

10. Web Security & Privacy

Blase Ur

May 2nd, 2019

CMSC 23210 / 33210



THE UNIVERSITY OF
CHICAGO



Security, Usability, & Privacy
Education & Research

Trust on the web

Overview

- Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS) enable secure communication
- Frequently encountered with web browsing (HTTPS) and more behind the scenes in app, VOIP, etc.

What we want to defend against

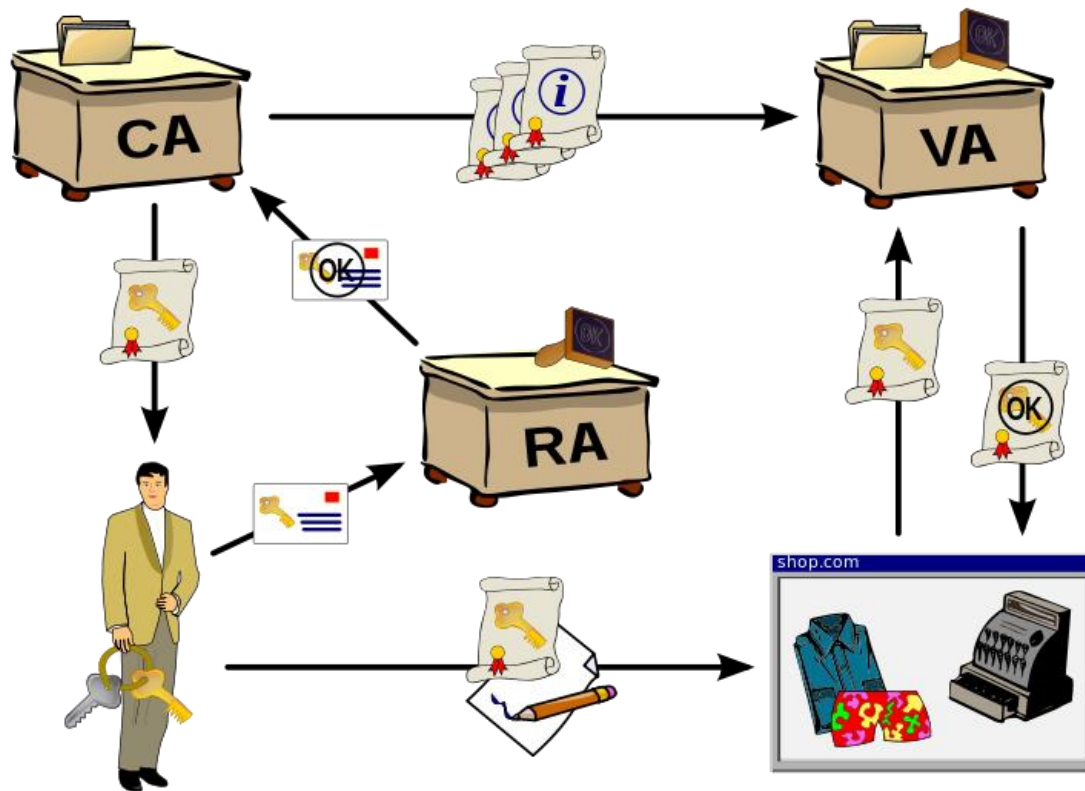
- People snooping on our communications
 - The contents of what we're sending
 - Session tokens (see, e.g., Firesheep)
- Man-in-the-middle attacks
 - We want to authenticate that we are talking to the right site, not an imposter
 - Use certificates inside a public-key infrastructure

How we could obtain trust

- Web of trust
 - People you already trust introduce you to people they trust
 - Can get complicated, doesn't scale well
 - Infrequently seen in practice
- Public-Key Infrastructure (PKI)
 - Certificates are issued by certificate authorities that bind cryptographic keys to identities

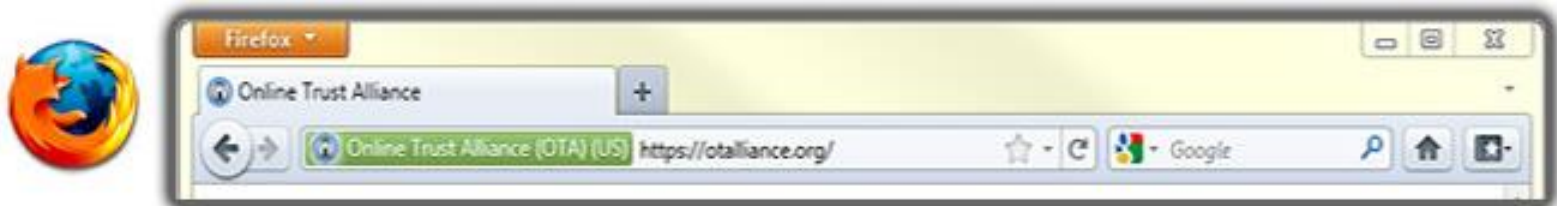
Public-Key Infrastructure

- Binding of keys to identities



















































What does SSL look like to users?

- Compare, e.g., the following:
 - <https://www.google.com> (normal certificate)
 - Go to Google images and then click on an image and see what happens (mixed content)
 - <https://www.thawte.com> (EV certificate)



What does SSL look like to users?

Browser	HTTPS	HTTPS minor error	HTTPS major error	HTTP	EV	Malware
Chrome 48 Win	 https://www	 https://mixe	 https://wro	 www.exami	 Symantec Co	 https://dow
Edge 20 Win	 example.	 https://mix	 wrong.host.bads	 example.com	 Symantec Co	 Unsafe website der
Firefox 44 Win	 https://www.e	 https://mixec	 https://expire	 www.example	 Symantec Corpo	 https://spacet
Safari 9 Mac	 example.com	 mixed.badssl.o	<i>URL hidden</i>	 example.com	 Symantec Cor	 downloadgam
Chrome 48 And	 https://v	 https://mixe	 https://v	 www.examp	 https://v	 https://spac
Opera Mini 14 And	 www.exami	 mixed.badssl.c	 wrong.host.ba	 www.example	 www.syma	<i>Unavailable</i>
UC Mini 10 And	 Example D	 mixed.bads	<i>Blocked</i>	 Example D	 Endpoint, C	<i>Blocked</i>
UC Browser 2 iOS	 Example Do.	 mixed.bads..	 wrong.host..	 Example Do.	 Endpoint, C.	<i>Unavailable</i>
Safari 9 iOS	 example.c	 mixed.badss	 wrong.host	 example.com	 Symantec	<i>Unavailable</i>

(From Felt et al. SOUPS 2016)

How does PKI look to browsers?

- Hundreds of trusted certificate authorities
 - Certificate authorities (CAs) sign the certificates binding identities to keys
 - See, e.g., Firefox's advanced settings

How does PKI look to site admins?

- Apply for a certificate
 - Validation process
 - Certificate authorities (CAs) delegate trust (“chain of trust”)
 - CAs sell you a certificate

Issues with SSL/TLS/PKIs

- Implementation issues
- Communicating to users what is happening
- Compromised Certificate Authorities
- Man-in-the-middle attacks
 - Downgrade/dumbing-down attacks
 - Addition of “rogue” certificates
- Revocation
- Timing attacks and other side channels

Compromised CAs

- Comodo and Diginotar both suffered breaches in 2011 that let attackers issue rogue certificates
- What about untrustworthy CAs?
 - Compelled certificate creation attacks (see, e.g., Soghoian and Stamm FC '11)

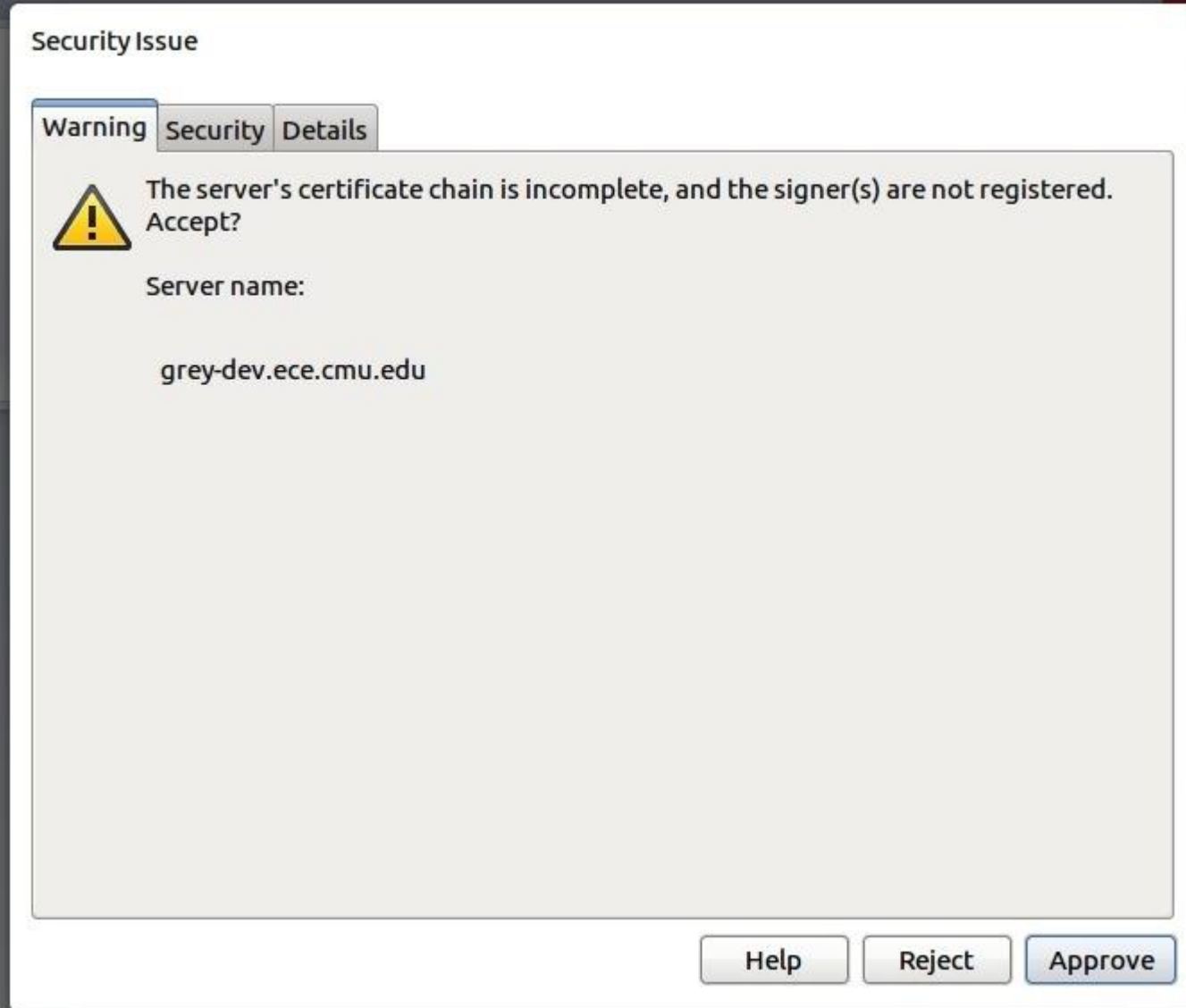
Man-in-the-middle attacks (MITM)

- Effectively, many corporations perform MITM attacks by adding certificates to users' computers and presenting “fake” certificates to users.
- A man in the middle can also tell you a site doesn't support SSL/TLS (downgrade) or any strong ciphers (dumbing down)
 - Why does this create a huge problem?
 - Why is this hard to deal with?

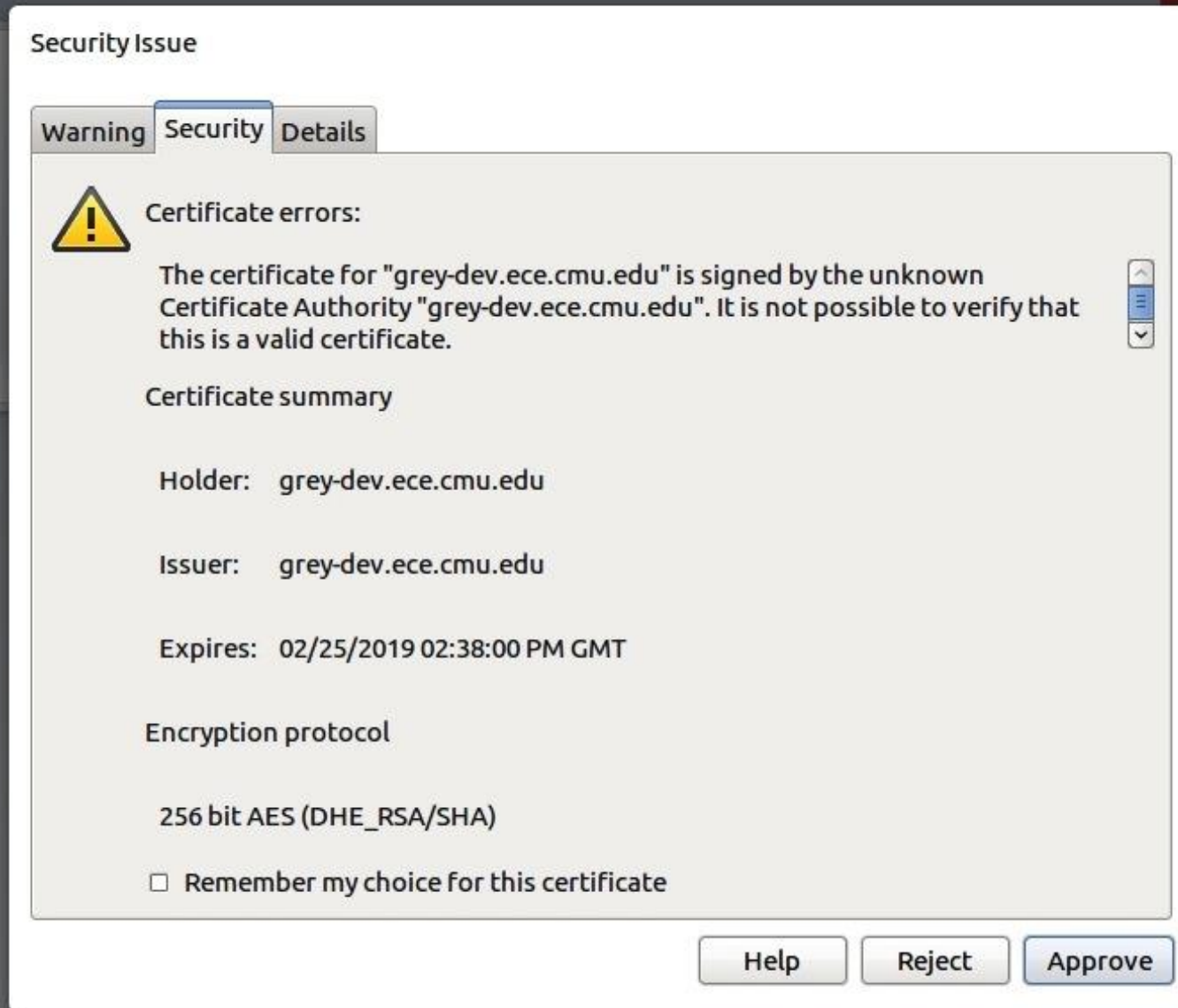
Warnings



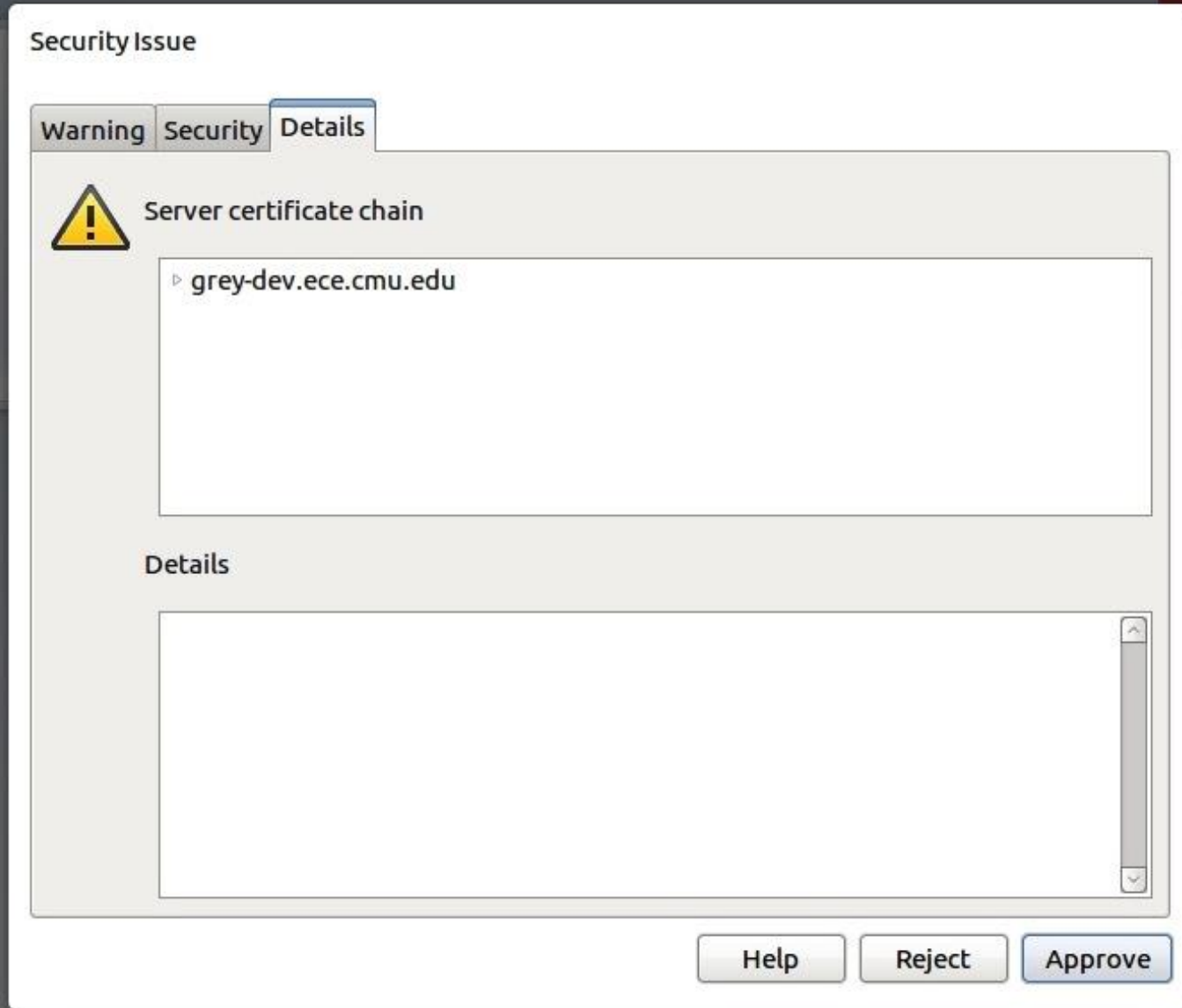
Opera



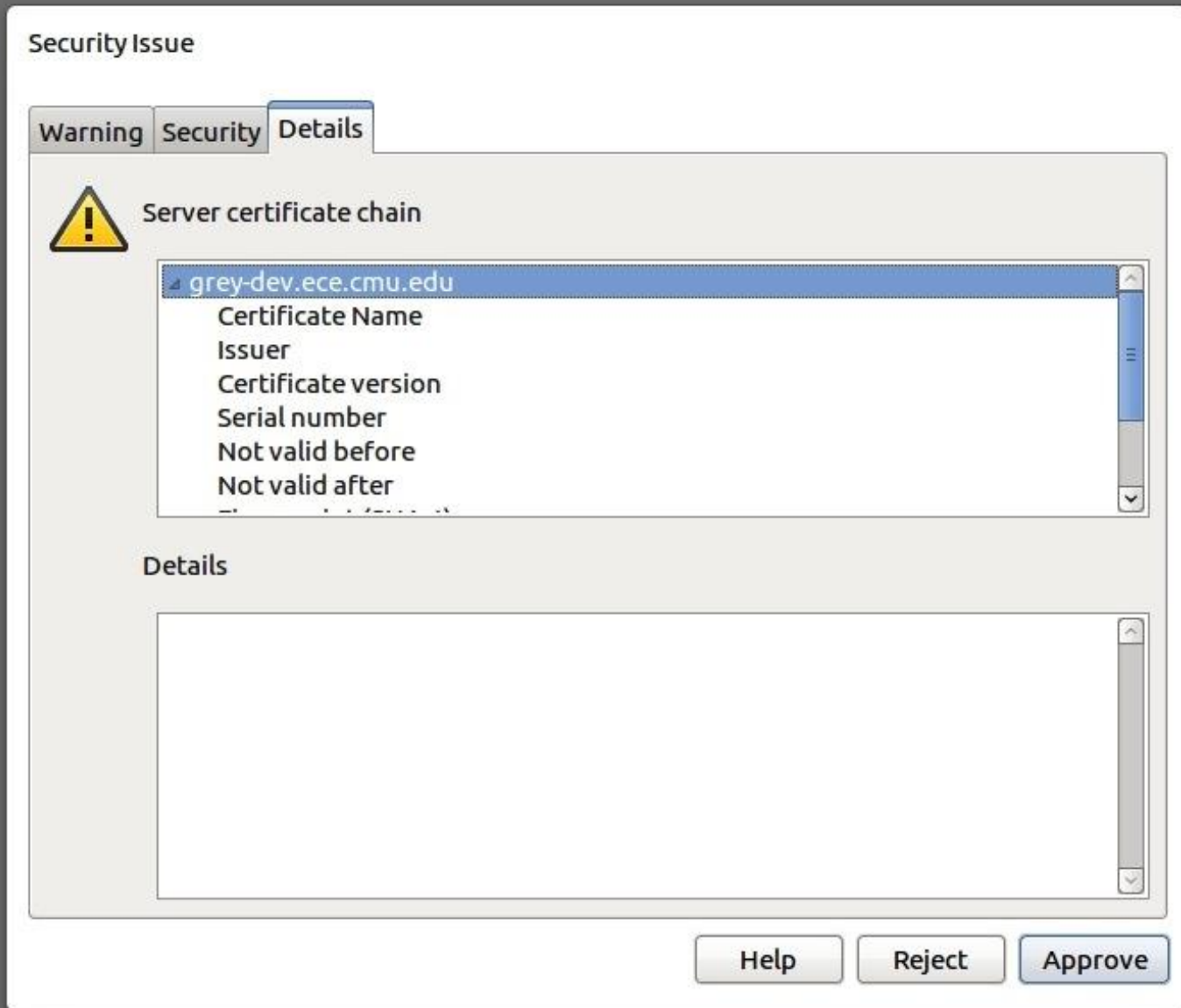
Opera



Opera



Opera



Chromium



The site's security certificate is not trusted!

You attempted to reach **grey-dev.ece.cmu.edu**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chromium cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.

Proceed anyway

Back to safety

▶ [Help me understand](#)

Chromium



You attempted to reach **grey-dev.ece.cmu.edu**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chromium cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.

Proceed anyway

Back to safety

▼ [Help me understand](#)

When you connect to a secure website, the server hosting that site presents your browser with something called a "certificate" to verify its identity. This certificate contains identity information, such as the address of the website, which is verified by a third party that your computer trusts. By checking that the address in the certificate matches the address of the website, it is possible to verify that you are securely communicating with the website you intended, and not a third party (such as an attacker on your network).

In this case, the certificate has not been verified by a third party that your computer trusts. Anyone can create a certificate claiming to be whatever website they choose, which is why it must be verified by a trusted third party. Without that verification, the identity information in the certificate is meaningless. It is therefore not possible to verify that you are communicating with **grey-dev.ece.cmu.edu** instead of an attacker who generated his own certificate claiming to be **grey-dev.ece.cmu.edu**. You should not proceed past this point.

If, however, you work in an organization that generates its own certificates, and you are trying to connect to an internal website of that organization using such a certificate, you may be able to solve this problem securely. You can import your organization's root certificate as a "root certificate", and then certificates issued or verified by your organization will be trusted and you will not see this error next time you try to connect to an internal website. Contact your organization's help staff for assistance in adding a new root certificate to your computer.

Mozilla Firefox



This Connection is Untrusted

You have asked Firefox to connect securely to **grey-dev.ece.cmu.edu**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

- ▶ **Technical Details**
- ▶ **I Understand the Risks**

Mozilla Firefox



You have asked Firefox to connect securely to **grey-dev.ece.cmu.edu**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

▼ Technical Details

grey-dev.ece.cmu.edu uses an invalid security certificate.

The certificate is not trusted because it is self-signed.

(Error code: sec_error_untrusted_issuer)

▼ I Understand the Risks

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

Add Exception...

Deploying certs more widely

- EFF's Let's Encrypt
 - <https://letsencrypt.org/>

Online tracking

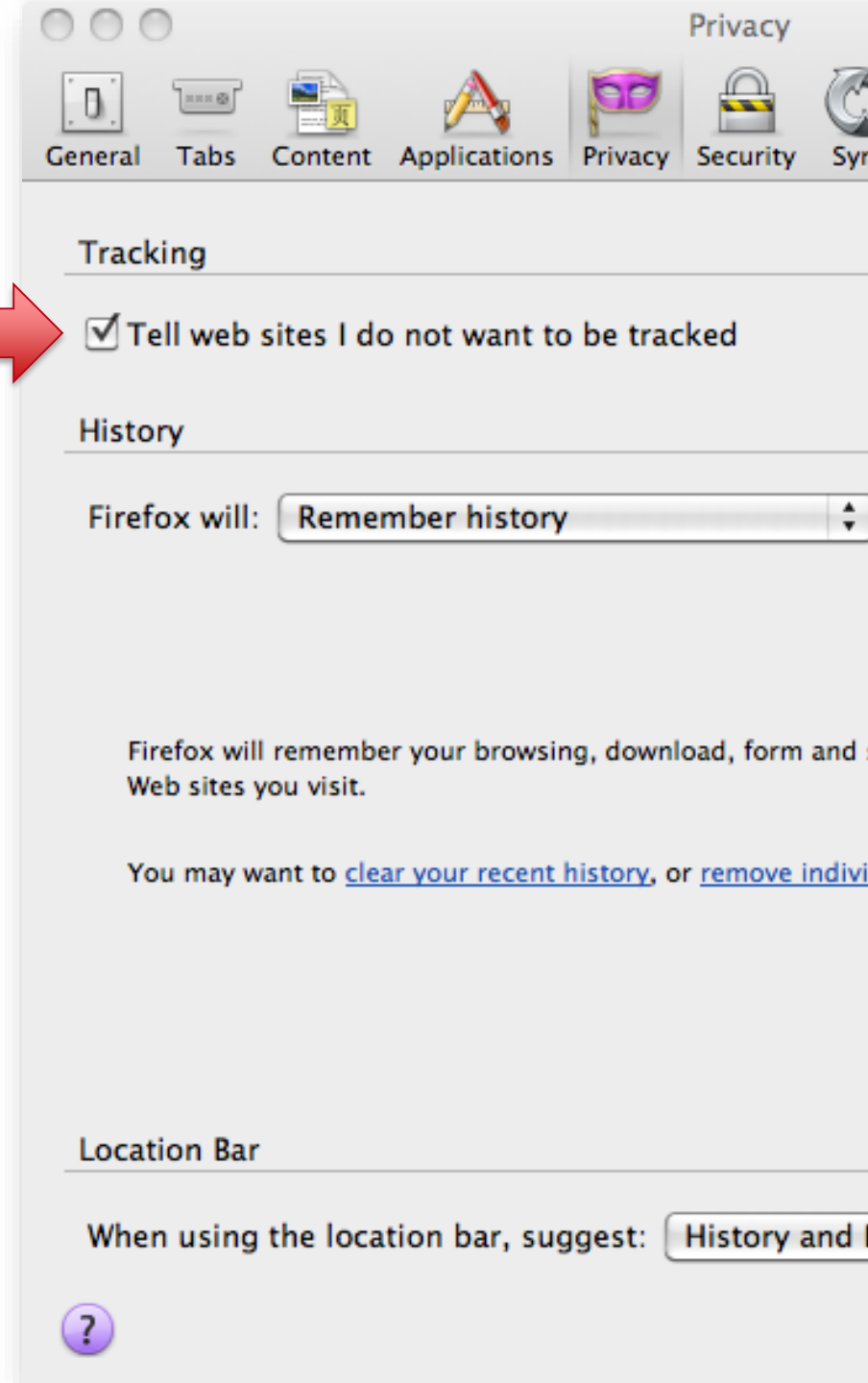
Online Tracking

- First party = the site you are visiting (whose address is in the URL bar)
- Third party = other sites contacted as a result of your visit to that site
- First-party tracking (e.g., for search)
 - Consider DuckDuckGo and alternatives

Online Behavioral Advertising (OBA)

Do not track

- Proposed W3C standard
- User checks a box
- Browser sends “do not track” header to website
- Website stops “tracking”
- W3C working group trying to define what that means



Tools to stop tracking, effective?

- Browser privacy settings
 - Cookie blocking
 - P3P
 - Tracking Protection Lists
 - Do Not Track
- Browser add-ons
- Opt-out cookies
- Digital Advertising Alliance (DAA) AdChoices icon and associated opt-out pages



DoNotTrackMe



Existing Privacy Tools

The Disconnect browser extension interface is shown. It features a top bar with the 'DISCONNECT' logo, 'Help', and 'Share' links. Below this is a social media section with icons for Facebook (0), Google+ (1), and Twitter (1). The main content area is divided into categories: Advertising (2 requests), Analytics (7 requests), Social (0 requests), and Content (0 requests). Each category has a list of blocked trackers with checkboxes and request counts. At the bottom, there are options to 'Whitelist site', 'Visualize page', 'Show counter', and 'Cap counter'. A bar chart shows 'Time saved' and 'Bandwidth saved'. A green button at the bottom says 'Get Mobile Protection'.

DISCONNECT Help Share

f 0 g 1 t 1

Advertising
2 requests

- ✓ Adobe 1 request
- ✓ Nielsen 1 request

Analytics
7 requests

Social
0 requests

Content
0 requests

☰ Whitelist site Visualize page

✓ Show counter ✓ Cap counter

Time saved Bandwidth saved

Get Mobile Protection

The Blur browser extension interface is shown on the ESPN website. It features a top bar with the 'espn.com' logo and '8 trackers blocked'. Below this is a section for 'Tracker blocking is on for this website'. A list of blocked trackers is shown: Google AdSense, Demdex, Twitter Badge, and Omniture, each with a 'blocked' status and a green checkmark. A link says 'see your tracker blocking stats and learn more about these companies'. A blue bar at the bottom says '21 trackers blocked since Feb '17'. Below this is a link 'Correct how Blur works in the form below'. The bottom of the interface shows the 'oBLUR' logo and links for 'Settings', 'Help', and 'Go Premium'.

Final Final

espn.com X
8 trackers blocked

Tracker blocking is **on** for this website

Google AdSense blocked ✓
Demdex blocked ✓
Twitter Badge blocked ✓
Omniture blocked ✓

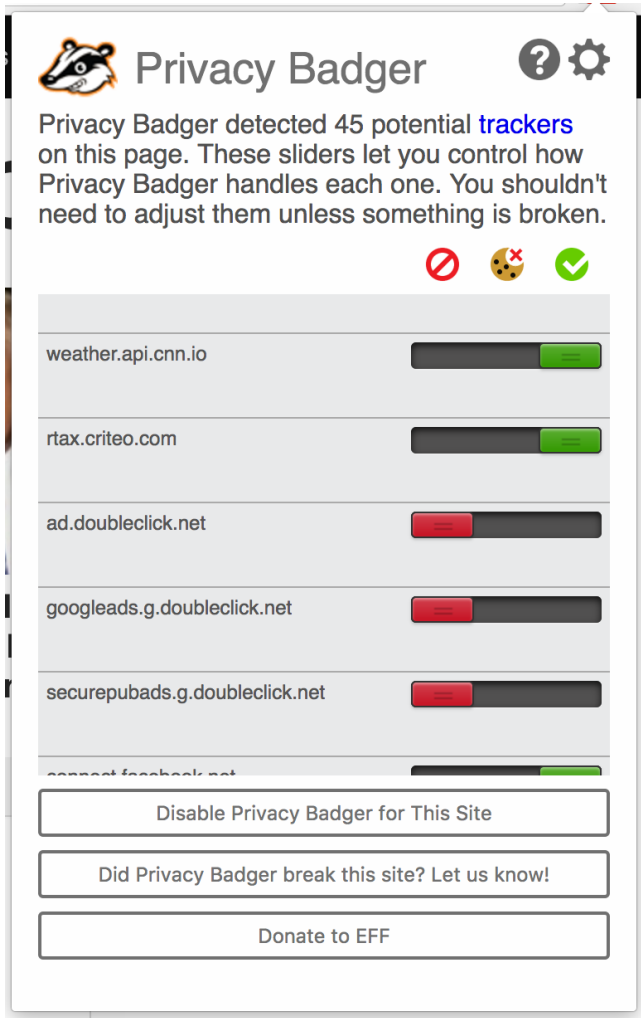
[see your tracker blocking stats and learn more about these companies](#)

21 trackers blocked since Feb '17

[Correct how Blur works in the form below](#)

oBLUR [Settings](#) [Help](#) [Go Premium](#)

Existing Privacy Tools



Privacy Badger

Privacy Badger detected 45 potential **trackers** on this page. These sliders let you control how Privacy Badger handles each one. You shouldn't need to adjust them unless something is broken.

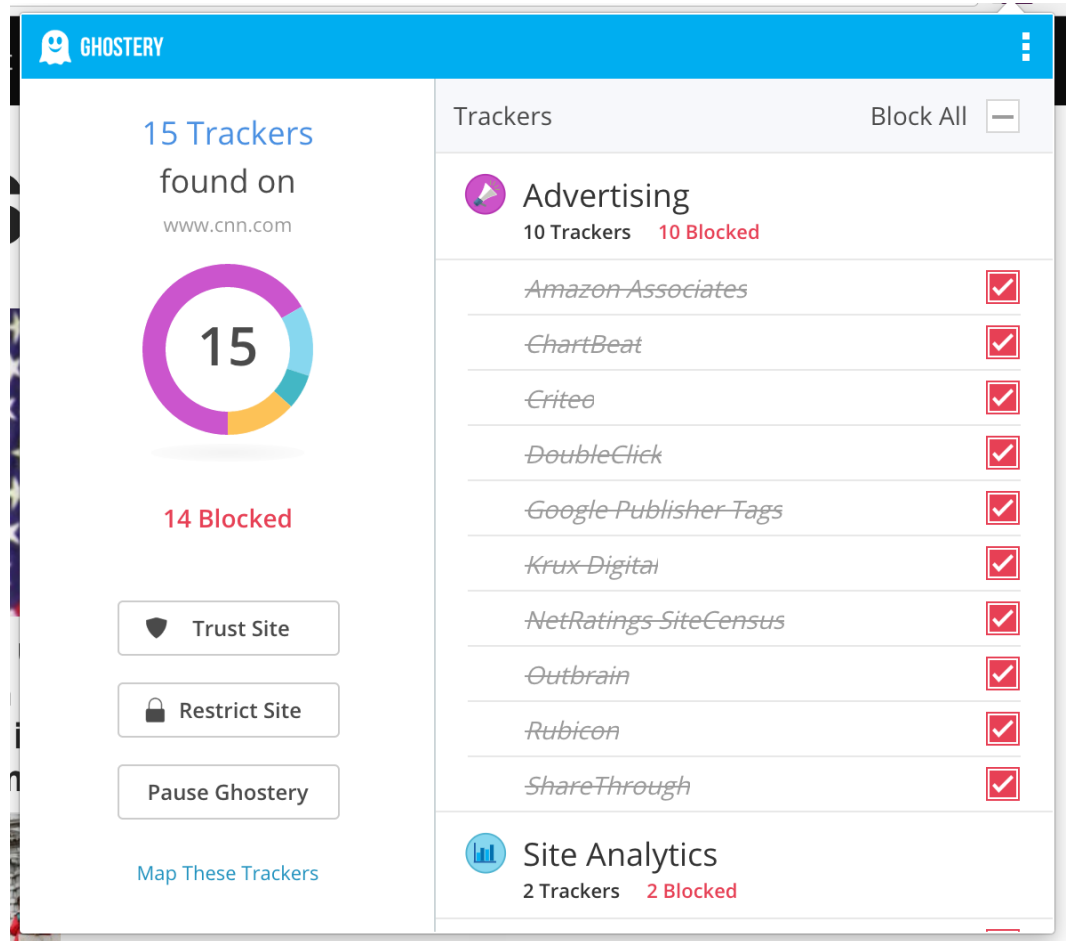
🚫 🍪 ✖️ ✅

Tracker	Control
weather.api.cnn.io	<input type="checkbox"/>
rtax.criteo.com	<input type="checkbox"/>
ad.doubleclick.net	<input type="checkbox"/>
googleads.g.doubleclick.net	<input type="checkbox"/>
securepubads.g.doubleclick.net	<input type="checkbox"/>
connect.facebook.net	<input type="checkbox"/>

Disable Privacy Badger for This Site

Did Privacy Badger break this site? Let us know!

Donate to EFF



GHOSTERY

15 Trackers found on www.cnn.com

15

14 Blocked

Trust Site

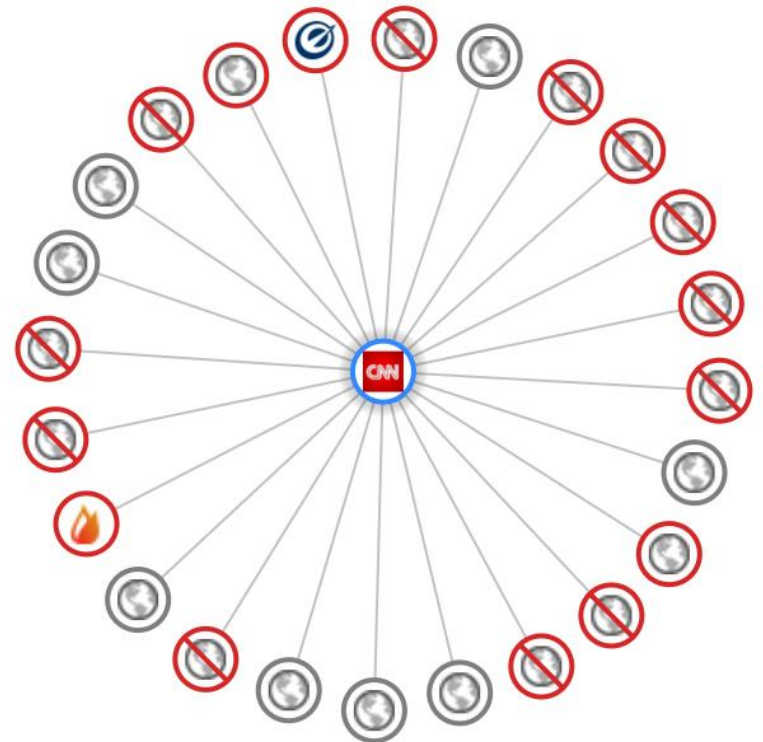
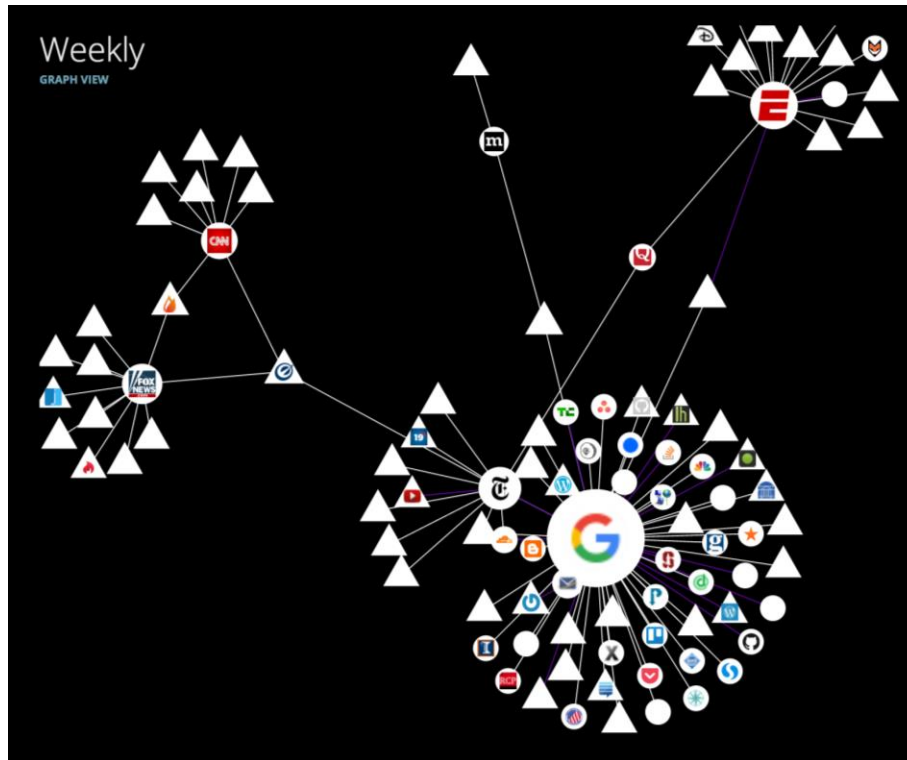
Restrict Site

Pause Ghostery

[Map These Trackers](#)

Trackers	Block All
Advertising 10 Trackers 10 Blocked	<input type="checkbox"/>
Amazon Associates	<input checked="" type="checkbox"/>
ChartBeat	<input checked="" type="checkbox"/>
Criteo	<input checked="" type="checkbox"/>
DoubleClick	<input checked="" type="checkbox"/>
Google Publisher Tags	<input checked="" type="checkbox"/>
Krux Digital	<input checked="" type="checkbox"/>
NetRatings SiteCensus	<input checked="" type="checkbox"/>
Outbrain	<input checked="" type="checkbox"/>
Rubicon	<input checked="" type="checkbox"/>
ShareThrough	<input checked="" type="checkbox"/>
Site Analytics 2 Trackers 2 Blocked	<input type="checkbox"/>

Existing Tools' Connection Graphs



Browser fingerprinting

- Use features of the browser that are relatively unique to your machine
 - Fonts
 - GPU model anti-aliasing (Canvas fingerprinting)
 - User-agent string
 - *(Often not)* IP address *(Why not?)*

Browser fingerprinting

- <https://panopticklick.eff.org/>

Private browsing

Private Browsing



Private Browsing with Tracking Protection

When you browse in a Private Window, Firefox does not save:

- visited pages
- cookies
- searches
- temporary files

Firefox will save your:

- bookmarks
- downloads

Private Browsing doesn't make you anonymous on the Internet. Your employer or Internet service provider can still know what page you visit.



Tracking Protection ☒

Some websites use trackers that can monitor your activity across the Internet. With Tracking Protection Firefox will block many trackers that can collect information about your browsing behavior.

[See how it works](#)

Learn more about [Private Browsing](#).

Private Browsing



You've gone incognito

Pages you view in incognito tabs won't stick around in your browser's history, cookie store, or search history after you've closed all of your incognito tabs. Any files you download or bookmarks you create will be kept.

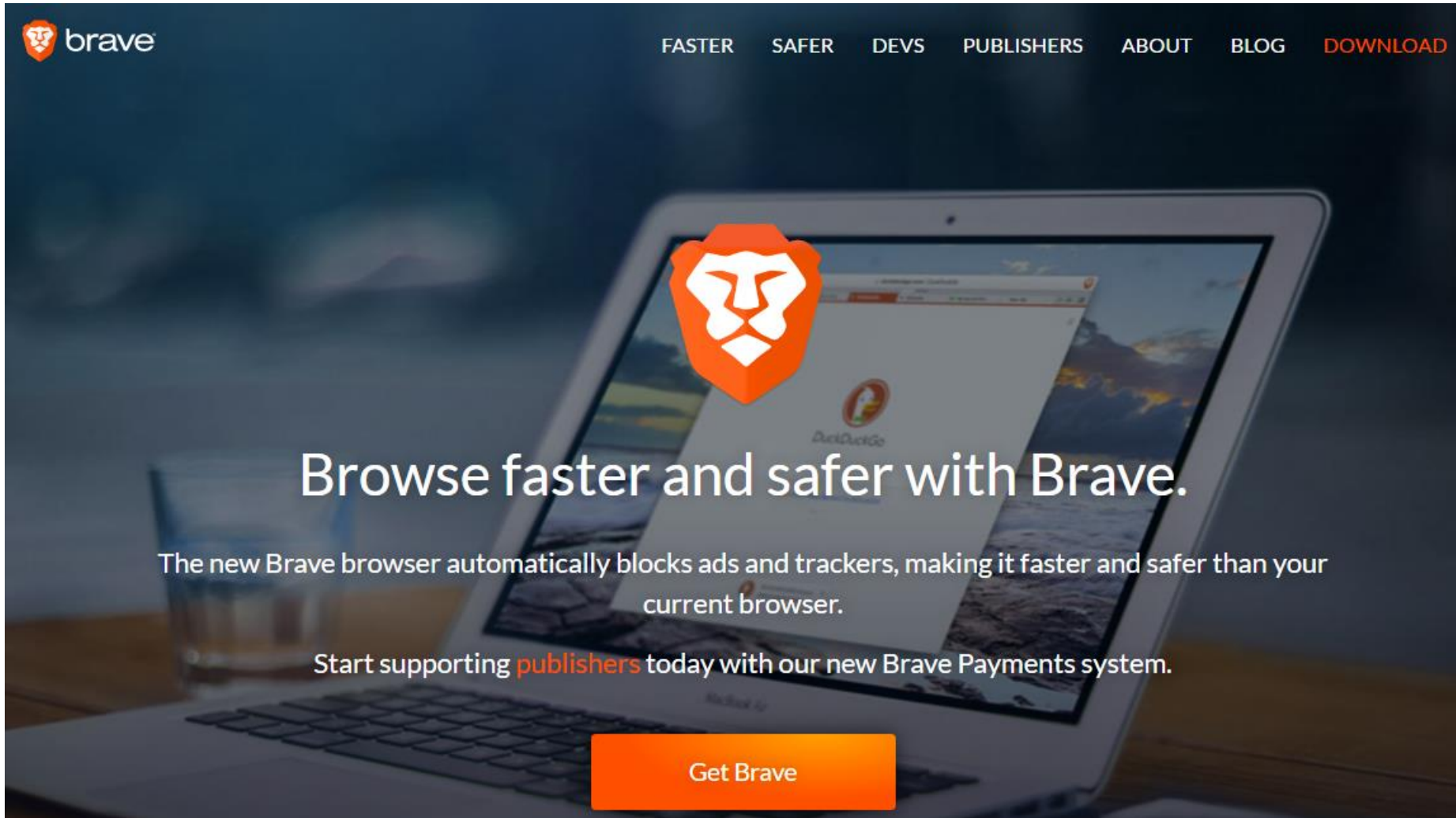
However, you aren't invisible. Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit.

[LEARN MORE](#)

NoScript



Brave

The image shows the Brave browser homepage. At the top left is the Brave logo, which consists of an orange shield with a white lion's head inside, followed by the word "brave" in a lowercase, sans-serif font. To the right of the logo is a navigation menu with the following links: "FASTER", "SAFER", "DEVS", "PUBLISHERS", "ABOUT", "BLOG", and "DOWNLOAD" (which is highlighted in orange). The background of the page is a dark, blurred image of a laptop on a desk with a glass of water. Overlaid on the laptop screen is a large, semi-transparent orange shield with a white lion's head, which is the Brave logo. Below the logo, the text "Browse faster and safer with Brave." is displayed in a large, white, sans-serif font. Underneath this, a smaller line of text reads: "The new Brave browser automatically blocks ads and trackers, making it faster and safer than your current browser." Further down, another line of text says: "Start supporting publishers today with our new Brave Payments system." At the bottom center, there is a large, orange, rounded rectangular button with the text "Get Brave" in white, sans-serif font.