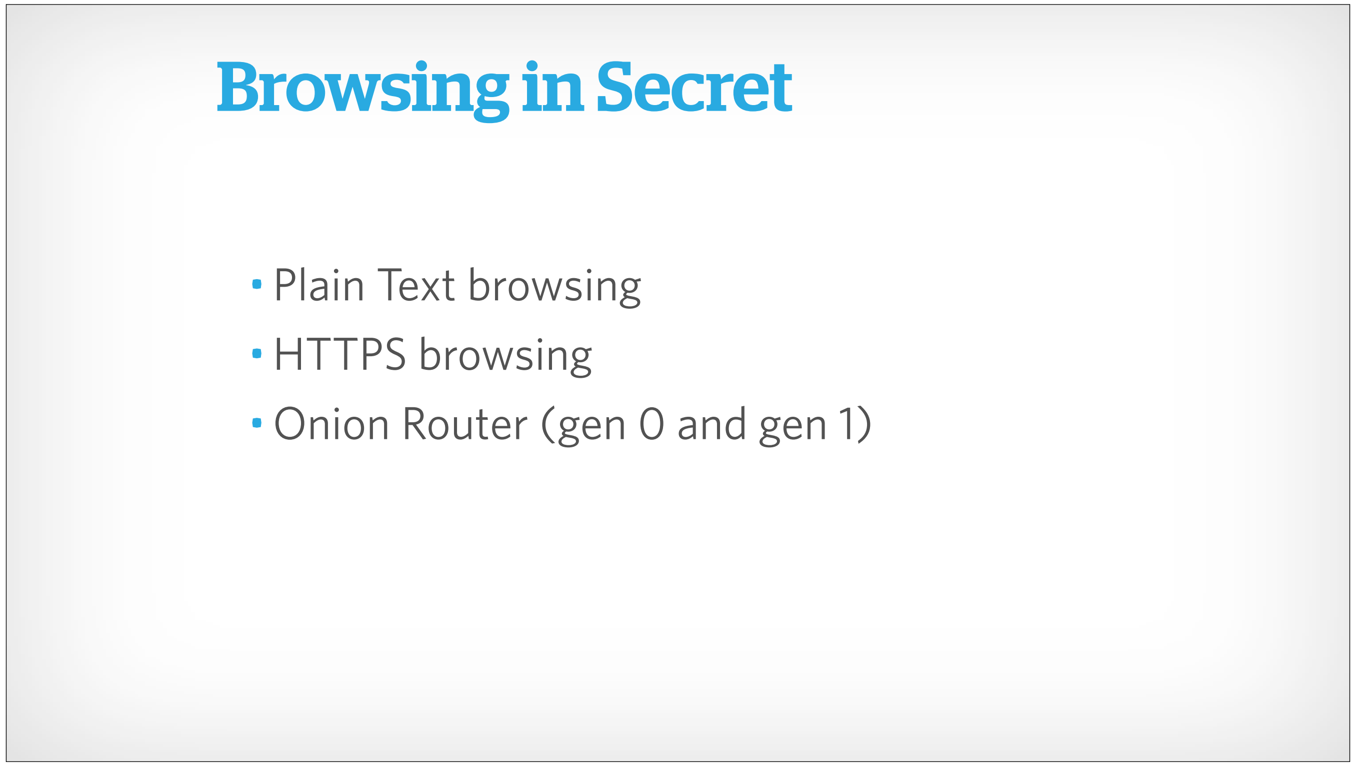
```
<!QBPGLCR ugzy>
<ugzy ynat="ra-HF">
  <urnq>
    <zrgn punefrg="hgs-8">
    <gvgyr>Jro qrfvta, qrirybczrag, naq fgengrtl |
Sbhe Xvgpuraf</gvgyr>
    <zrgn anzr="ivrjcbeg" pbagrag="jvqgu=qrivpr-
jvqgu, vavgvny-fpnyr=1.0, znkvzhz-fpnyr=1.0">
    <zrgn cebcregl="bt:gvgyr" pbagrag="Jro qrfvta,
qrirybczrag, naq fgengrtl">
<zrgn cebcregl="bt:glcr" pbagrag="negvpyr">
<zrgn cebcregl="bt:hey" pbagrag="uggc://
sbhexvgpuraf.pbz/">
<vvax ery="pnabavpny" uers="uggc://
```

The content is protected



```
HTTP/1.1 200 OK
Server: nginx/1.6.1
Date: Sat, 20 Aug 2016 03:49:34 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 56595
Last-Modified: Wed, 17 Aug 2016 00:07:26 GMT
Connection: keep-alive
Vary: Accept-Encoding
ETag: "57b3aabe-dd13"
Expires: Sun, 21 Aug 2016 03:49:34 GMT
Cache-Control: max-age=86400
X-UA-Compatible: IE=Edge
Accept-Ranges: bytes
```

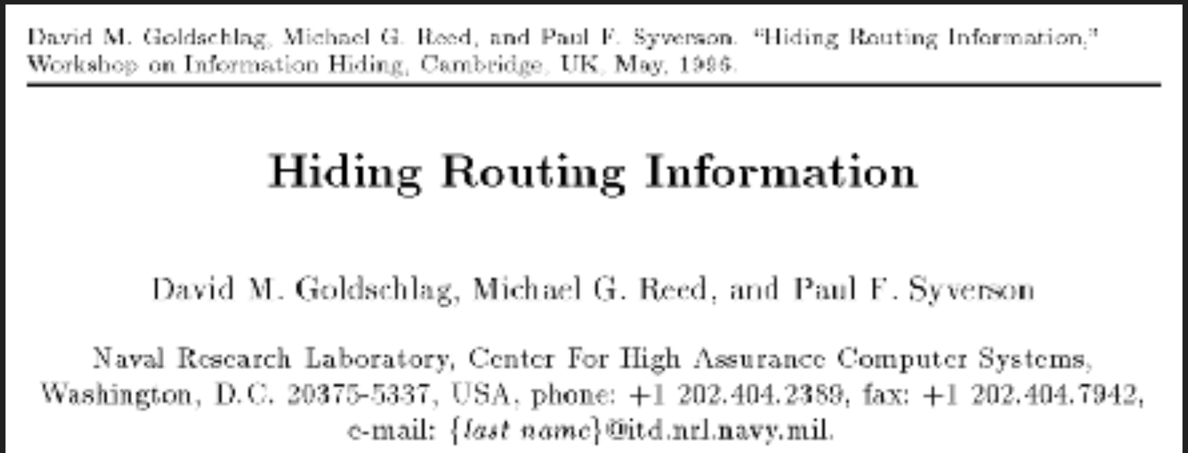
But you still leak the metadata



Browsing in Secret

- Plain Text browsing
- HTTPS browsing
- Onion Router (gen 0 and gen 1)

Onion Router was a product of the US Naval Research Lab, conceived in the mid 1990s as a method of securing web browsing through obscurity

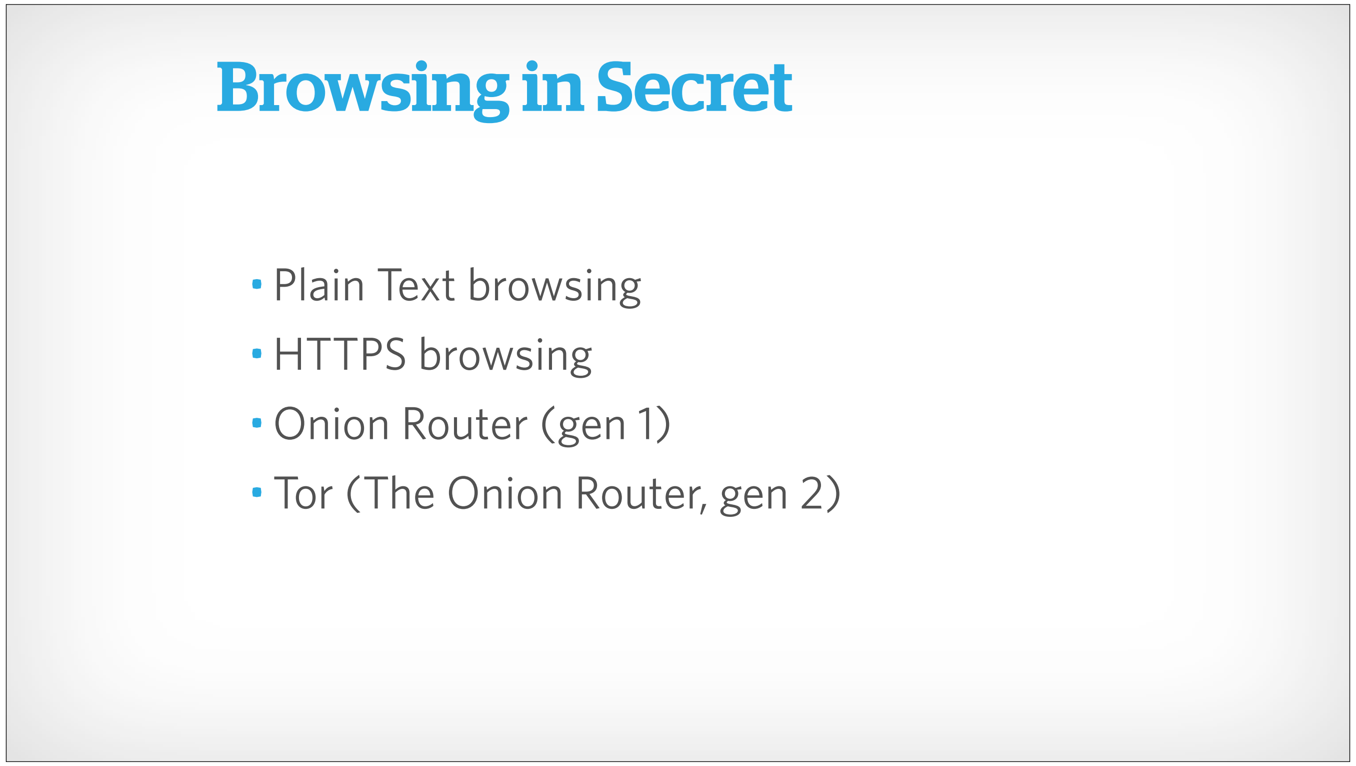


David M. Goldschlag, Michael G. Reed, and Paul F. Syverson. "Hiding Routing Information,"
Workshop on Information Hiding, Cambridge, UK, May, 1996.

Hiding Routing Information

David M. Goldschlag, Michael G. Reed, and Paul F. Syverson

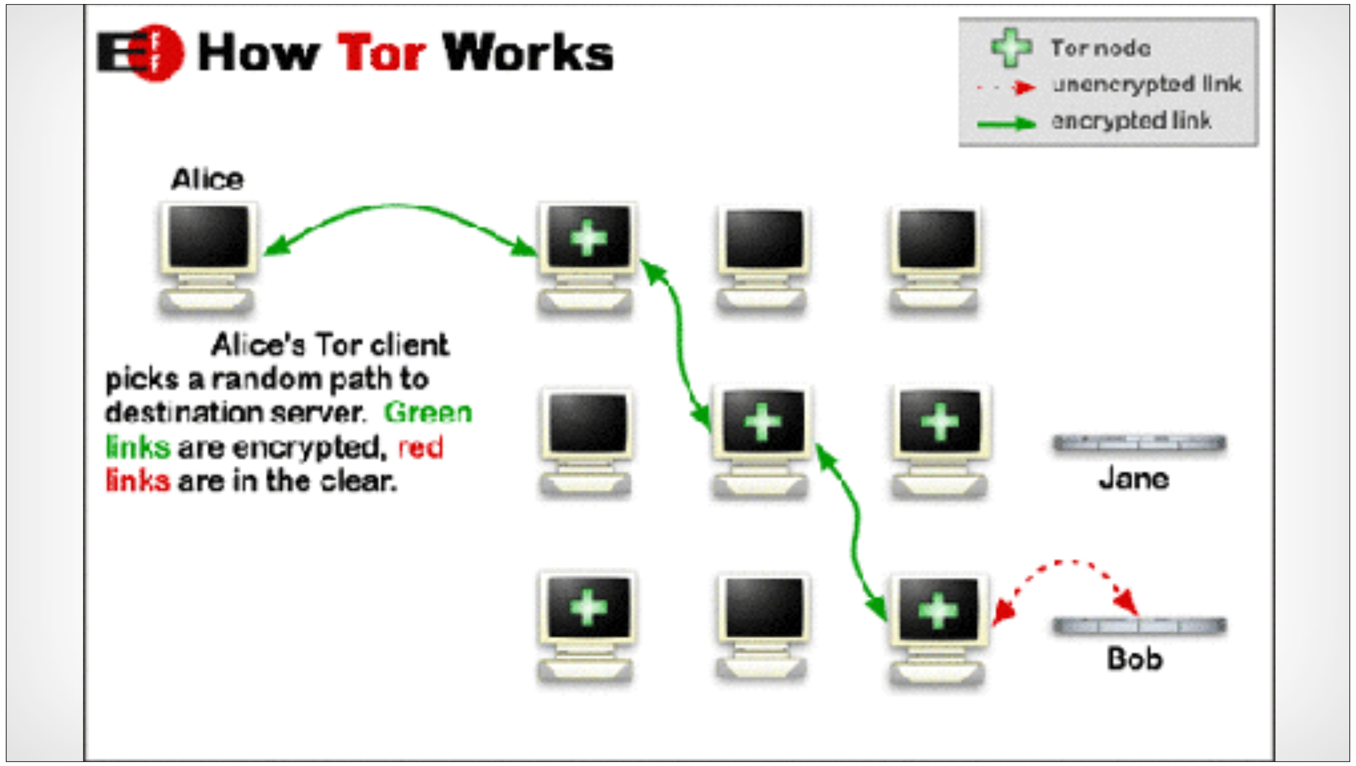
Naval Research Laboratory, Center For High Assurance Computer Systems,
Washington, D.C. 20375-5337, USA, phone: +1 202.404.2389, fax: +1 202.404.7942,
e-mail: {*last name*}@itd.nrl.navy.mil.



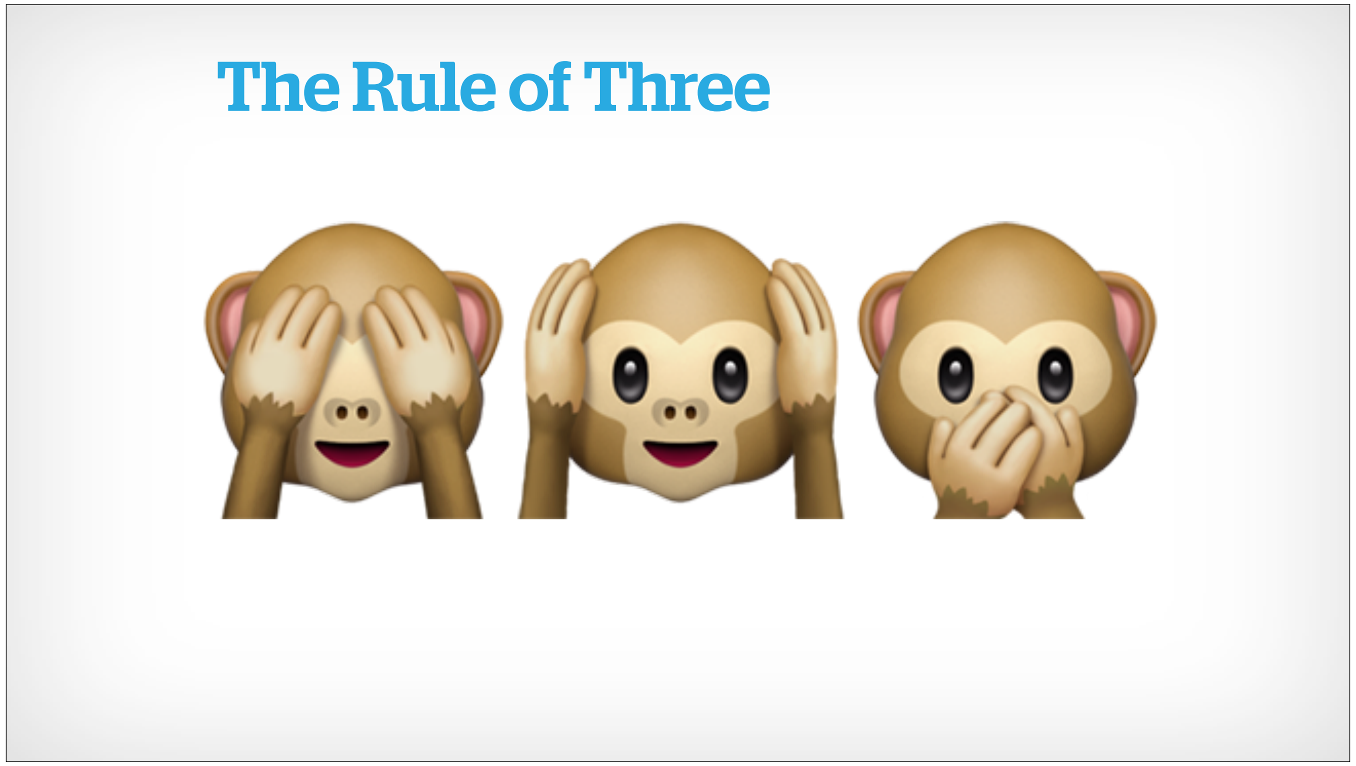
Browsing in Secret

- Plain Text browsing
- HTTPS browsing
- Onion Router (gen 1)
- Tor (The Onion Router, gen 2)

In 2002 this research was turned into Tor, an open source implementation funded in part by the EFF


How Tor Works
Tor node
unencrypted link
encrypted link
Alice
Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Bob

Rather than taking a single, determined path from your computer to the server, Tor uses a random selection of intermediaries to cover your tracks

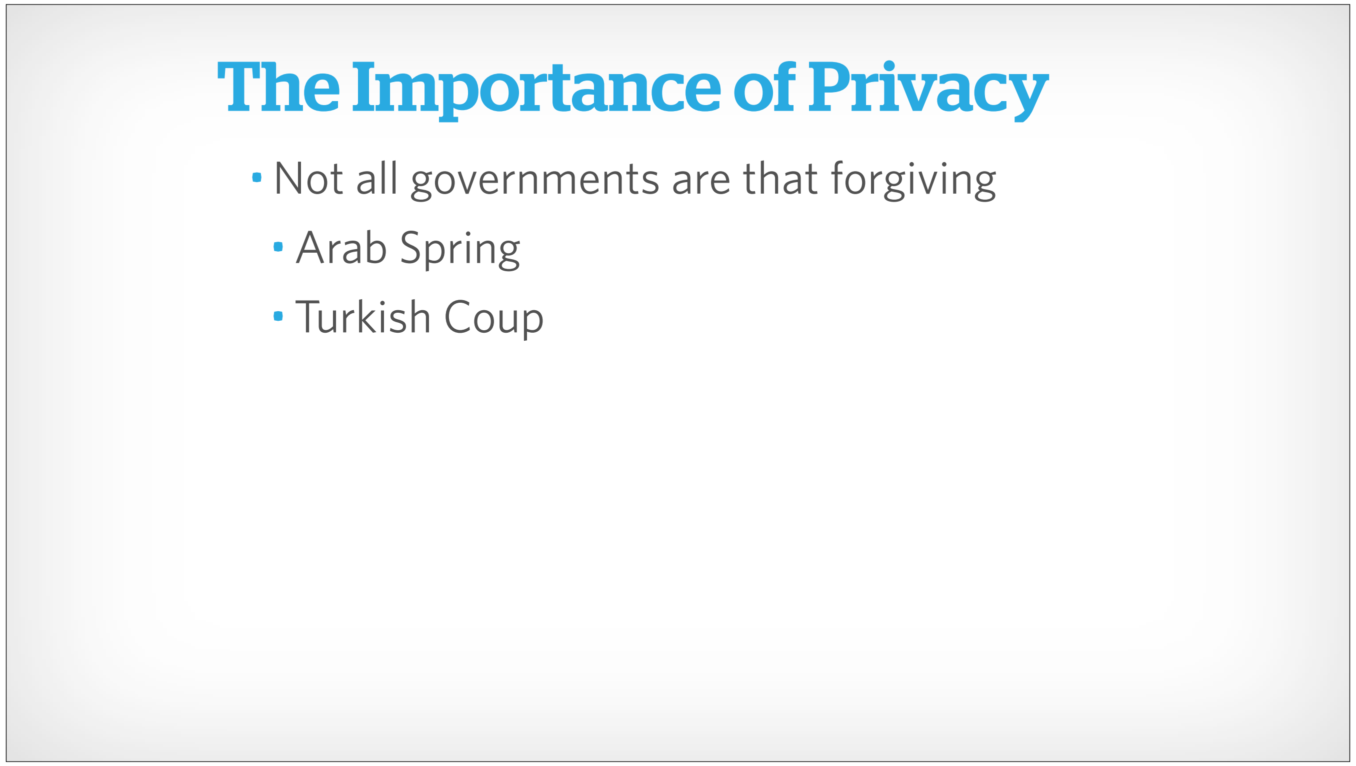


The Rule of Three

Rather than taking a single, determined path from your computer to the server, Tor uses a random selection of intermediaries to cover your tracks

So Why Bother?

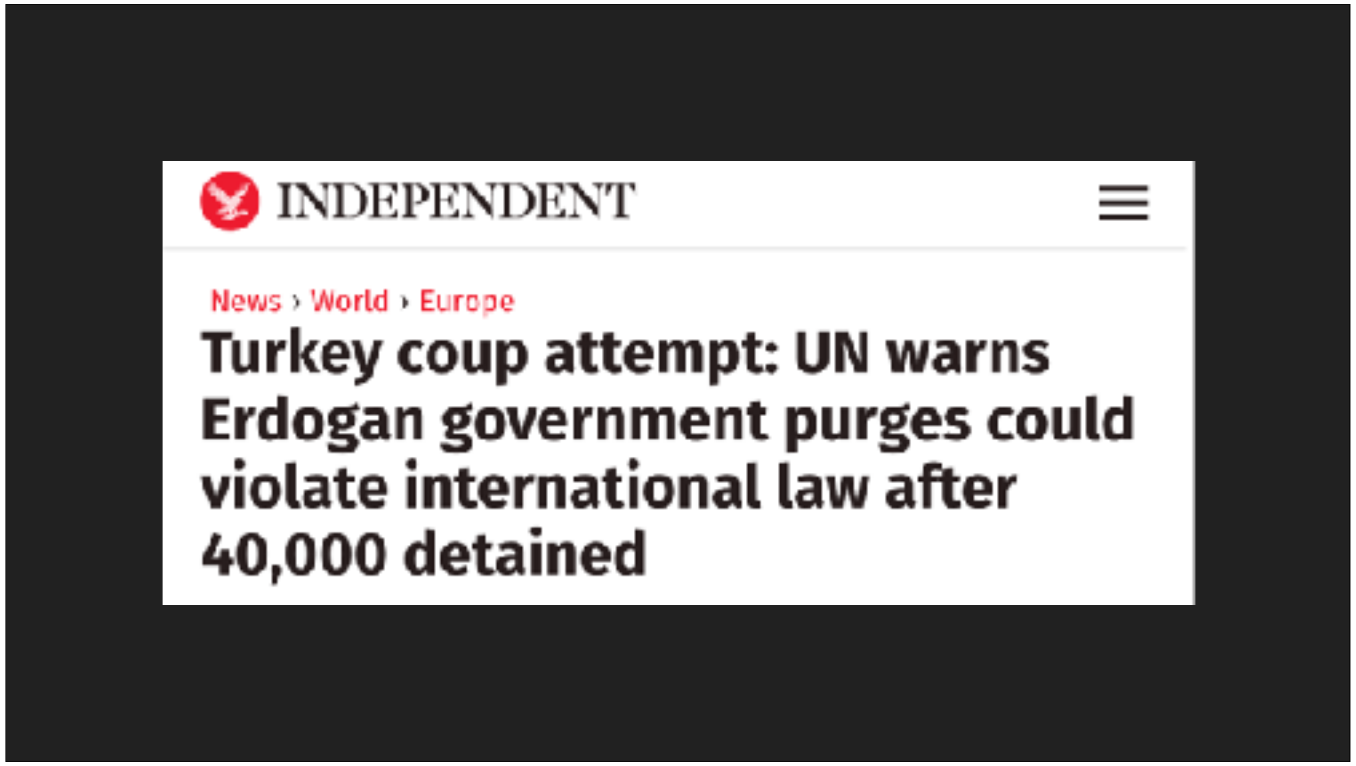
So why bother? Seems like a lot of effort just to look at some websites.



The Importance of Privacy

- Not all governments are that forgiving
  - Arab Spring
  - Turkish Coup

Privacy, particularly online, is kind of an abstract concept. Why is it so important?

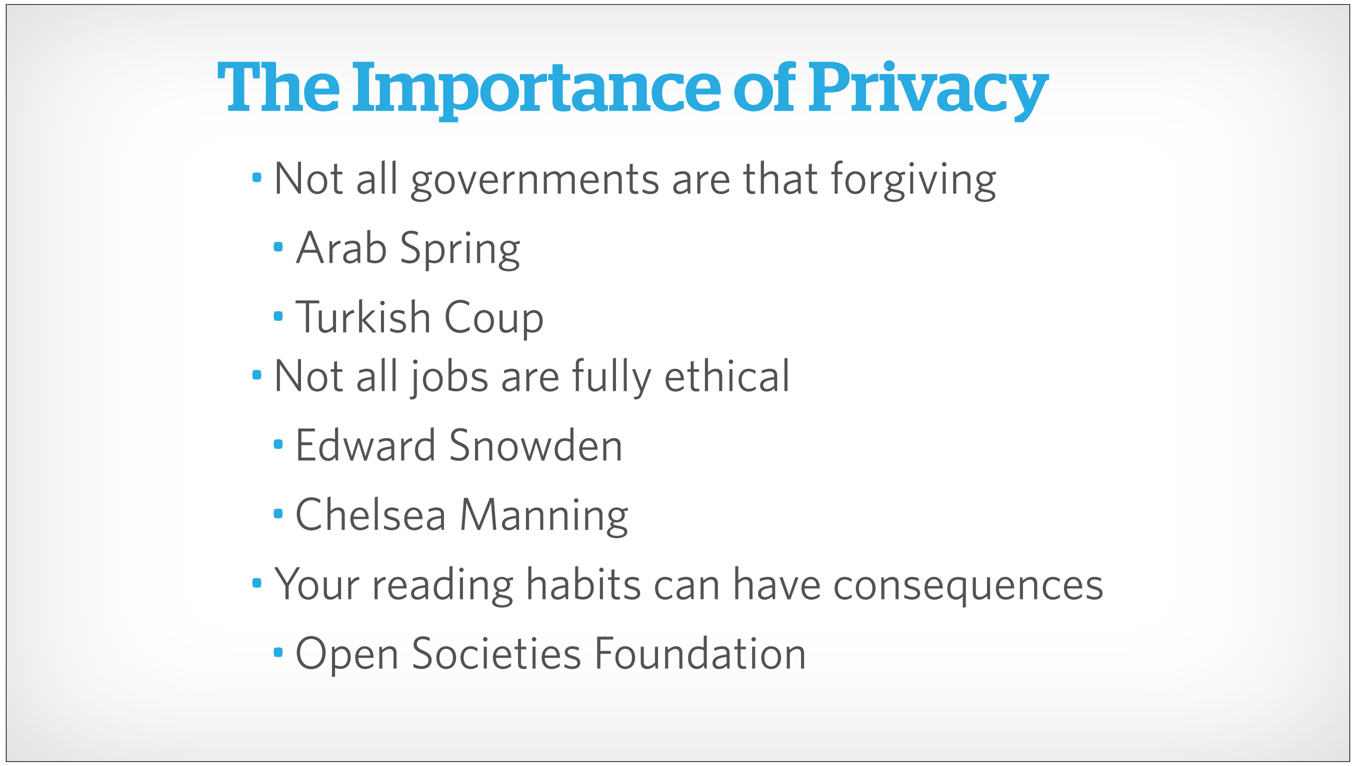


INDEPENDENT

News › World › Europe

Turkey coup attempt: UN warns Erdogan government purges could violate international law after 40,000 detained

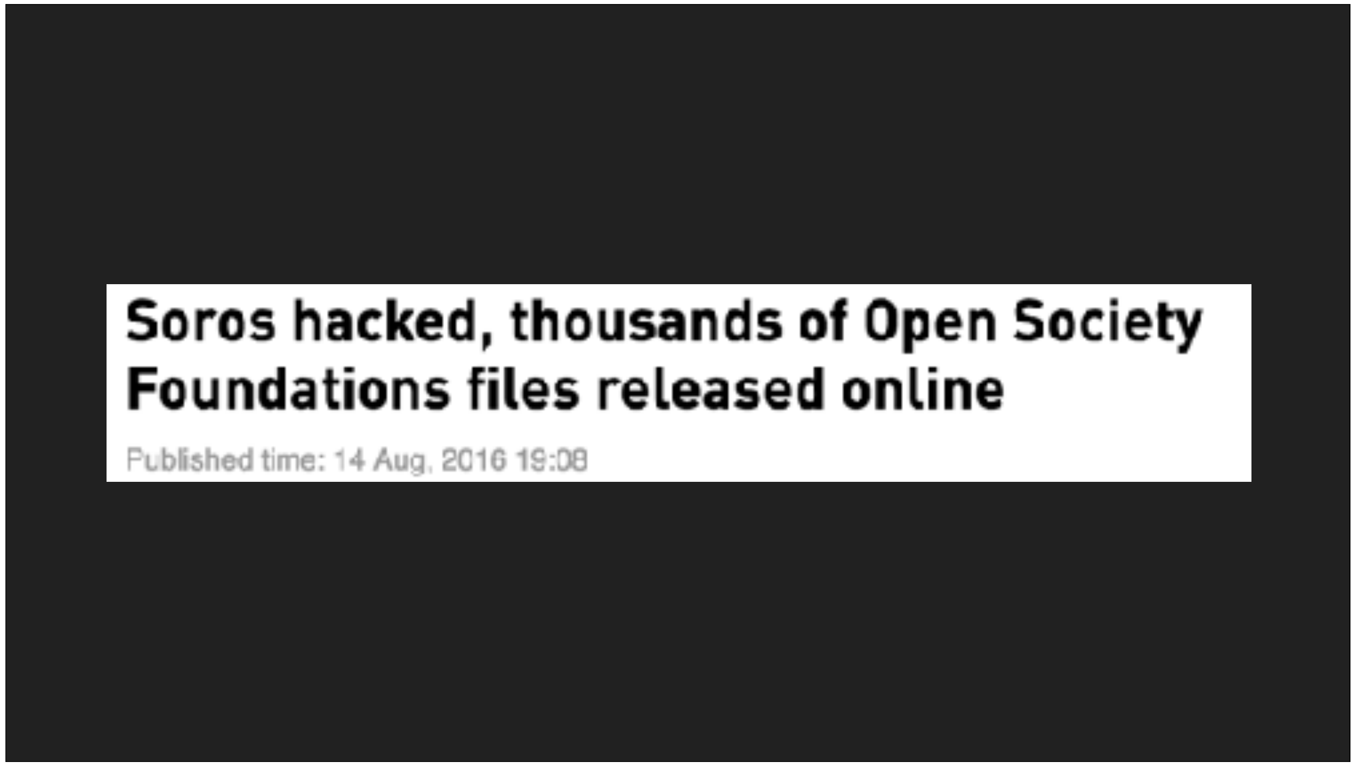
From 8/19/2016



The Importance of Privacy

- Not all governments are that forgiving
  - Arab Spring
  - Turkish Coup
- Not all jobs are fully ethical
  - Edward Snowden
  - Chelsea Manning
- Your reading habits can have consequences
  - Open Societies Foundation

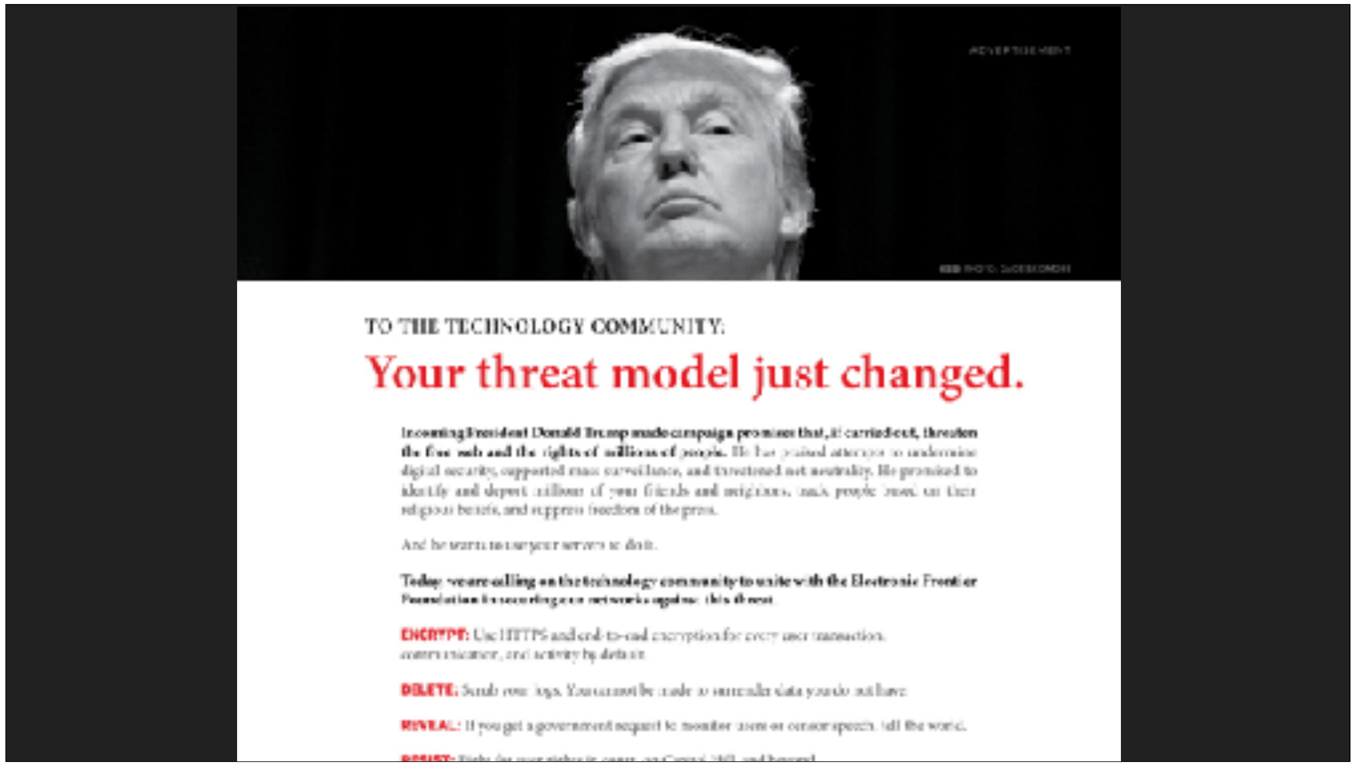
Privacy, particularly online, is kind of an abstract concept. Why is it so important?



Soros hacked, thousands of Open Society Foundations files released online

Published time: 14 Aug, 2016 19:08

From 8/19/2016



ADVERTISEMENT

TO THE TECHNOLOGY COMMUNITY:

Your threat model just changed.

Incoming President Donald Trump made campaign promises that, if carried out, threaten the free web and the rights of millions of people. He has praised attempts to undermine digital security, supported mass surveillance, and threatened net neutrality. He promised to identify and deport millions of your friends and neighbors, track people based on their religious beliefs, and suppress freedom of the press.

And he wants to use your servers to do it.

Today we are calling on the technology community to unite with the Electronic Frontier Foundation in securing our networks against this threat.

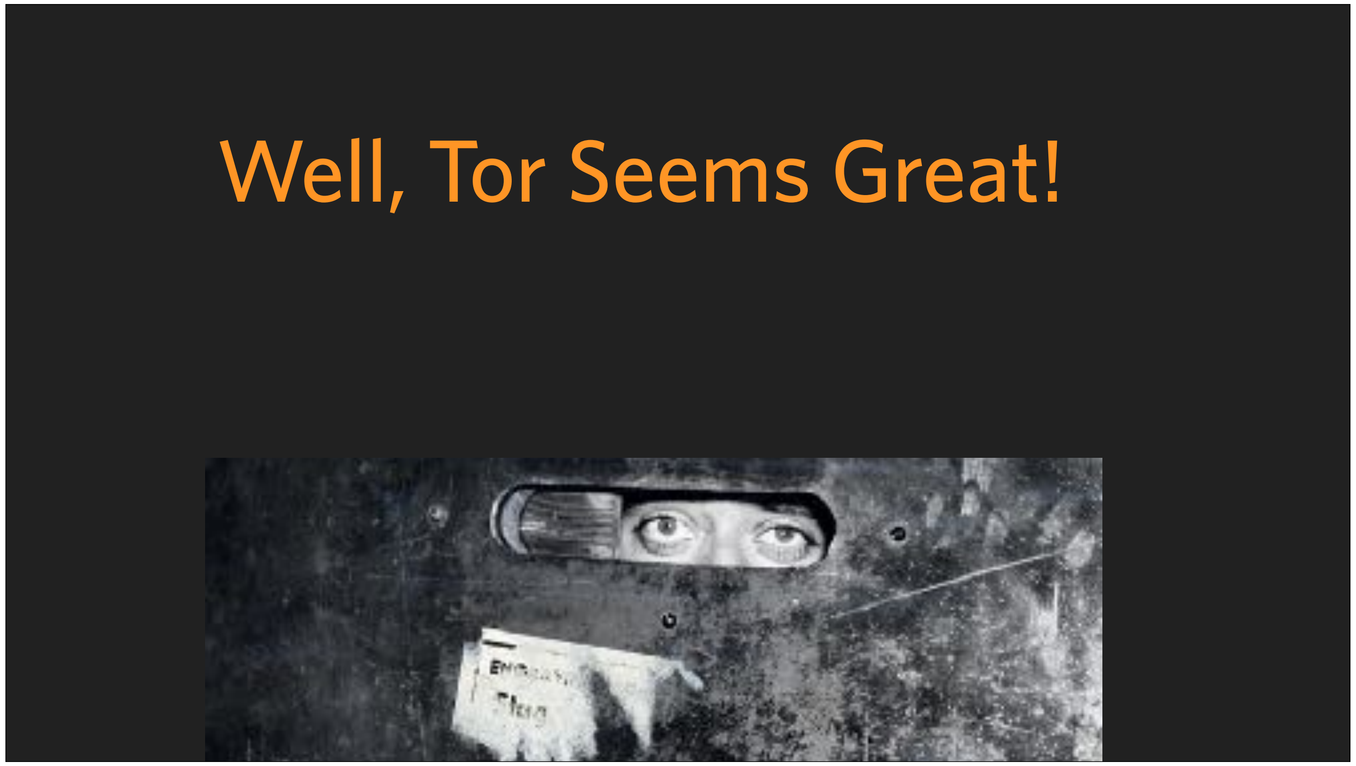
ENCRYPT: Use HTTPS and end-to-end encryption for every user transaction, communication, and activity by default.

DELETE: Scrub your logs. You cannot be made to surrender data you do not have.

REVEAL: If you get a government request to monitor users or censor speech, tell the world.

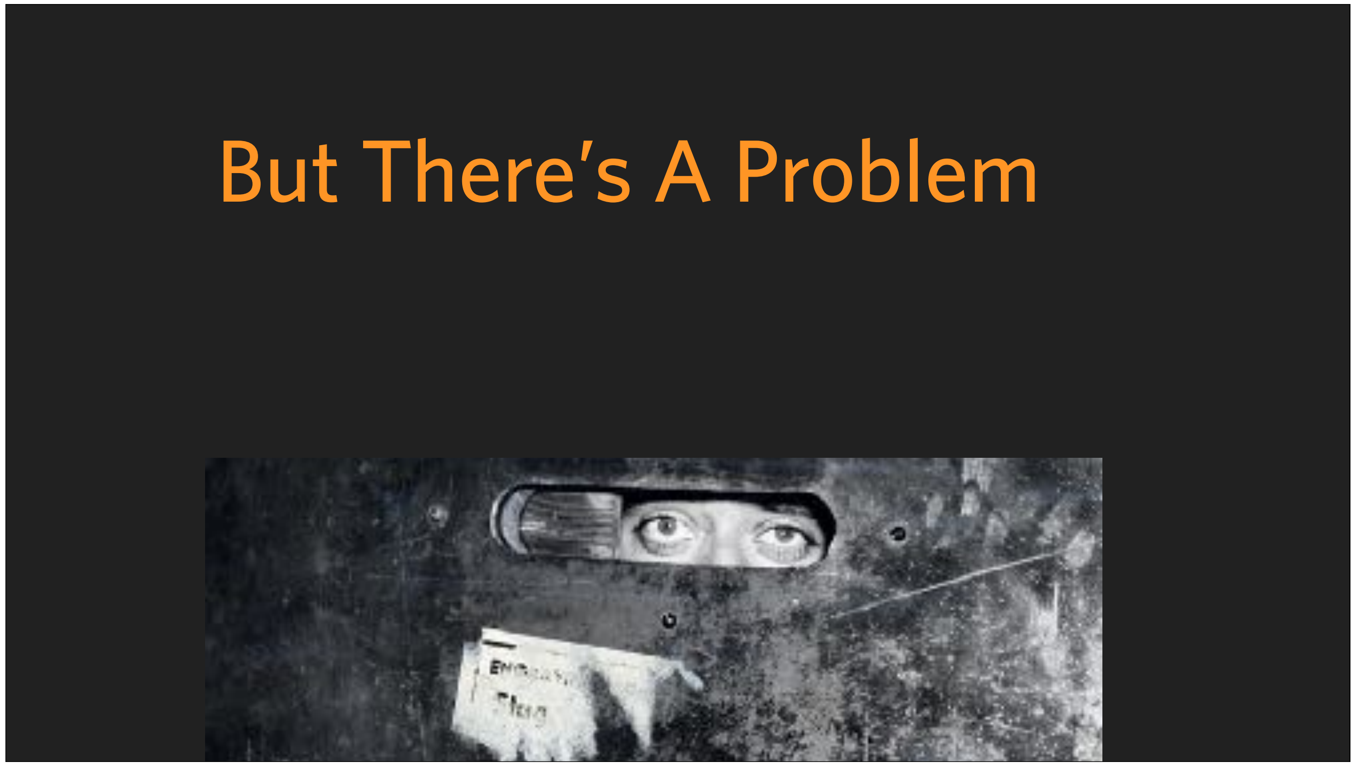
RESIST: Fight for user rights in court, on Capitol Hill, and beyond.

And, y’know.



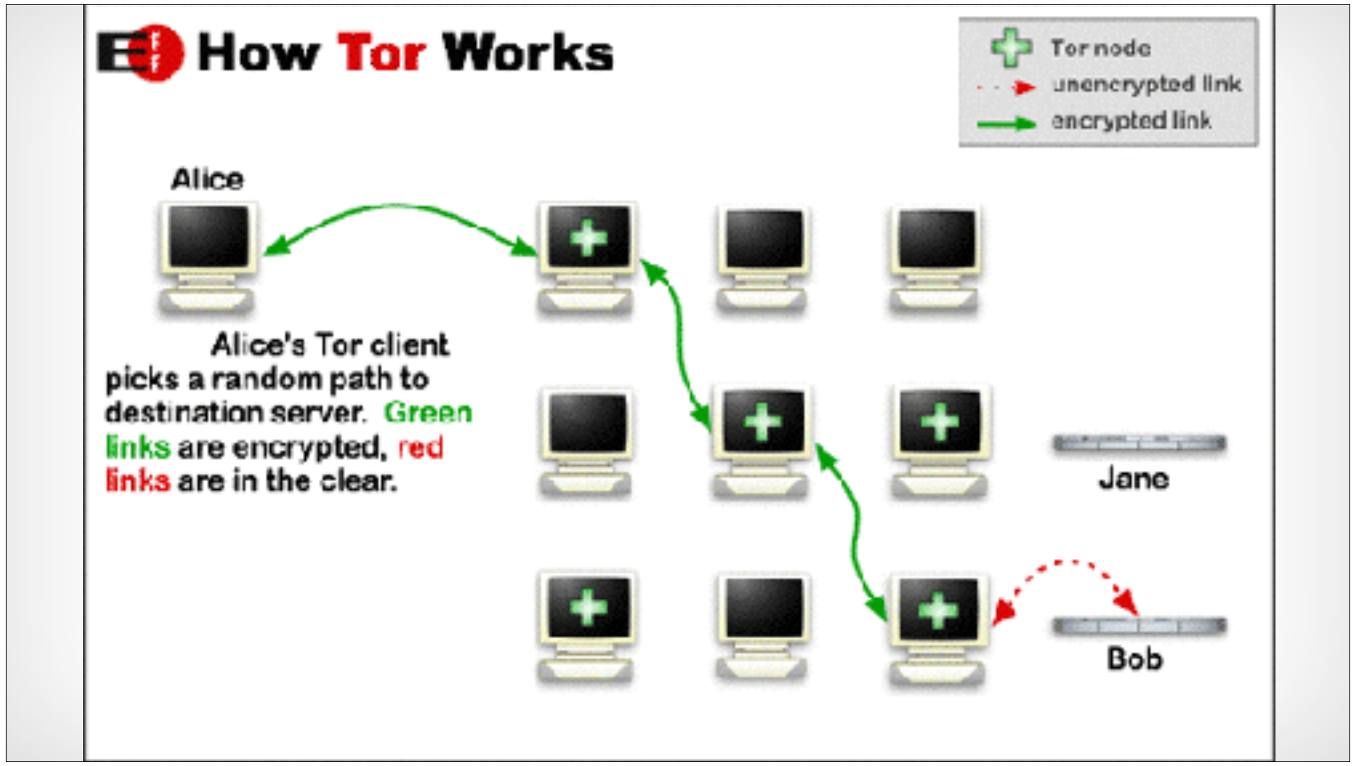
Well, Tor Seems Great!

That’s all fine and good as long as you trust all the monkeys. But what if you don’t?



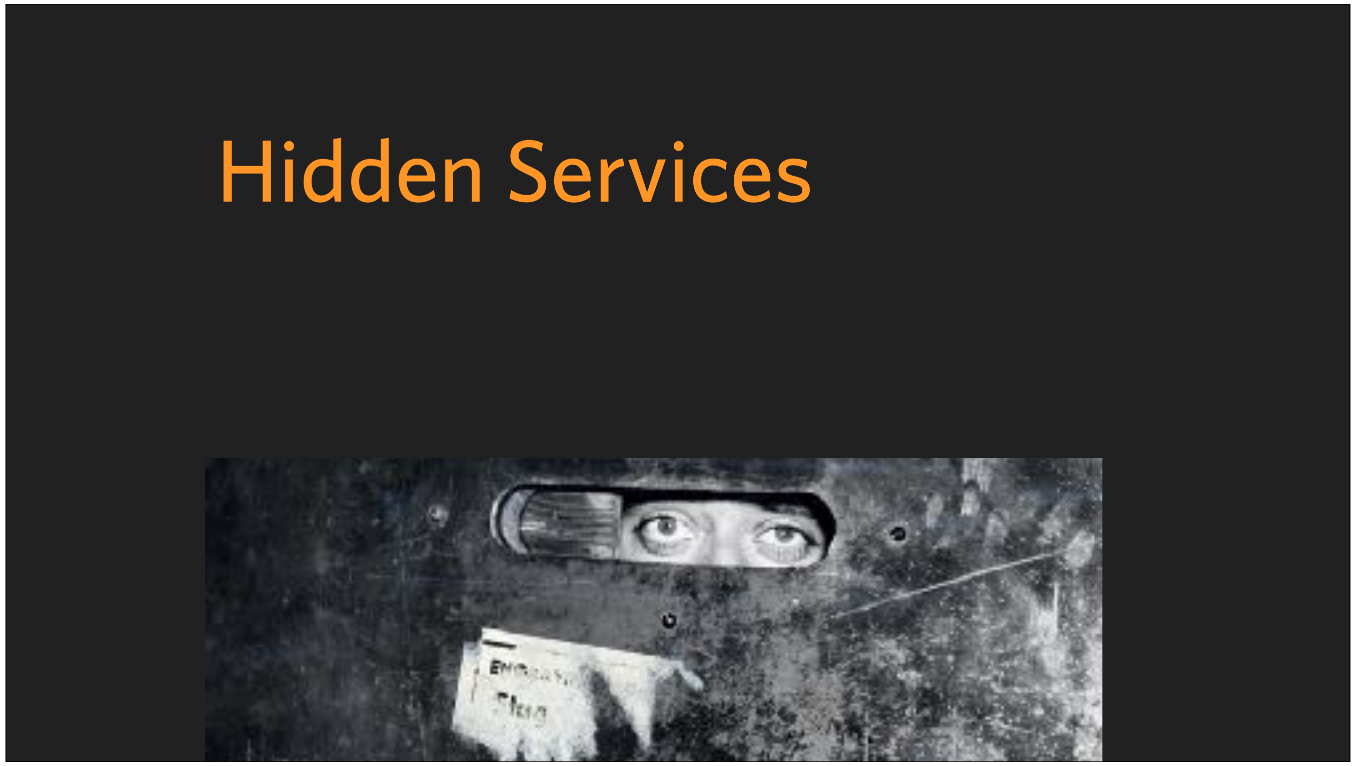
But There's A Problem

That's all fine and good as long as you trust all the monkeys. But what if you don't?



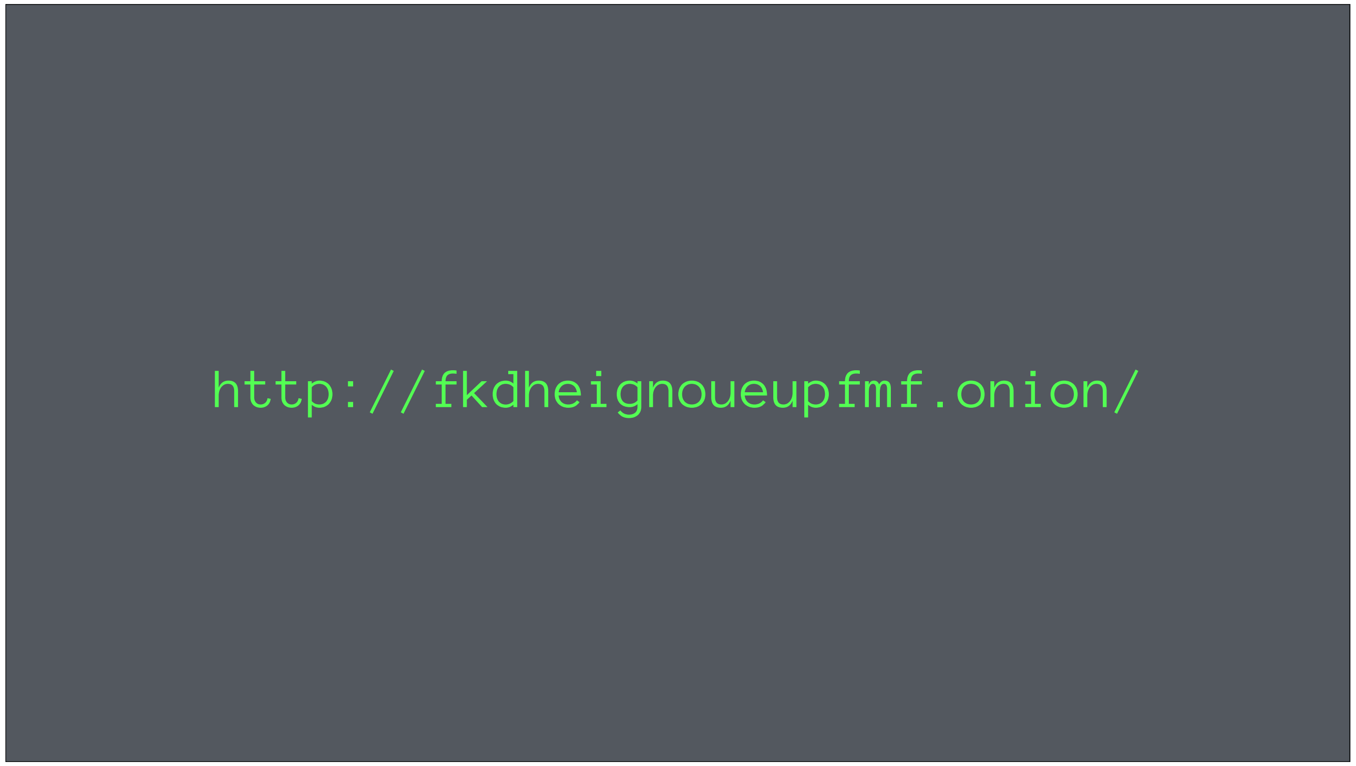
How Tor Works
Tor node
unencrypted link
encrypted link
Alice
Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Bob

If you notice, in the red line, there is an unencrypted hop. That final node, known as the exit node, has to decrypt your traffic to deliver it to a web server that doesn't speak Tor. This is where bad actors can prey on the chain of trust, either breaking into these exit nodes to spy, or even setting up their own exit nodes explicitly to spy.



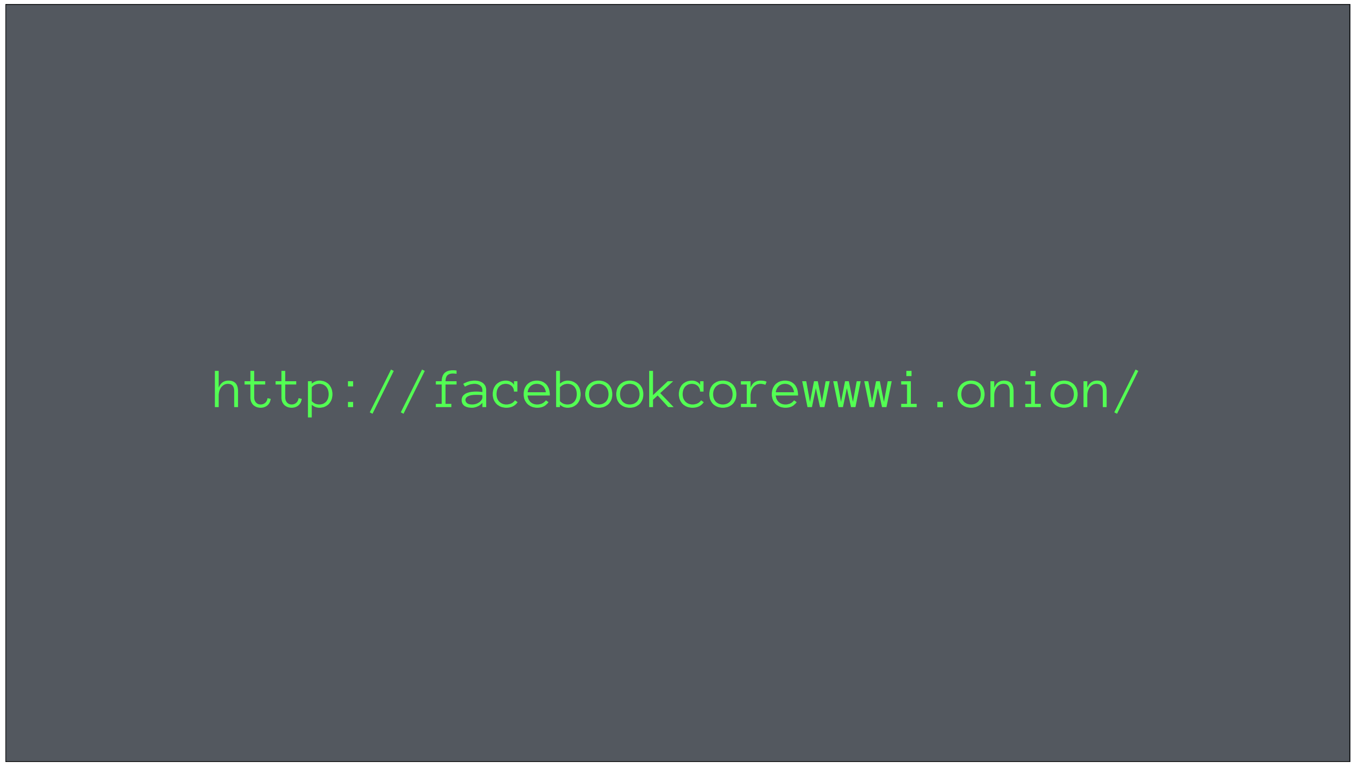
Hidden Services

And that’s where hidden services come in. This is where you actually put your server on the Tor network. It is no longer directly accessible, you need the Tor browser just to find it.



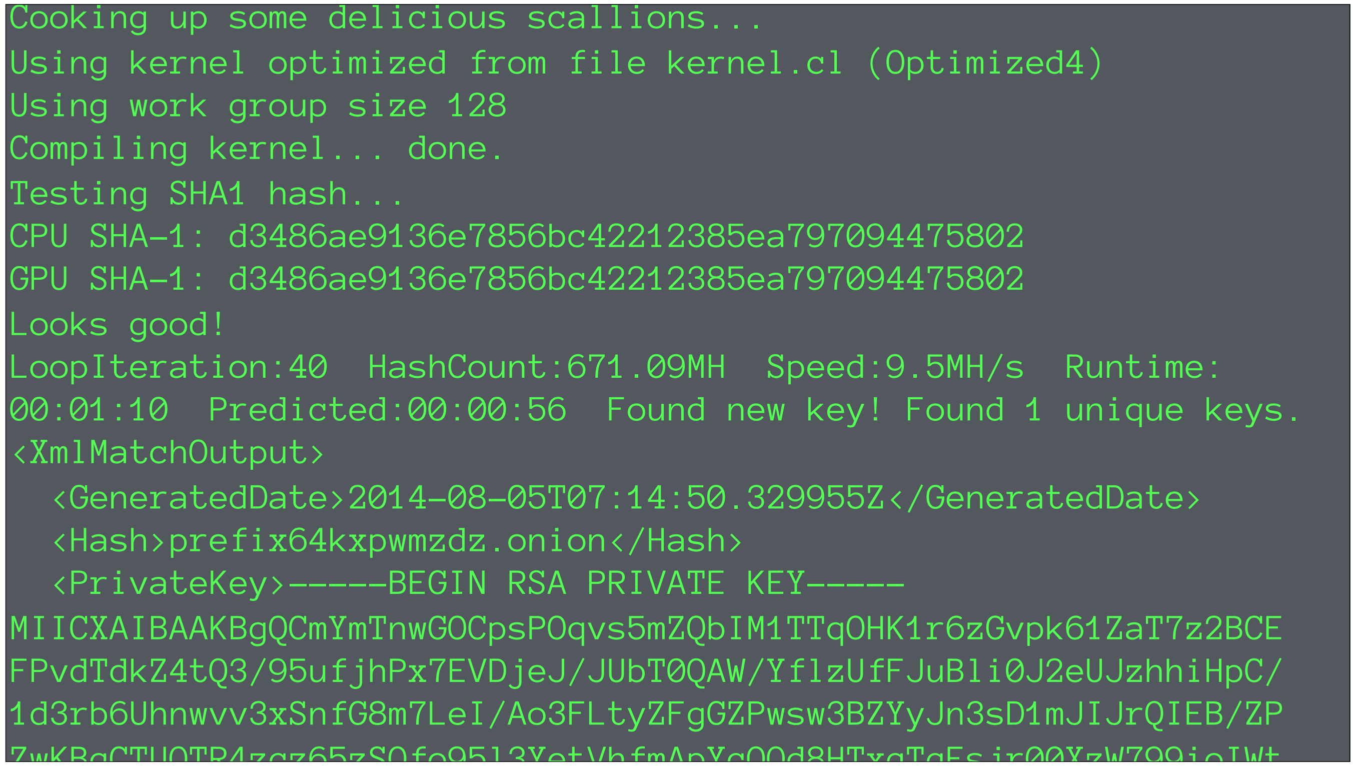
```
http://fkdheignoueupfmf.onion/
```

This is what you URL looks like. Not the friendliest. 16 cryptographically generated characters.



http://facebookcorewwwi.onion/

This is a real vanity domain name. These can’t be bought, they can only be earned. These URLs are the hash result of a public key, so you have to generate the public keys, and then generate the hash, and then sort.

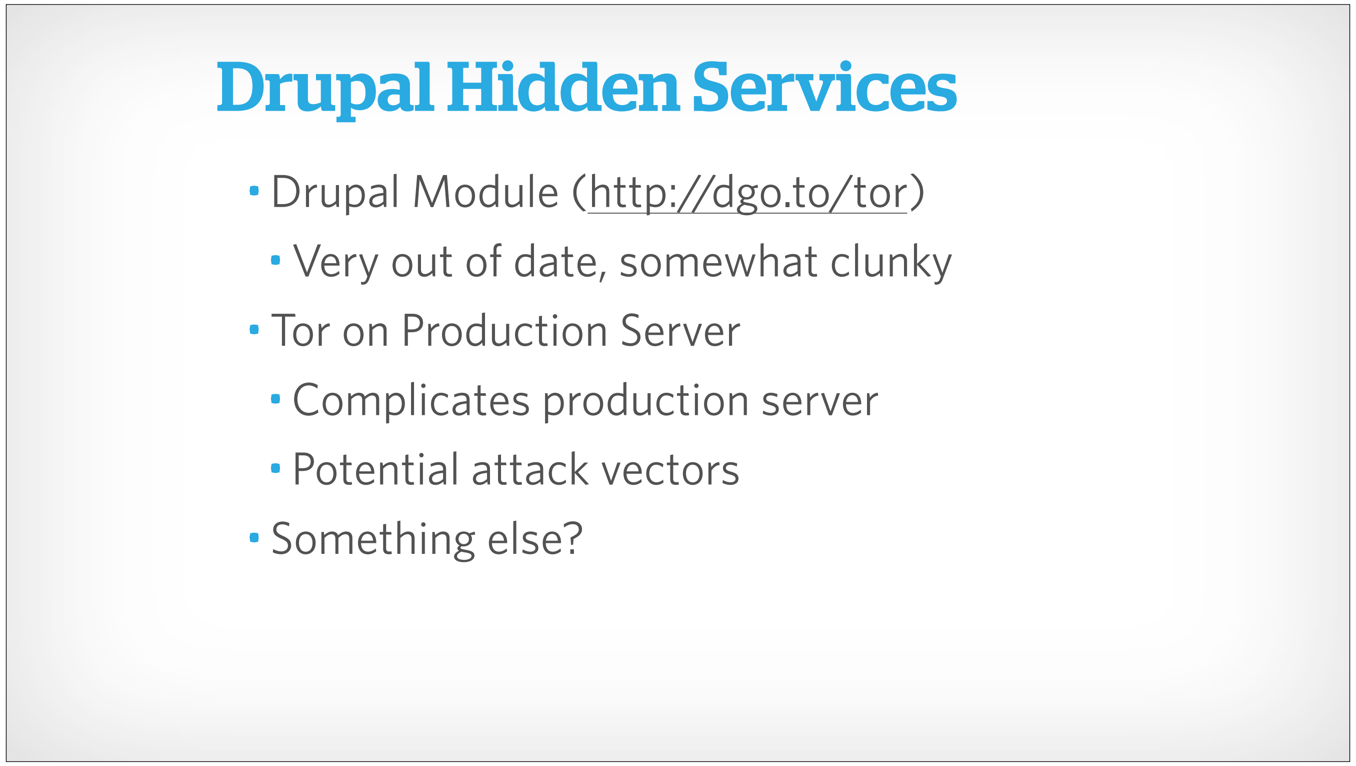


```
Cooking up some delicious scallions...
Using kernel optimized from file kernel.cl (Optimized4)
Using work group size 128
Compiling kernel... done.
Testing SHA1 hash...
CPU SHA-1: d3486ae9136e7856bc42212385ea797094475802
GPU SHA-1: d3486ae9136e7856bc42212385ea797094475802
Looks good!
LoopIteration:40  HashCount:671.09MH  Speed:9.5MH/s  Runtime:
00:01:10  Predicted:00:00:56  Found new key! Found 1 unique keys.
<XmlMatchOutput>
  <GeneratedDate>2014-08-05T07:14:50.329955Z</GeneratedDate>
  <Hash>prefix64kxpwmzdz.onion</Hash>
  <PrivateKey>-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQCmYmTnwGOCpsPOqvs5mZQbIM1TTqOHK1r6zGvpk61ZaT7z2BCE
FPvdTdkZ4tQ3/95ufjhPx7EVDjeJ/JUbT0QAW/YflzUfFJuBli0J2eUJzhhiHpC/
1d3rb6Uhnwvv3xSnfG8m7LeI/Ao3FLtyZFgGZPwsw3BZYyJn3sD1mJIJrQIEB/ZP
ZwKBgCTUOTR4zcz65zSOfo9513YetVhfmApYcOOd8HTxqTqEsjr00XzW799joIWt
```

This is a real vanity domain name. These can’t be bought, they can only be earned. These URLs are the hash result of a public key, so you have to generate the public keys, and then generate the hash, and then sort.

But Drupal?

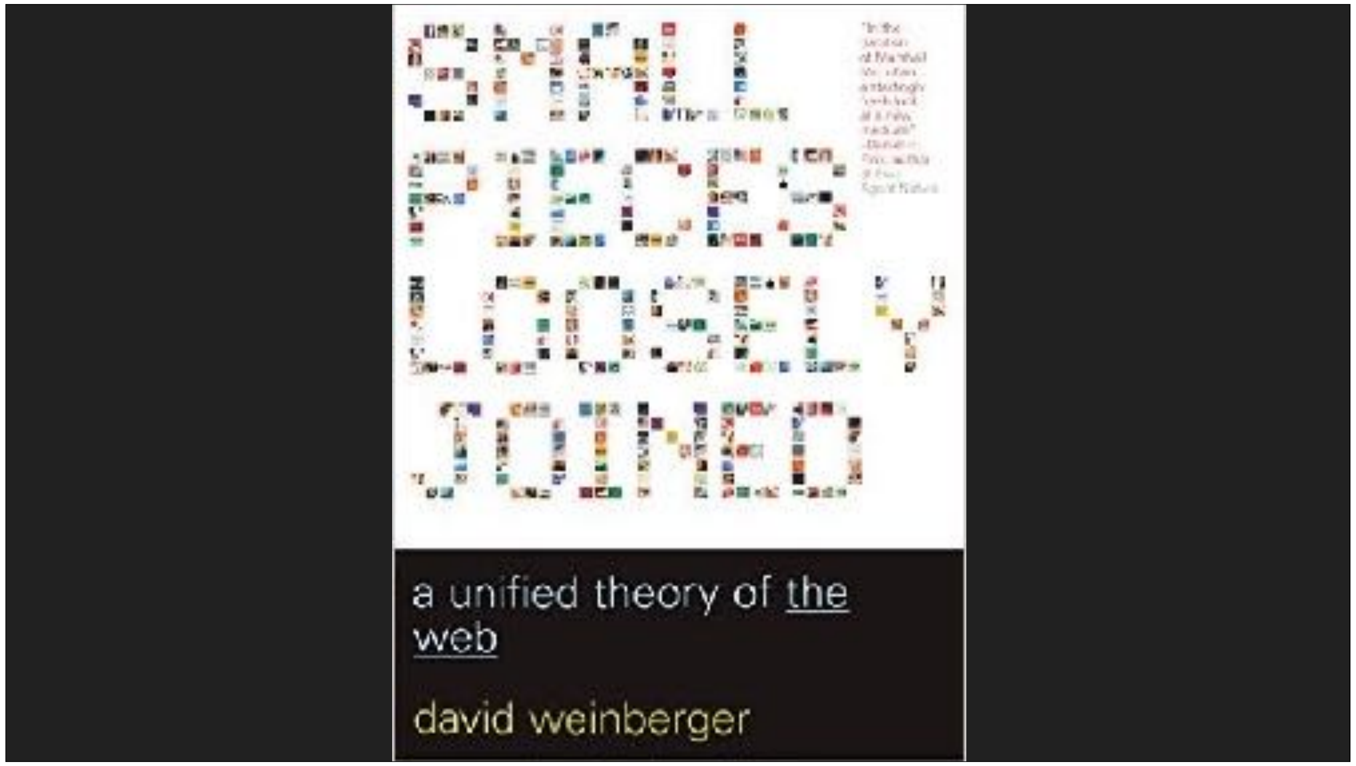
And that’s where hidden services come in. This is where you actually put your server on the Tor network. It is no longer directly accessible, you need the Tor browser just to find it.



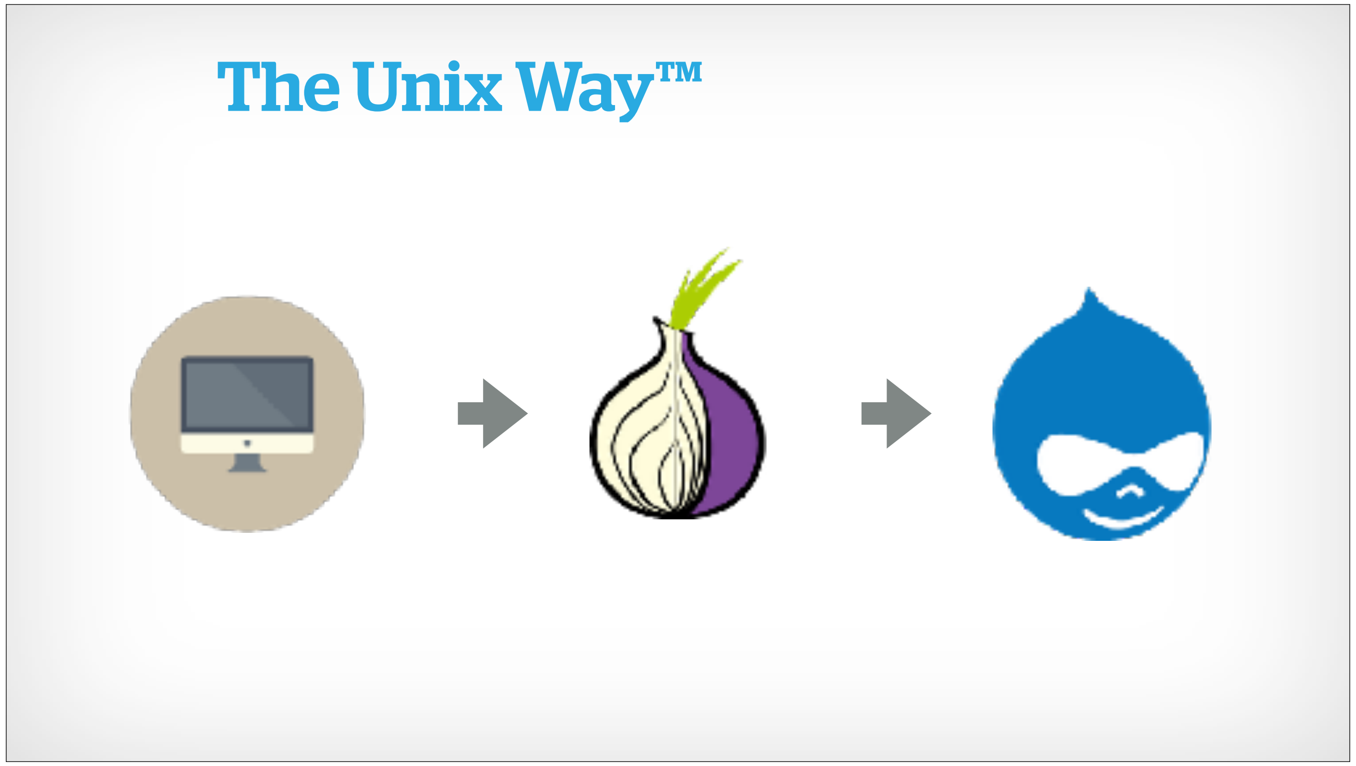
Drupal Hidden Services

- Drupal Module (http://dgo.to/tor)
  - Very out of date, somewhat clunky
- Tor on Production Server
  - Complicates production server
  - Potential attack vectors
- Something else?

The Drupal module is wicked out of date
Putting the Tor service on the same server is fine, but complicates the setup, and leaves attack surface

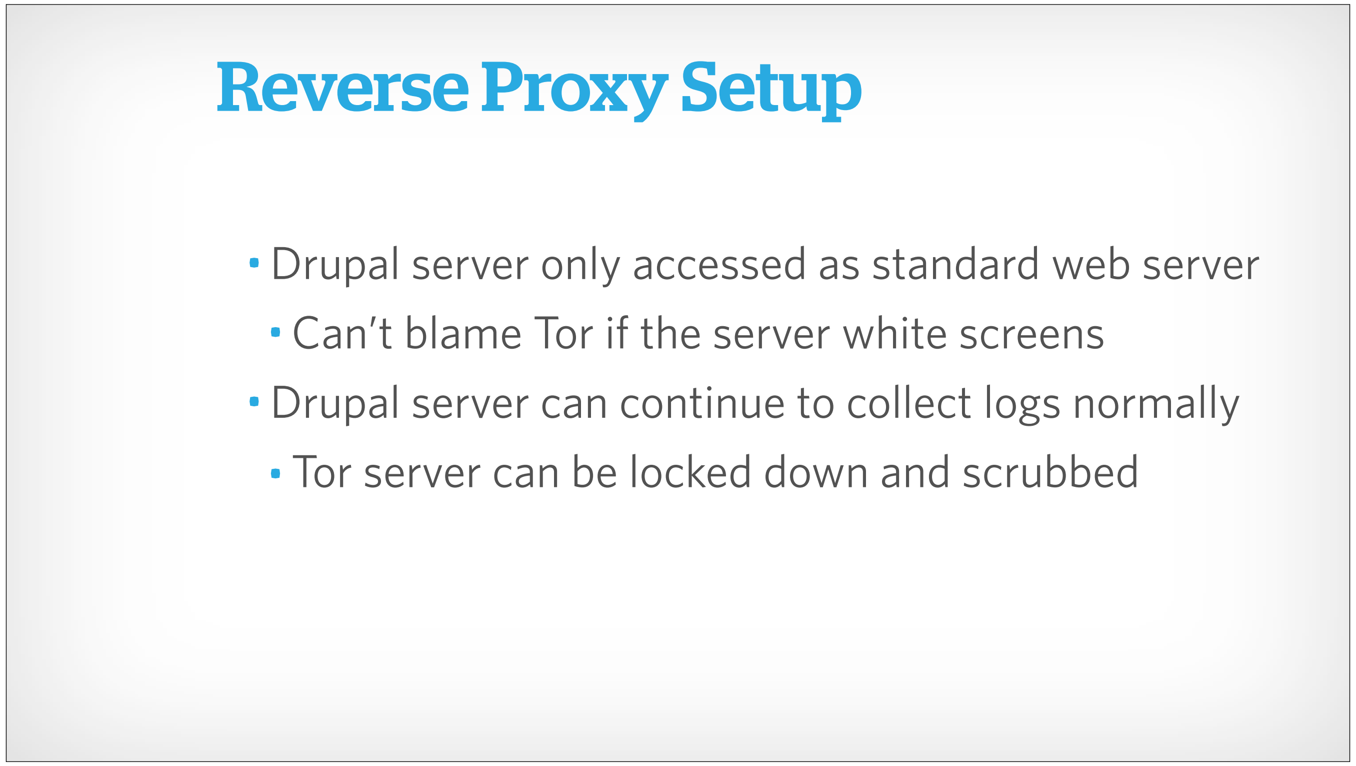


And that’s where hidden services come in. This is where you actually put your server on the Tor network. It is no longer directly accessible, you need the Tor browser just to find it.



The Unix Way™

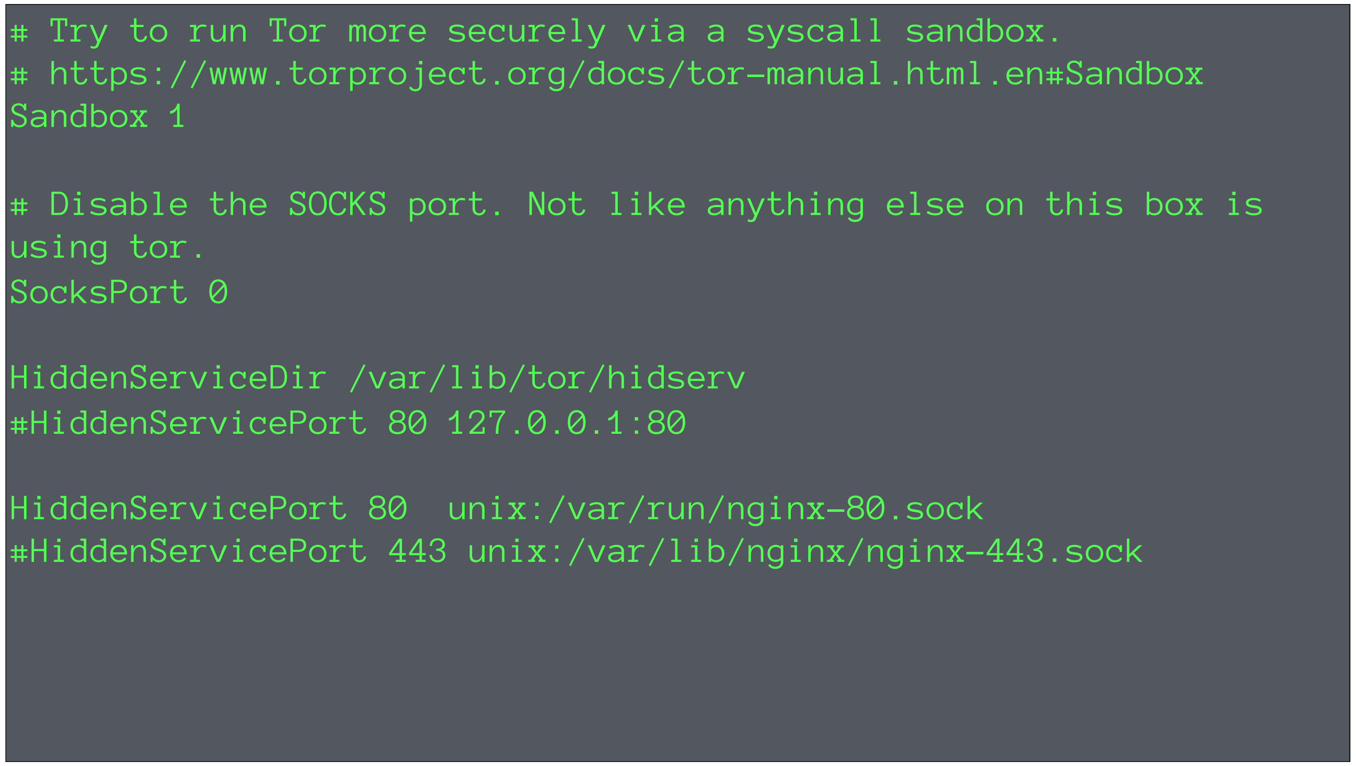
Two servers. Standard production Drupal server is hidden behind an Nginx proxy server with Tor installed.



Reverse Proxy Setup

- Drupal server only accessed as standard web server
  - Can't blame Tor if the server white screens
- Drupal server can continue to collect logs normally
  - Tor server can be locked down and scrubbed

Two servers. Standard production Drupal server is hidden behind an Nginx proxy server with Tor installed. Debugging a server without logs is kind of a pain, so keep them turned on where you need them, but now where you don't.

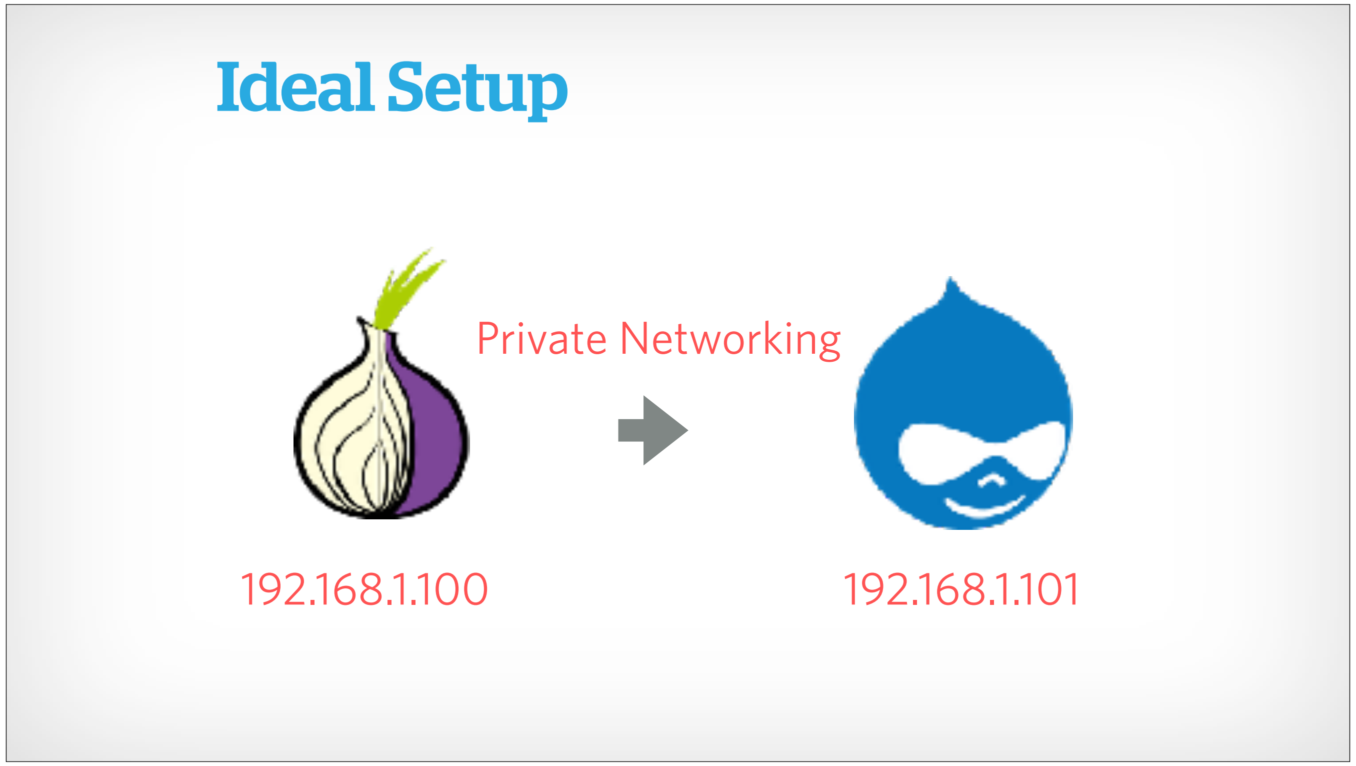


```
# Try to run Tor more securely via a syscall sandbox.
# https://www.torproject.org/docs/tor-manual.html.en#Sandbox
Sandbox 1

# Disable the SOCKS port. Not like anything else on this box is
using tor.
SocksPort 0

HiddenServiceDir /var/lib/tor/hidserv
#HiddenServicePort 80 127.0.0.1:80

HiddenServicePort 80  unix:/var/run/nginx-80.sock
#HiddenServicePort 443 unix:/var/lib/nginx/nginx-443.sock
```

For a command line, hacker centric piece of software, Tor is surprisingly simple to setup

```
server {
    server_name fdg22p3lmweopgho.onion;
    listen unix:/var/run/nginx-80.sock;
    allow "unix:";
    deny all;
    #listen 80;
    #allow 127.0.0.1;

    # Set cache on this nginx end so that we avoid fetching from
    # the real infrastructure when possible.
    proxy_cache tor;
    proxy_cache_valid any 5m;
    proxy_cache_revalidate on;
    proxy_cache_use_stale timeout updating;
    proxy_cache_key $request_uri;
    proxy_ignore_headers expires set-cookie;
```

nginx less so, but it’s not too much work
first we setup the basic server and point it to our Tor socket, and throw some caching into the mix



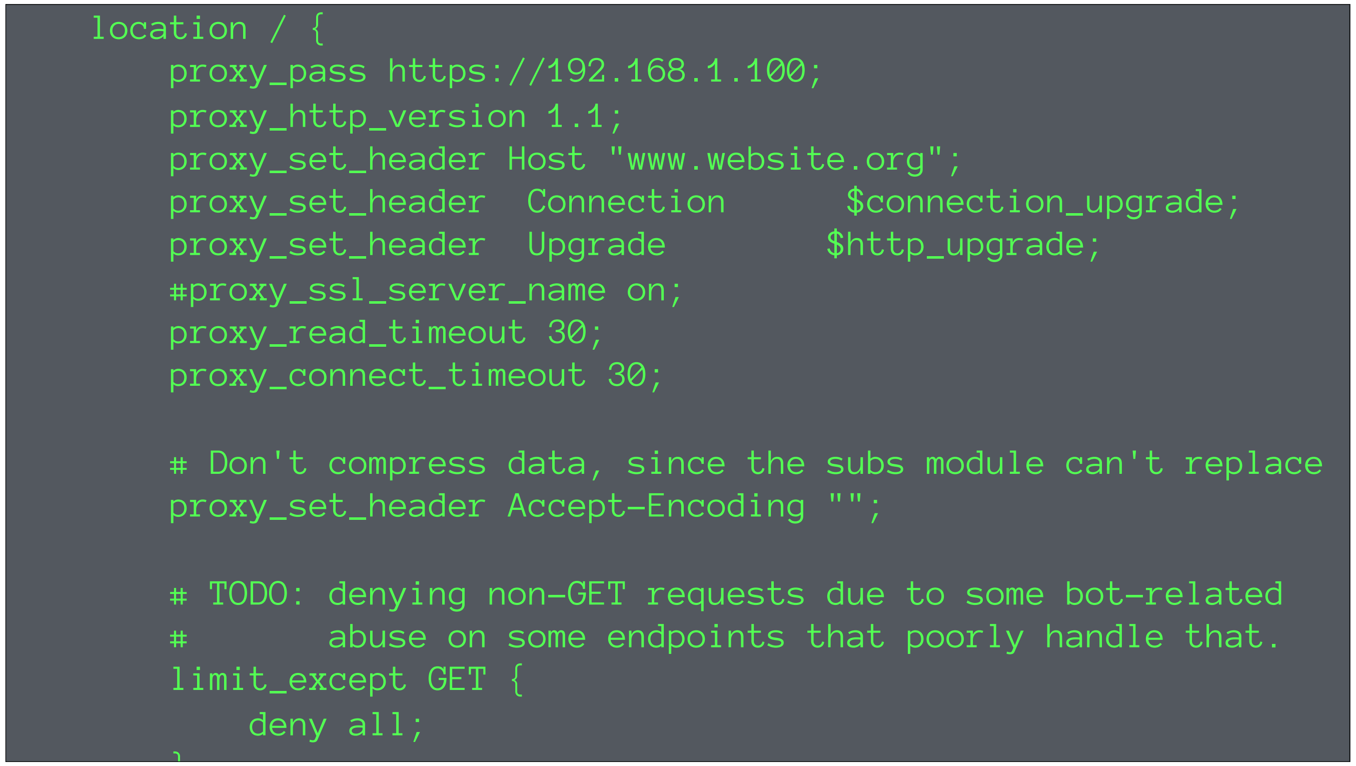
Ideal Setup

Private Networking

192.168.1.100

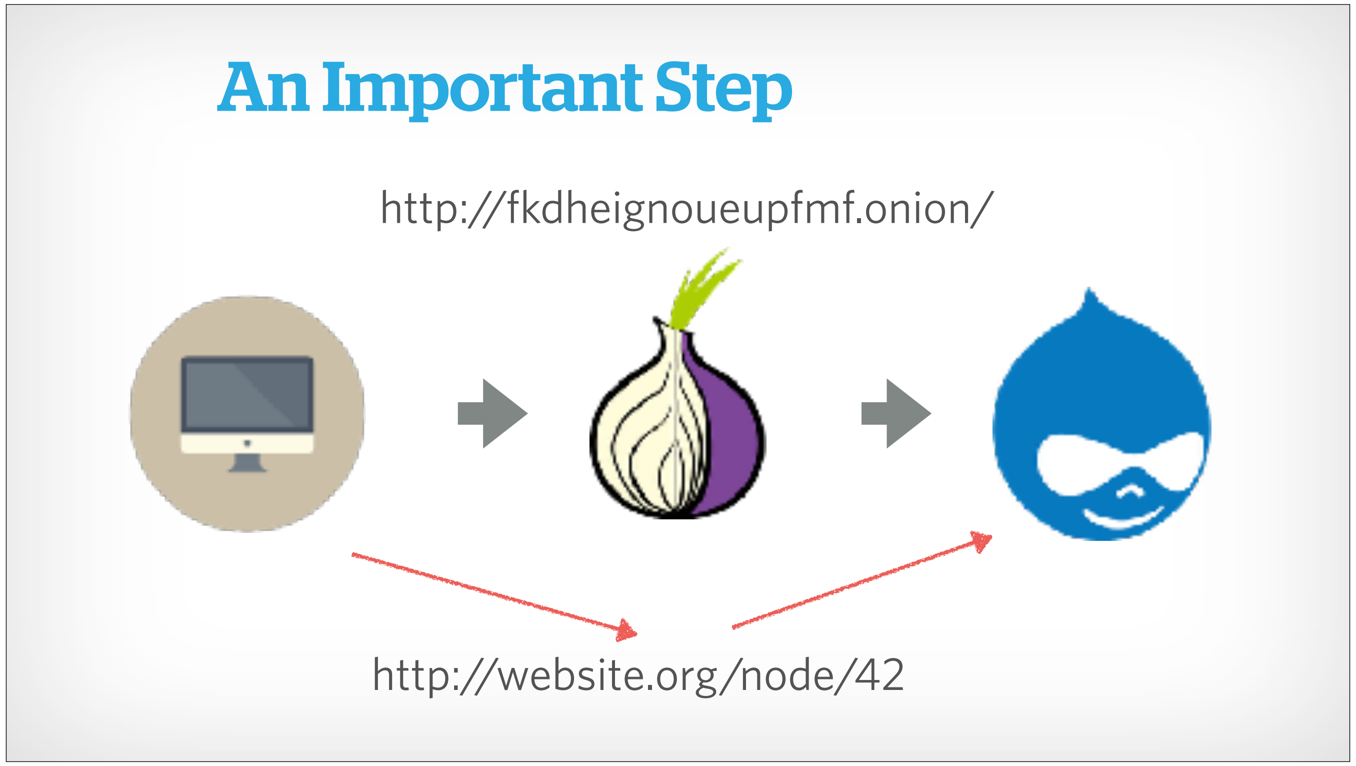
192.168.1.101

You aren’t doing a lot of good if you let Drupal and Tor talk to each other over public networking. Our particular setup was easily accomplished because the client was in the Rackspace Cloud, which allows for direct machine to machine internal networking. This kind of setup wouldn’t be possible in all managed hosting, like on Pantheon, but can be accomplished when you control the full stack or use something like Rackspace. You could maybe do it on Acquia? If you asked really nice.



```
    location / {
        proxy_pass https://192.168.1.100;
        proxy_http_version 1.1;
        proxy_set_header Host "www.website.org";
        proxy_set_header  Connection      $connection_upgrade;
        proxy_set_header  Upgrade        $http_upgrade;
        #proxy_ssl_server_name on;
        proxy_read_timeout 30;
        proxy_connect_timeout 30;

        # Don't compress data, since the subs module can't replace
        proxy_set_header Accept-Encoding "";

        # TODO: denying non-GET requests due to some bot-related
        #       abuse on some endpoints that poorly handle that.
        limit_except GET {
            deny all;
        }
```

Make the actual reverse proxy connection to the internal IP of our host Drupal server



An Important Step

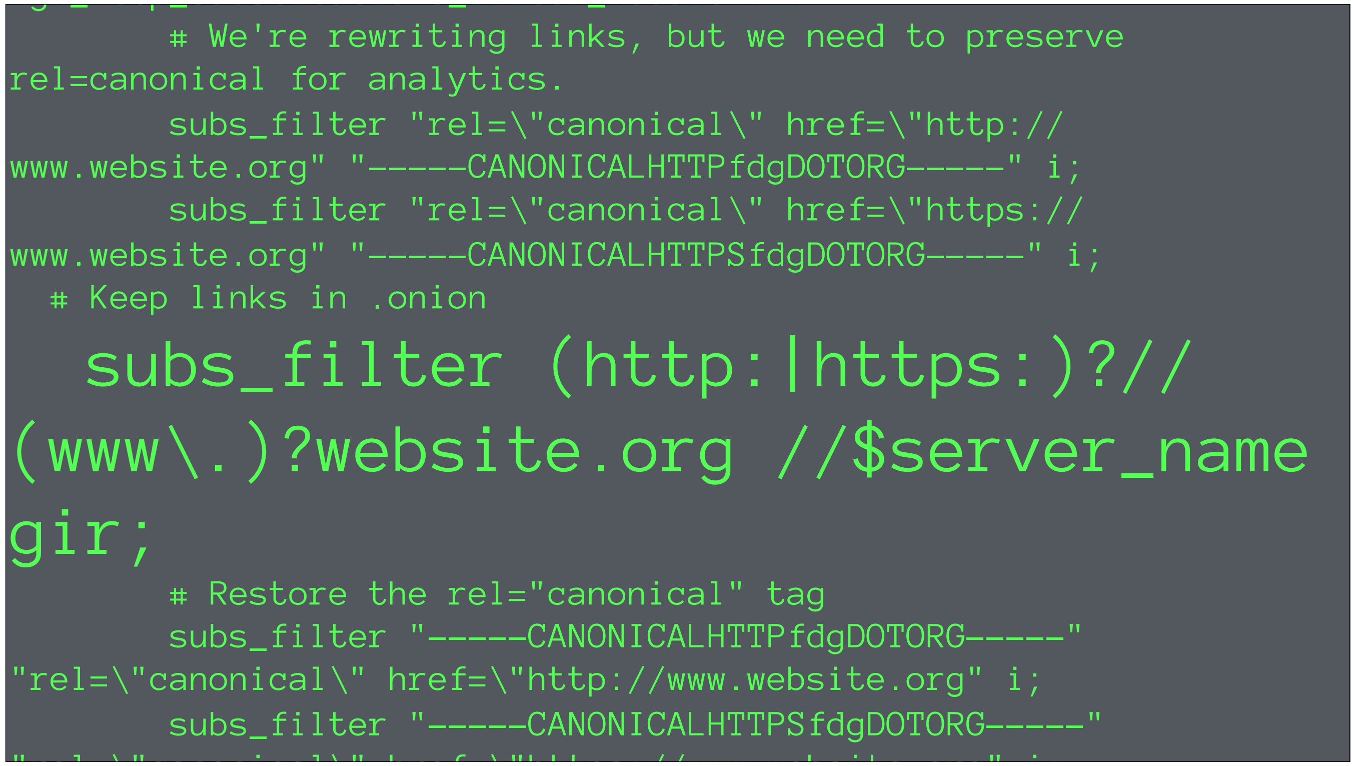
http://fkdheignoueupfmf.onion/

http://website.org/node/42

We need to make sue we don’t accidentally kick people out of their protected connection

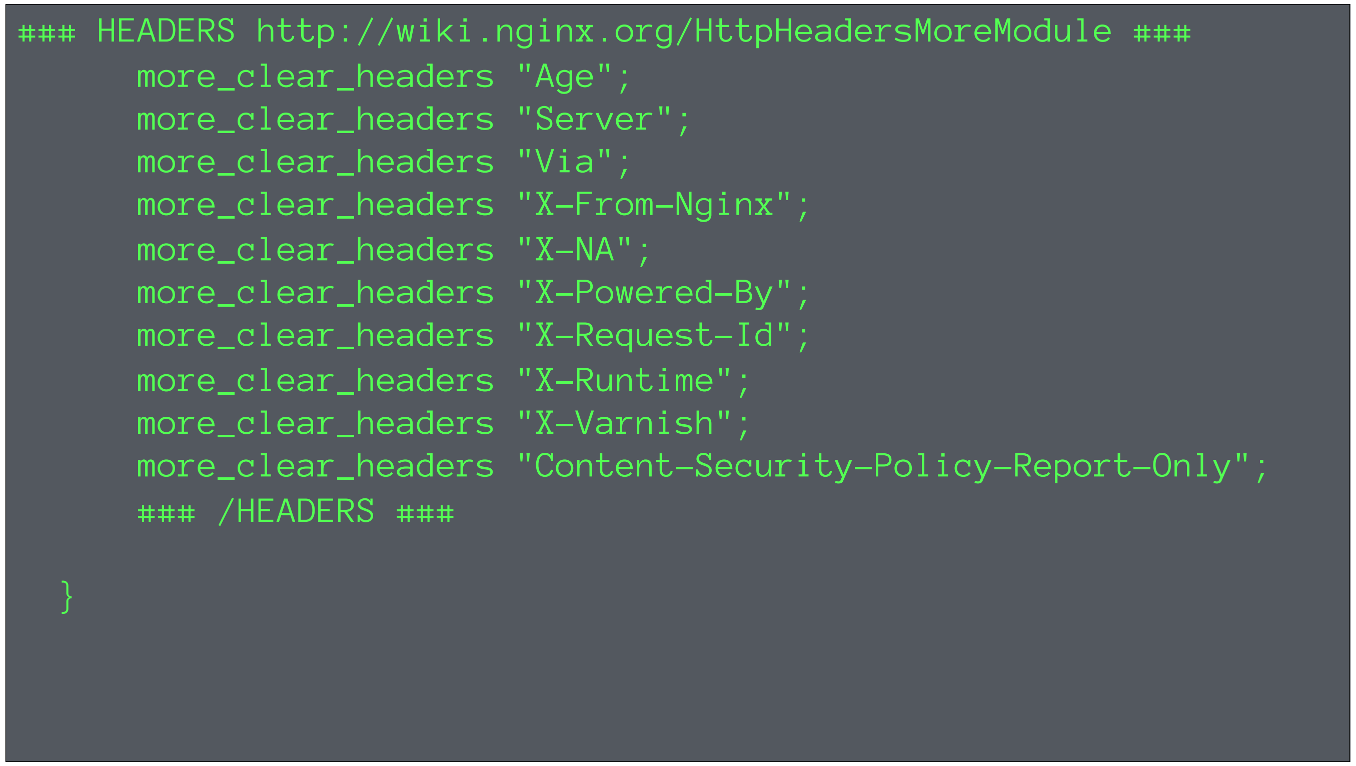
```
### SUBS https://github.com/yaoweibin/
ngx_http_substitutions_filter_module ###
        # We're rewriting links, but we need to preserve
rel=canonical for analytics.
        subs_filter "rel=\"canonical\" href=\"http://
www.website.org" "-----CANONICALHTTPfdgDOTORG-----" i;
        subs_filter "rel=\"canonical\" href=\"https://
www.website.org" "-----CANONICALHTTPSfdgDOTORG-----" i;
  # Keep links in .onion
  subs_filter (http:|https:)?//(www\.)?website.org //$server_name
gir;
        # Restore the rel="canonical" tag
        subs_filter "-----CANONICALHTTPfdgDOTORG-----"
"rel=\"canonical\" href=\"http://www.website.org" i;
        subs_filter "-----CANONICALHTTPSfdgDOTORG-----"
"rel=\"canonical\" href=\"https://www.website.org" i;
        ### /SUBS ###
```

The fun begins. We first need to recompile nginx to enable rewriting of strings
I’m not 100% clear why analytics are important to onion sites, but publishers always want their metatags
Then we rewrite all links and images on the site to keep them communicating over tor



```
        # We're rewriting links, but we need to preserve
rel=canonical for analytics.
        subs_filter "rel=\"canonical\" href=\"http://
www.website.org" "-----CANONICALHTTPfdgDOTORG-----" i;
        subs_filter "rel=\"canonical\" href=\"https://
www.website.org" "-----CANONICALHTTPSfdgDOTORG-----" i;
  # Keep links in .onion
  subs_filter (http:|https:)?//
(www\.)?website.org //$server_name
gir;
        # Restore the rel="canonical" tag
        subs_filter "-----CANONICALHTTPfdgDOTORG-----"
"rel=\"canonical\" href=\"http://www.website.org" i;
        subs_filter "-----CANONICALHTTPSfdgDOTORG-----"
```

Then we rewrite all links and images on the site to keep them communicating over tor

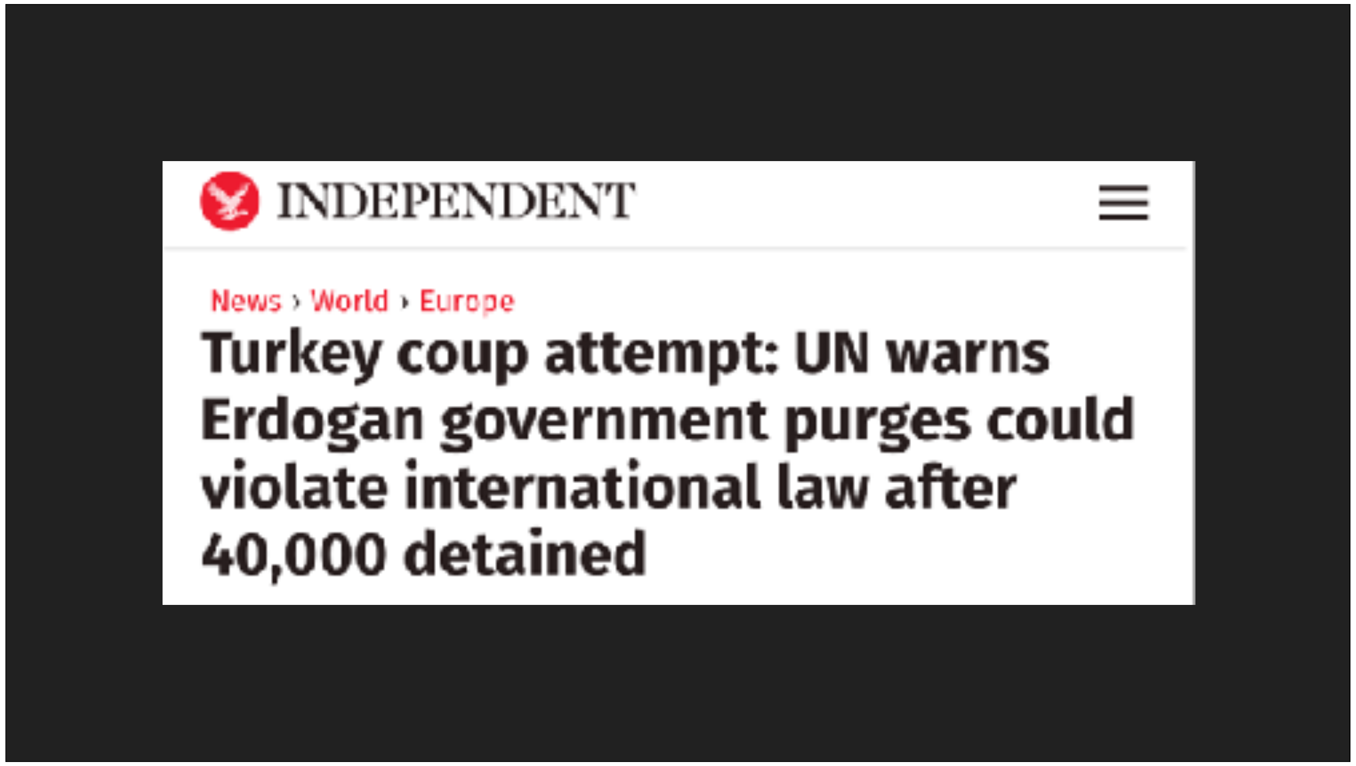


```
### HEADERS http://wiki.nginx.org/HttpHeadersMoreModule ###
      more_clear_headers "Age";
      more_clear_headers "Server";
      more_clear_headers "Via";
      more_clear_headers "X-From-Nginx";
      more_clear_headers "X-NA";
      more_clear_headers "X-Powered-By";
      more_clear_headers "X-Request-Id";
      more_clear_headers "X-Runtime";
      more_clear_headers "X-Varnish";
      more_clear_headers "Content-Security-Policy-Report-Only";
      ### /HEADERS ###

  }
```

Finally, we use another custom module to keep nginx from lying to browsers

Ideal Setup

All of this is well and good, but what if someone shows up with a warrant?

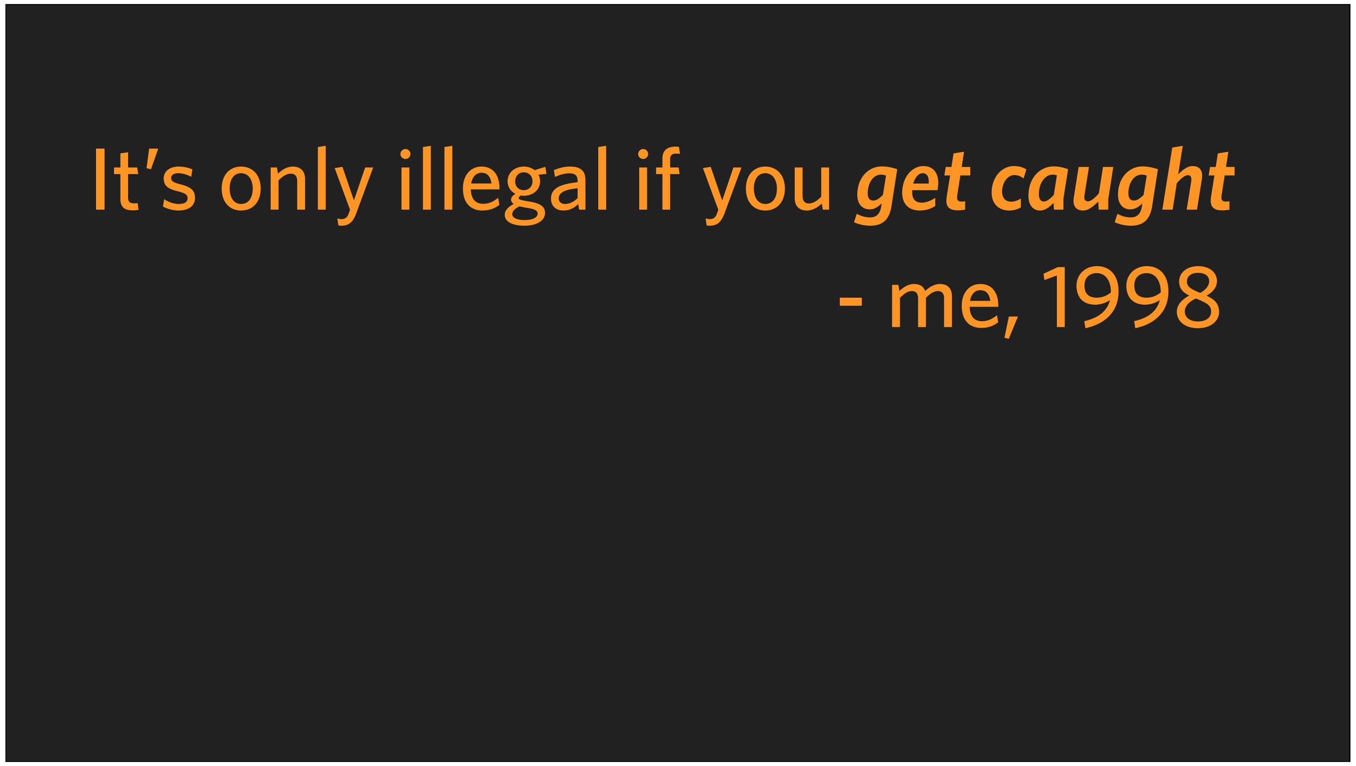


INDEPENDENT

News › World › Europe

Turkey coup attempt: UN warns Erdogan government purges could violate international law after 40,000 detained

It’s only secure if they can’t prove anything

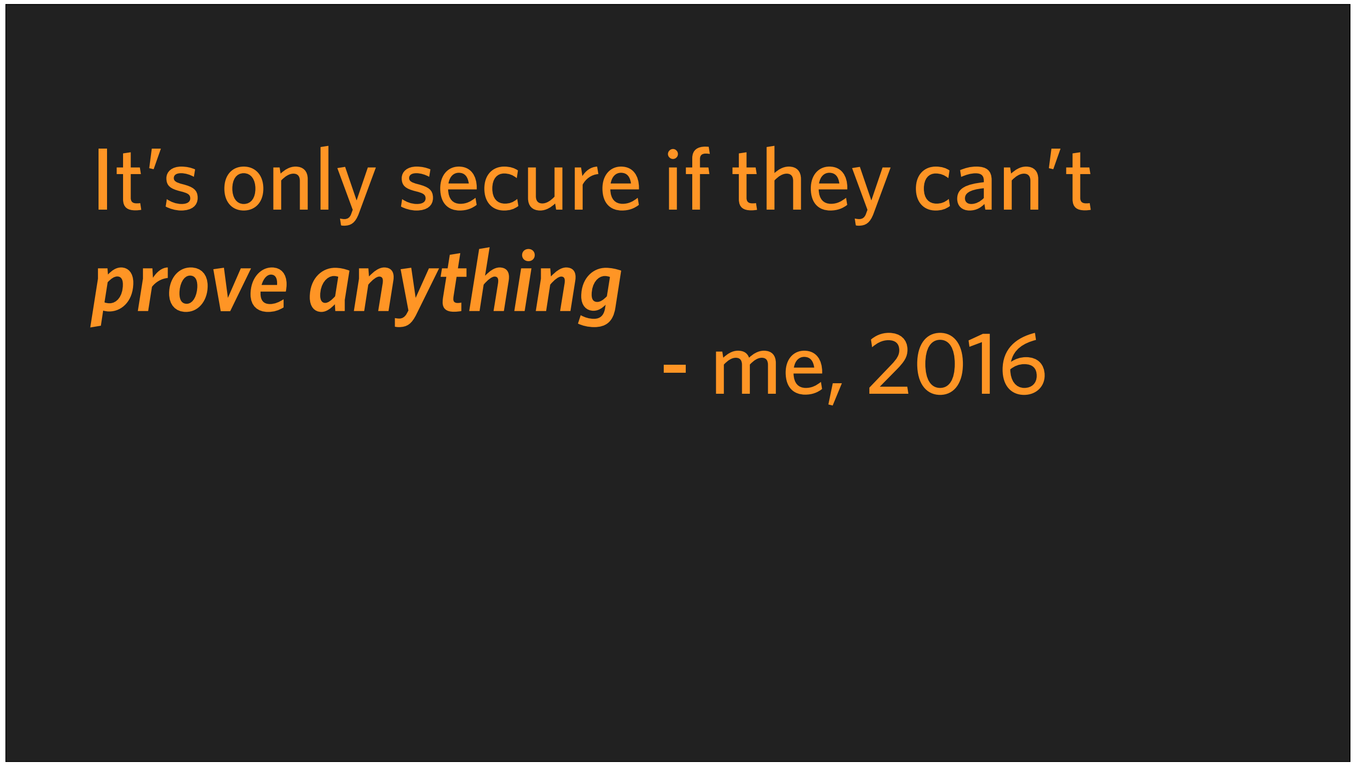


It’s only illegal if you ***get caught***

- me, 1998

The motto of my misspent youth

It’s only secure if they can’t prove anything

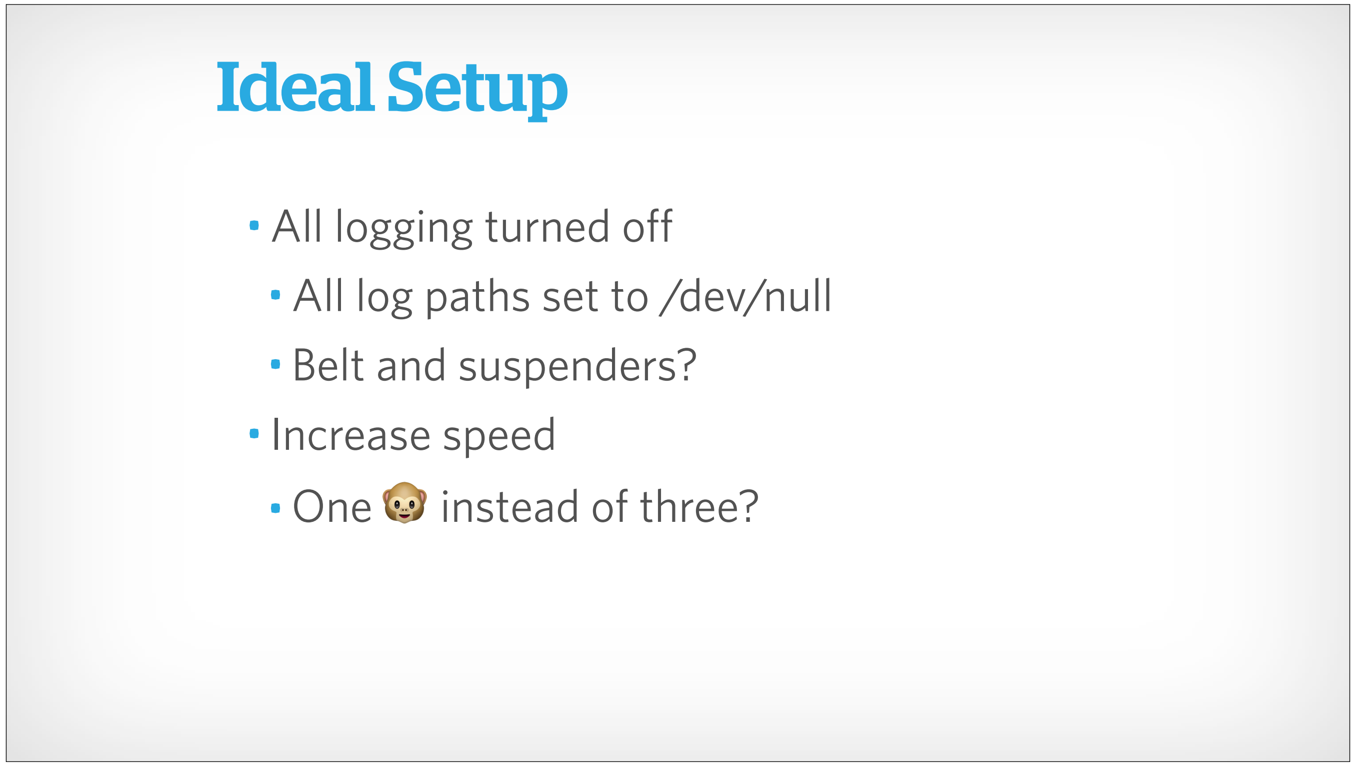


It's only secure if they can't ***prove anything***

- me, 2016

The motto of my misspent youth

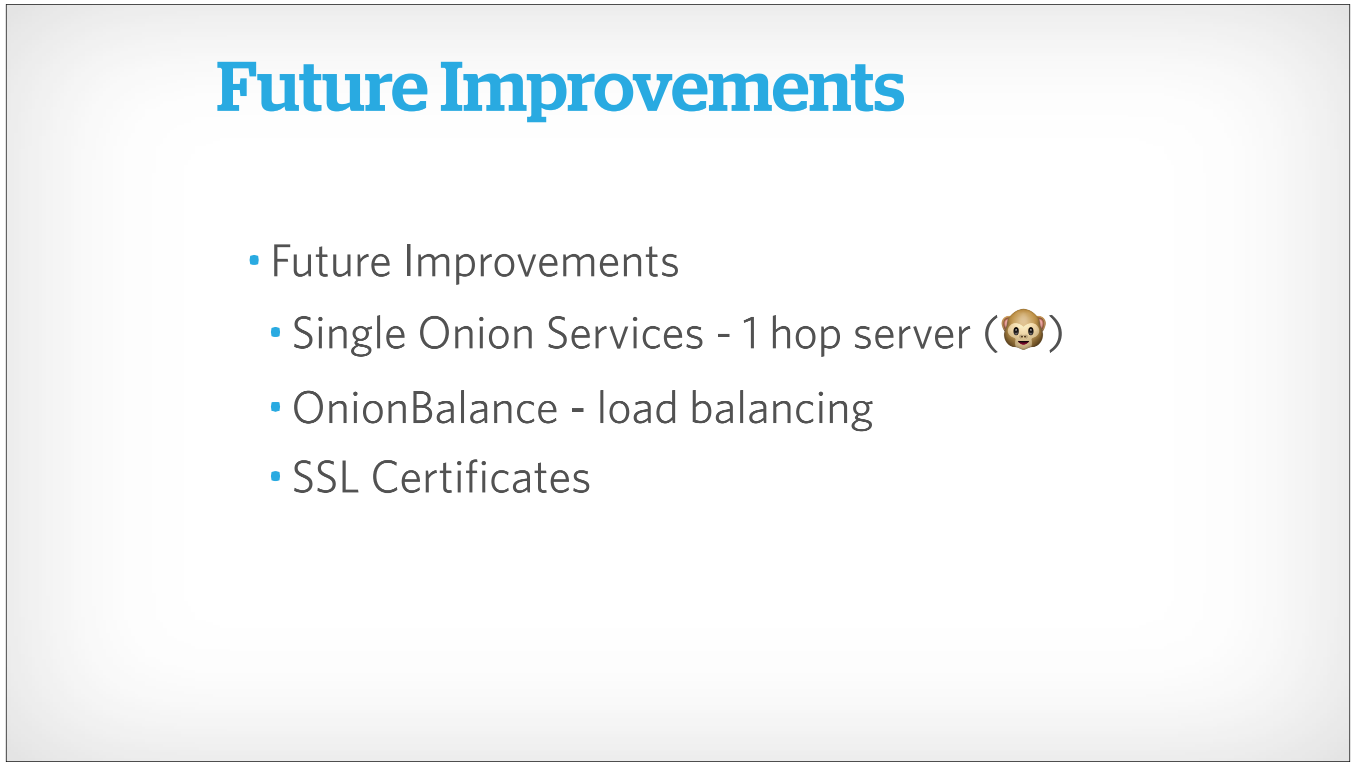
It's only secure if they can't prove anything



Ideal Setup

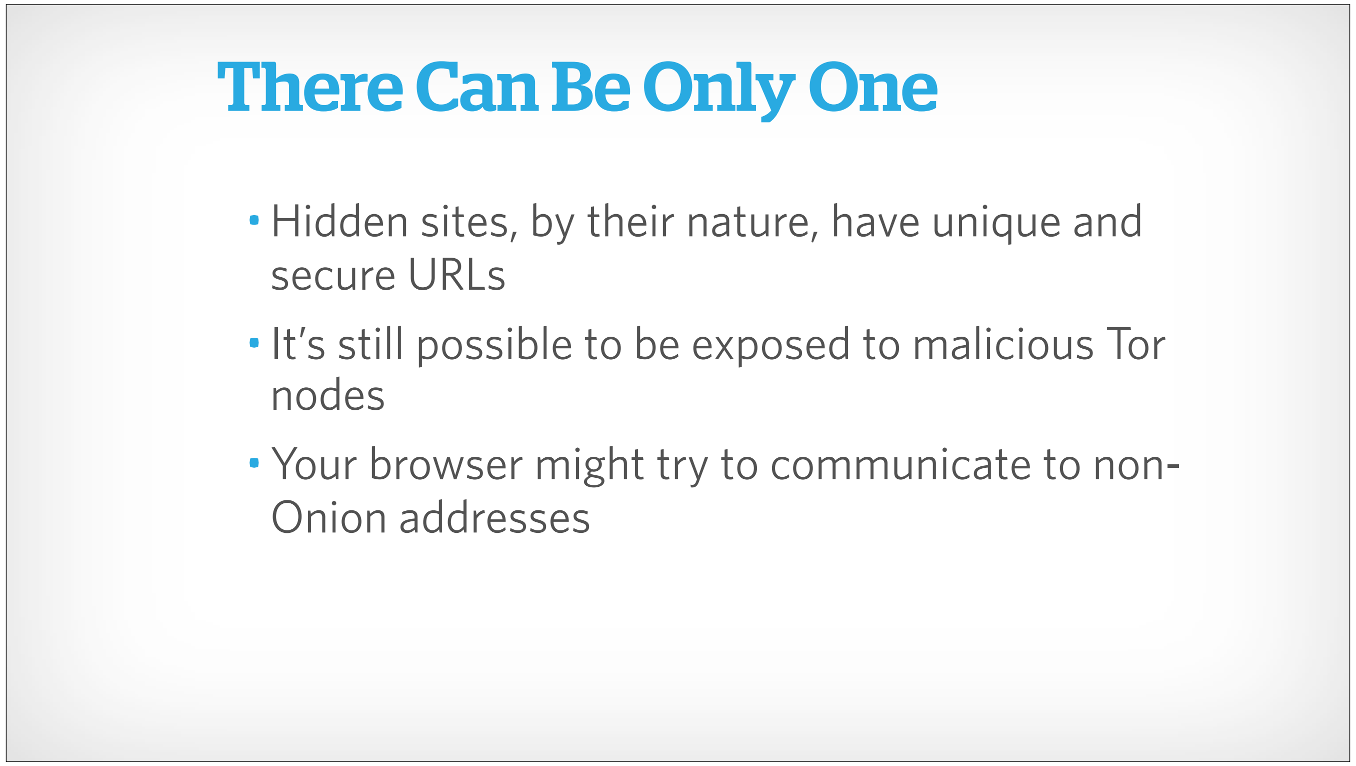
- All logging turned off
  - All log paths set to /dev/null
  - Belt and suspenders?
- Increase speed
  - One 🐵 instead of three?

You aren’t doing a lot of good if you let Drupal and Tor talk to each other over public networking. Our particular setup was easily accomplished because the client was in the Rackspace Cloud, which allows for direct machine to machine internal networking. This kind of setup wouldn’t be possible in all managed hosting, like on Pantheon, but can be accomplished when you control the full stack or use something like Rackspace. You could maybe do it on Acquia? If you asked really nice.



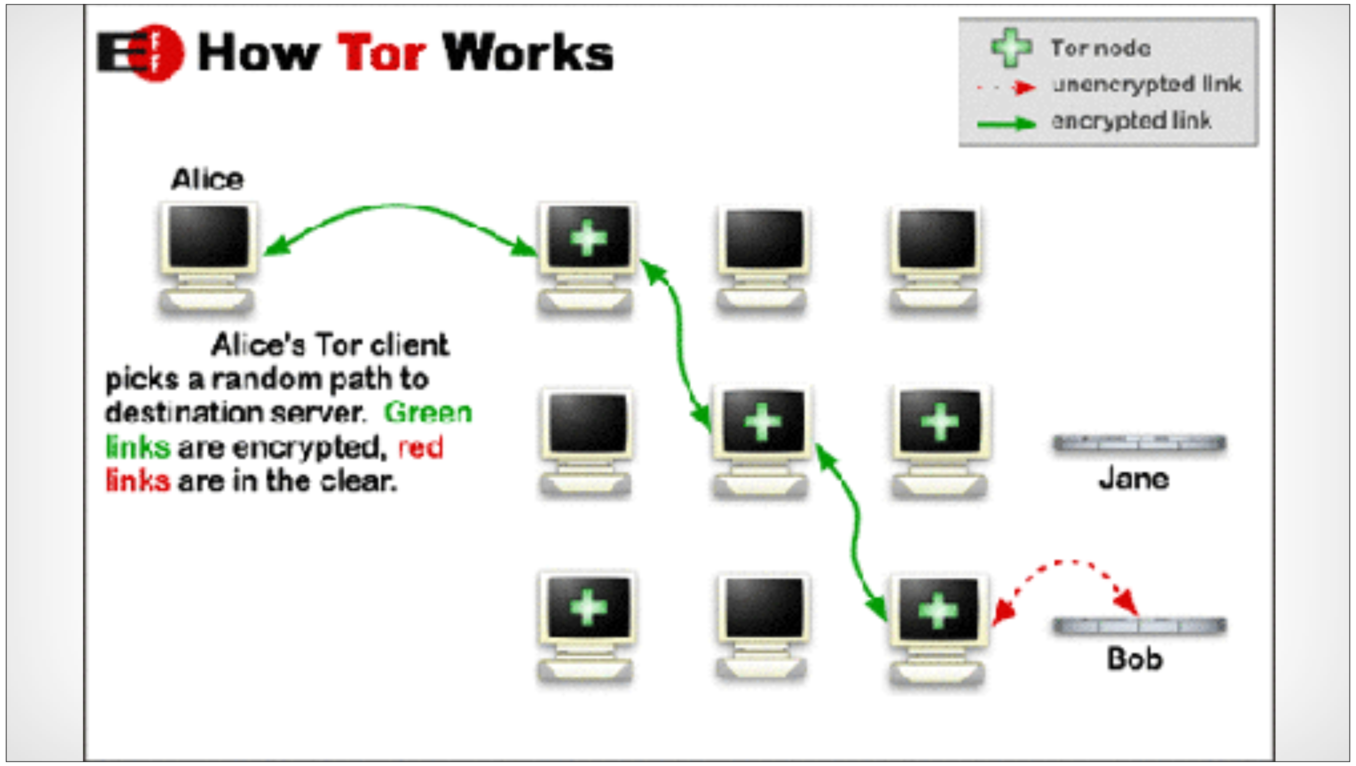
Future Improvements

- Future Improvements
  - Single Onion Services - 1 hop server (🐵)
  - OnionBalance - load balancing
  - SSL Certificates

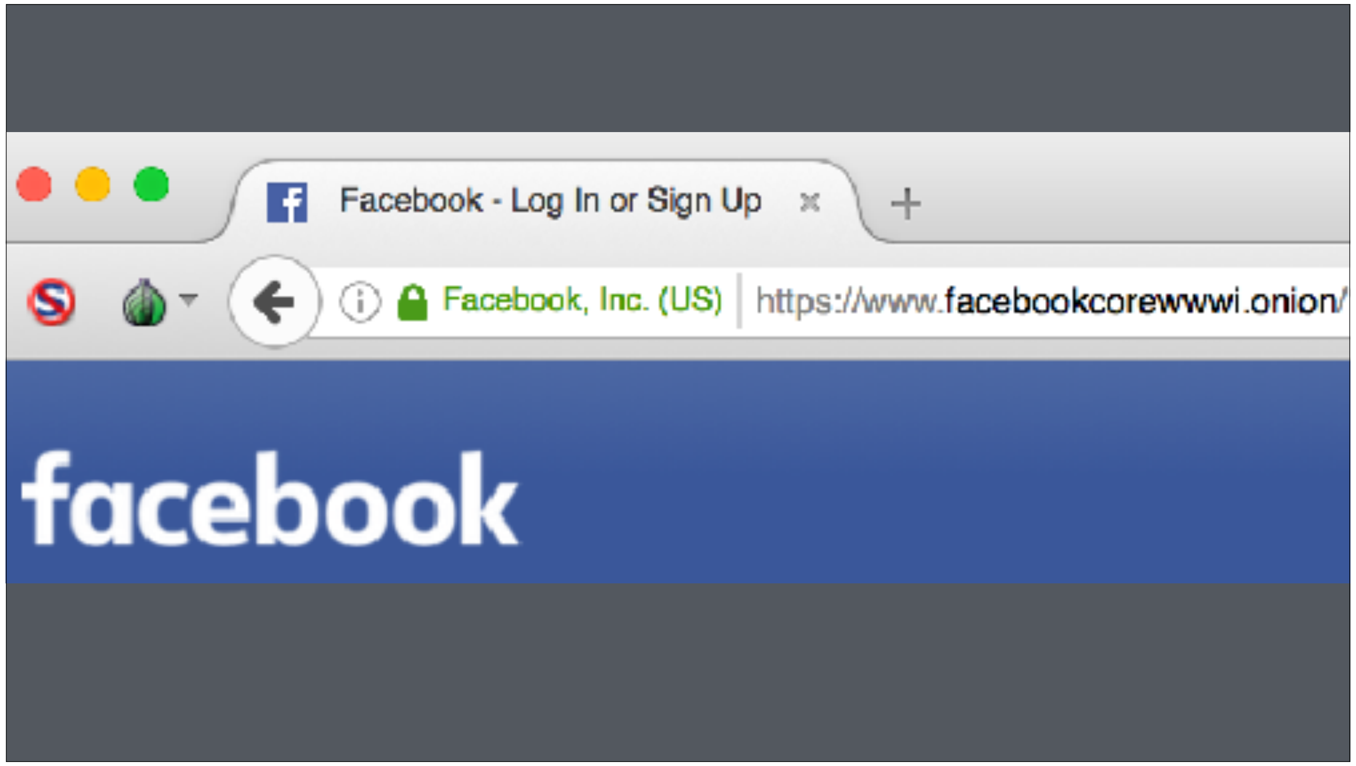


There Can Be Only One

- Hidden sites, by their nature, have unique and secure URLs
- It’s still possible to be exposed to malicious Tor nodes
- Your browser might try to communicate to non-Onion addresses


How Tor Works
Tor node
unencrypted link
encrypted link
Alice
Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Bob

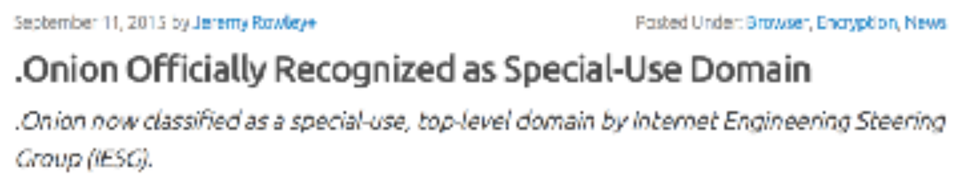
If you notice, in the red line, there is an unencrypted hop. That final node, known as the exit node, has to decrypt your traffic to deliver it to a web server that doesn't speak Tor. This is where bad actors can prey on the chain of trust, either breaking into these exit nodes to spy, or even setting up their own exit nodes explicitly to spy.


Facebook - Log In or Sign Up
Facebook, Inc. (US)
https://www.facebookcorewwwi.onion/
facebook

This is a real vanity domain name. These can’t be bought, they can only be earned. These URLs are the hash result of a public key, so you have to generate the public keys, and then generate the hash, and then sort.

There Can Be Only One

- DigiCert
  - Only game in town, currently



September 11, 2015 by Jeremy Rowley+

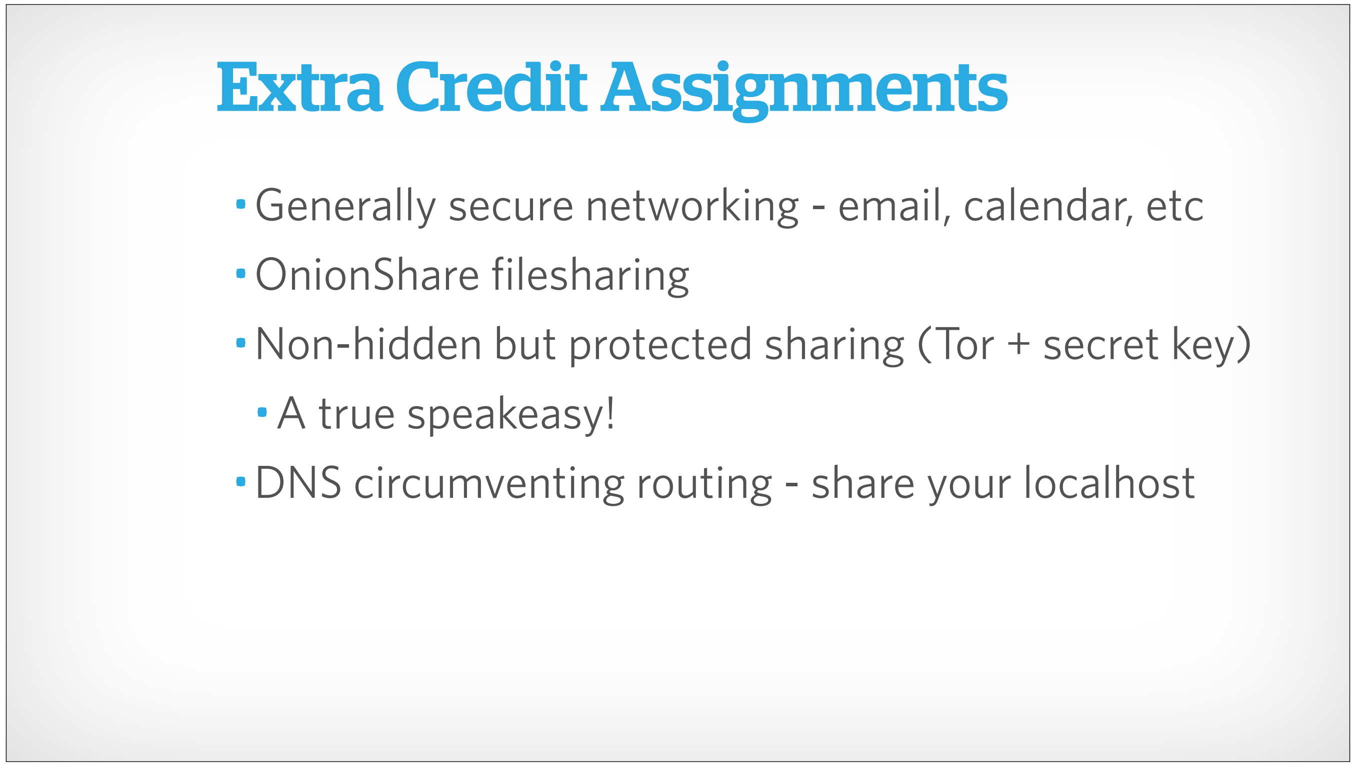
Posted Under: Browser, Encryption, News

.Onion Officially Recognized as Special-Use Domain

.Onion now classified as a special-use, top-level domain by Internet Engineering Steering Group (IESG).

There Can Be Only One

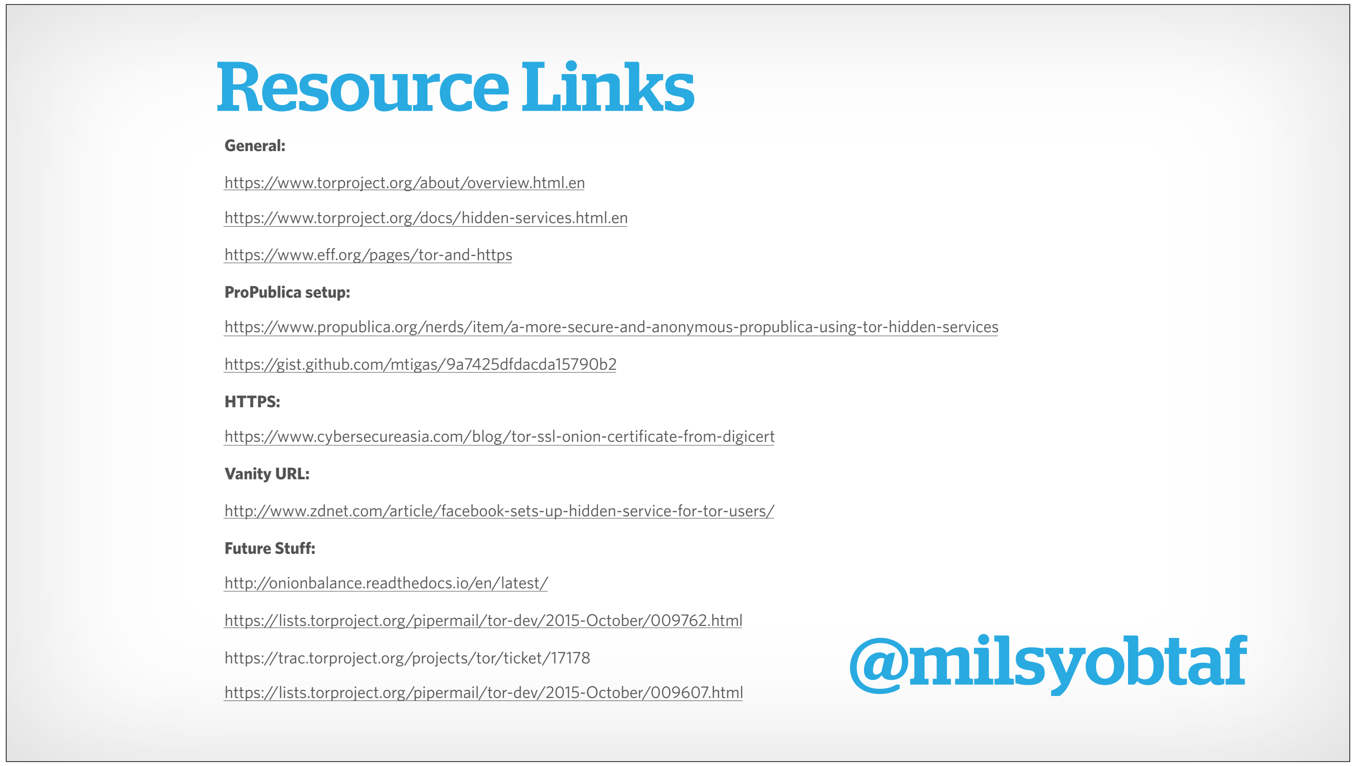
- DigiCert
  - Only game in town, currently
  - Working to standardize .onion as a TLD



Extra Credit Assignments

- Generally secure networking - email, calendar, etc
- OnionShare filesharing
- Non-hidden but protected sharing (Tor + secret key)
  - A true speakeasy!
- DNS circumventing routing - share your localhost

Setup secure tunnels between your mail and yourself
Sharing files easily and securely
Like an address plus a password, a true speakeasy
Unlike traditional HTTP, Tor is bidirectional by default, so you can bypass DNS limitations



Resource Links

General:

https://www.torproject.org/about/overview.html.en

https://www.torproject.org/docs/hidden-services.html.en

https://www.eff.org/pages/tor-and-https

ProPublica setup:

https://www.propublica.org/nerds/item/a-more-secure-and-anonymous-propublica-using-tor-hidden-services

https://gist.github.com/mtigas/9a7425dfdacda15790b2

HTTPS:

https://www.cybersecureasia.com/blog/tor-ssl-onion-certificate-from-digicert

Vanity URL:

http://www.zdnet.com/article/facebook-sets-up-hidden-service-for-tor-users/

Future Stuff:

http://onionbalance.readthedocs.io/en/latest/

https://lists.torproject.org/pipermail/tor-dev/2015-October/009762.html

https://trac.torproject.org/projects/tor/ticket/17178

https://lists.torproject.org/pipermail/tor-dev/2015-October/009607.html

@milsyobtaf

Don’t write these down!

Thanks!
Questions?

@milsyobtaf

https://github.com/milsyobtaf/prez