Security and Privacy for Activist Web Developers

Bill Budington
Developer at Radical Designs
https://github.com/hainish
@legind

Micah Lee
Web Developer at Electronic Frontier Foundation
https://github.com/micahflee
@micahflee

The Stack

The Stack

- Operating system
- Web and other services
- Web application
- Browser

Operating System Security

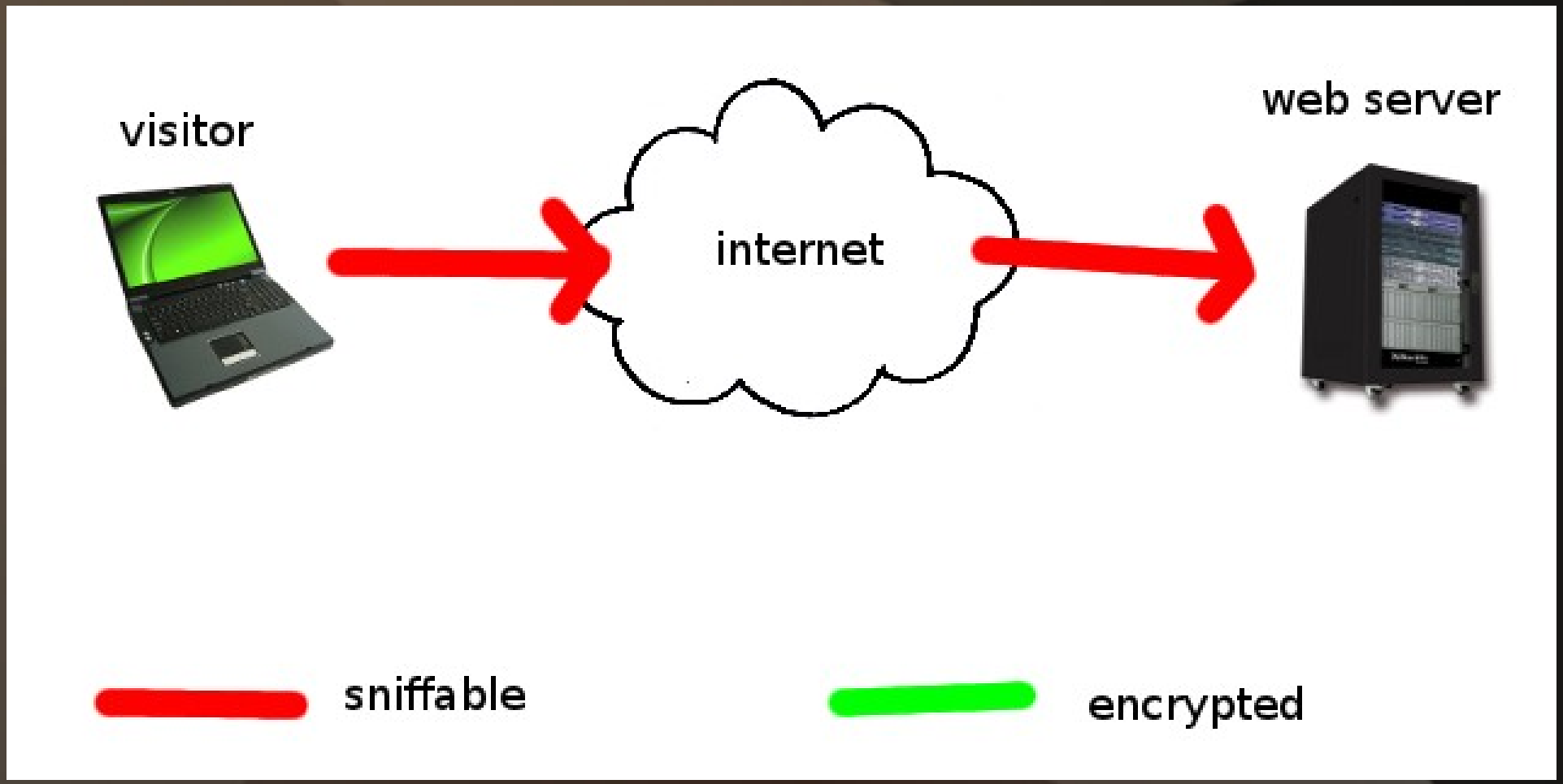
- This is assuming you have root on your web server
- Choose a Long-Term Support build
- Separate staging server
- Permissions
- Intrusion detection systems
- Monitoring software
- Helping Tor users access your site
- Port knocking

Intrusion Detection Systems

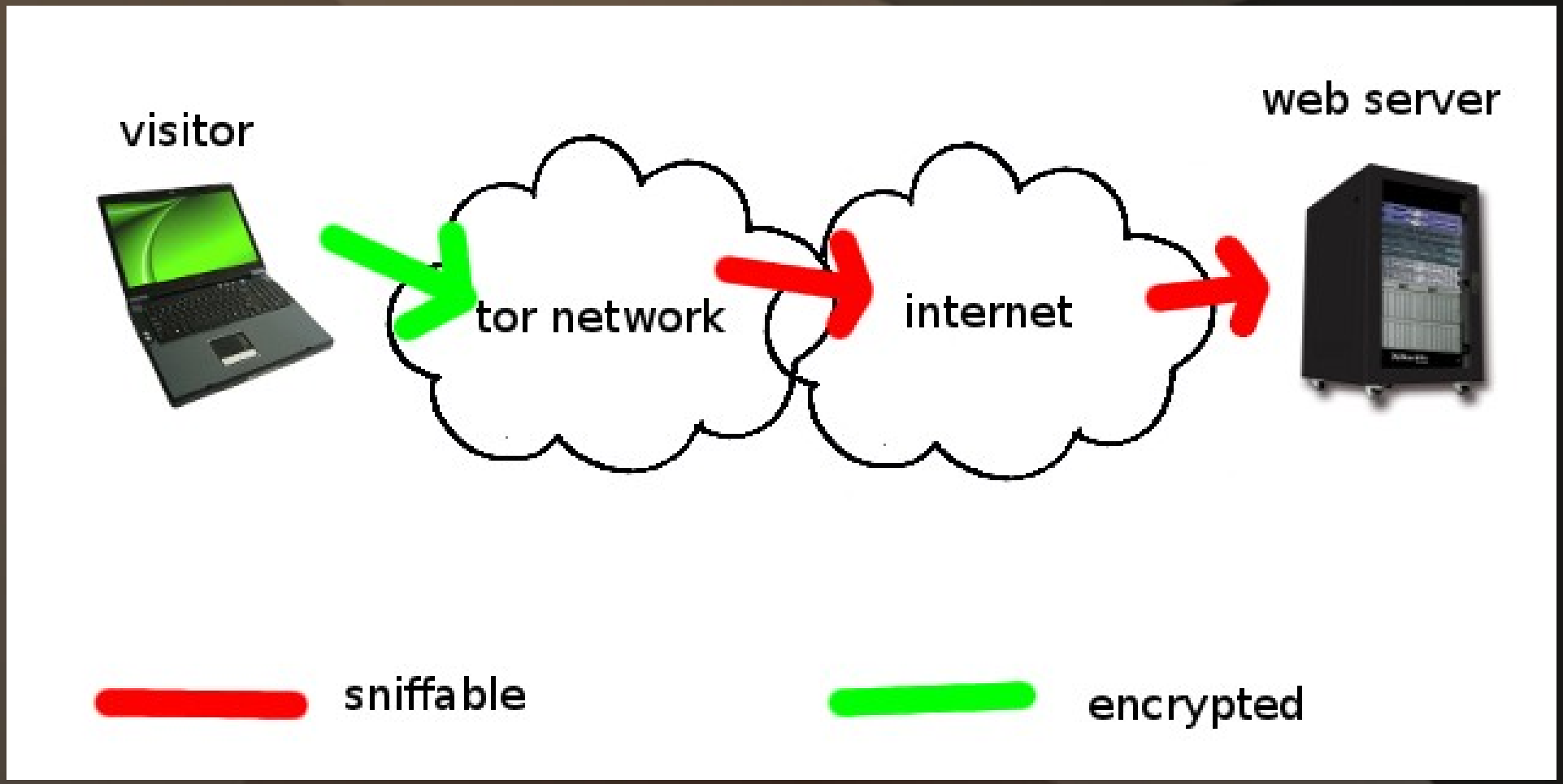
Intrusion Detection Systems

- Snort – packet-level IDS
- Rulesets – OinkMaster
- Updates
- Clients – Browser, Android
- Swinedroid: https://github.com/Hainish/Swinedroid
- Also: mod_security for Apache

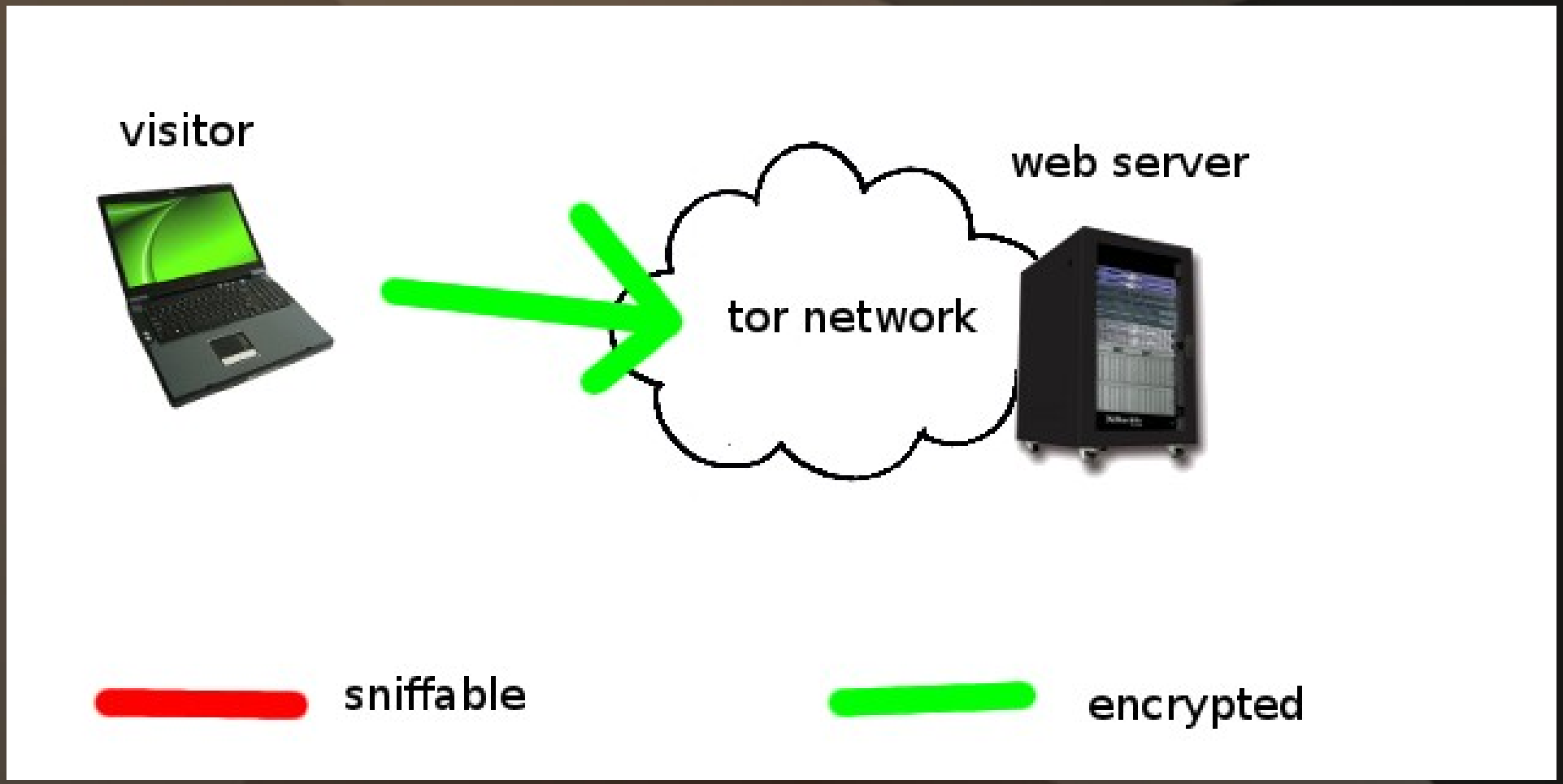
Using the web without Tor



Using the web with Tor



Accessing a Tor exit enclave website



Tor Exit Enclaves

Set an exit policy that only exits to your server

https://trac.torproject.org/projects/tor/wiki/doc/ExitEnclave

```
# what port to open for local application connections
SocksPort 9050
# accept connections only from localhost
SocksListenAddress 127.0.0.1
ORPort 9001
Nickname archivetpo
ExitPolicyRejectPrivate 0
ExitPolicy accept 38.229.70.19:443
ExitPolicy reject *:*
```

HTTPS

HTTPS

Here's how you force HTTPS from Apache config or .htaccess file:

```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
```

HTTP Strict Transport Security

- Tells modern browsers to only communicate to your server over HTTPS
- https://developer.mozilla.org/en/Security/HTTP_Strict_Transport_Security
- HTTPS responses should include this header:

```
Strict-Transport-Security: max-age=expireTime
[; includeSubdomains]
```

How to setup HSTS

In PHP:

```
if(!empty($_SERVER['HTTPS'])) {
    header(“Strict-Transport-Security: max-age=31536000; includeSubdomains”);
}
```

In Apache:

```
LoadModule headers_module modules/mod_headers.so
Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
```

Basic Authentication

- Have something on the internet that the public should never access?
- Built-in to the HTTP protocol
- Even if your web app has security holes, basic auth keeps the riff-raff out

Basic Authentication

Put this in your Apache config or .htaccess file:

```
AuthName "Are you allowed in?"
AuthType Basic
AuthUserFile /path/to/htpasswd
Require valid-user
AllowOverride All
```

Disable IP Address Logging in Apache

Here is Apache's default log format:

```
LogFormat "%h %l %u %t \"%r\" %>s %b" common
```

Make your own:

```
LogFormat "- %l %u %t \"%r\" %>s %b" noip
```

Then use it:

```
CustomLog /var/logs/apache2/access.log noip
```

Encrypt your IPs with cryptolog

I programmed it, still under development: https://git.eff.org/?p=cryptolog.git;a=summary

Makes this:

```
67.169.69.72 - - [12/May/2011:17:58:07 -0700]
"GET / HTTP/1.1" 200 430
```

Look like this:

```
UkezVh - - [12/May/2011:17:58:07 -0700] "GET /
HTTP/1.1" 200 430
```

Encrypt your IPs with cryptolog

git clone https://git.eff.org/public/cryptolog.git/

```
CustomLog "| /usr/bin/cryptolog -w
/root/cryptolog-access.log" common
```

```
CustomLog "| /usr/bin/cryptolog -c
/usr/bin/cronolog\\\ /root/cryptolog-access-%Y-
%m-%d.log" common
```

Encrypt your IPs with mod_log_iphash

- https://github.com/franzs/mod_log_iphash
- Uses hash function to turn your IPv4 address into a fake IPv6 address
- Can run AWStats against your logs
- Apache Module

```
LogFormat "%Z %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" iphash

CustomLog /var/log/httpd-access.log iphash
```

Encrypt your IPs with mod_log_iphash

- Error logs are not configurable in apache
- Not logging errors

```
ErrorLog /dev/null
```

- Iphash provides Apache patch
- Scrub logs often

Remote Administration

- Public key authentication is better than password authentication
- Logging in from an untrusted machine? Use barada!
- Use SSH or SFTP to transfer files
- **Never use FTP! It is old an insecure.**

#FTP Protest

Hide details from PHP with $_SERVER

- In Wordpress, add to wp-config.php
- In Drupal, add to sites/default/settings.php

```
$_SERVER['HTTP_REFERER'] = 'https://web/';
$_SERVER['HTTP_USER_AGENT'] = 'web browser';
$_SERVER['REMOTE_ADDR'] = '127.0.0.1';
$_SERVER['REMOTE_HOST'] = 'localhost';
```

What's in an HTTP request header?

When your browser makes an HTTP request, it tells the website:

- Your IP address
- Your user agent string (web browser, operating system, processor architecture, preferred language, etc.)
- Referer string (where you came from)
- Cookies

Third Party Scripts

When do you give this information to third parties?

- Facebook like buttons
- Twitter widgets
- Google Analytics
- Embedded YouTube videos
- Any <script>, <img>, etc. tag that loads something from a remote server

https://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy

Third Party Scripts

Use plain HTML links as share buttons

```
https://twitter.com/home?
status=PUT_TWITTER_STATUS_HERE

https://www.facebook.com/share.php?
u=PUT_URL_HERE

https://identi.ca/notice/new?
status_textarea=PUT_IDENTI_CA_STATUS_
HERE

http://sharetodiaspora.github.com/?
title=PUT_TITLE_HERE&url=PUT_URL_HERE
```

Load your Twitter feed from the server, not the client

How do you access the feed?

- Twitter API: **`https://dev.twitter.com/`**
- JSON URL to Twitter feed: **`https://twitter.com/statuses/user_timeline/michaflee.json`**

Example websites that do this:

- **`https://www.eff.org/`**
- **`https://globalchokepoints.org/`**

Let users “opt-in” before including third-party scripts

- Use text or image placeholder with Javascript click handler to include embed code

Examples:

- https://eff.org/issues/bloggers-under-fire

MyTube drupal module:
https://drupal.org/project/mytube

Let users “opt-in” before including third-party scripts

- Use text or image placeholder with Javascript click handler to include embed code

Examples:

- https://eff.org/issues/bloggers-under-fire

MyTube drupal module:
https://drupal.org/project/mytube

Web Development Tools

- **Firebug**
  https://getfirebug.com/
- **Live HTTP Headers**
  http://livehttpheaders.mozdev.org/
- **Tamper Data**
  https://addons.mozilla.org/en-US/firefox/addon/tamper-data/
- **Ghostery**
  http://www.ghostery.com/

Thank you!

Bill Budington - @legind

bill@inputoutput.io

https://github.com/hainish

Micah Lee - @micahflee

micahflee@riseup.net

https://github.com/micahflee