23- SSL, PKIs, and Secure Communication

Lorrie Cranor

April 12, 2017

05-436 / 05-836 / 08-534 / 08-734 / 19-534 / 19-734
Usable Privacy and Security

Carnegie Mellon University
CyLab

institute for SOFTWARE RESEARCH

Engineering & Public Policy

Today!

- SSL/TLS
- Comparing crypto key fingerprints

SSL

- 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 does SSL defend against?

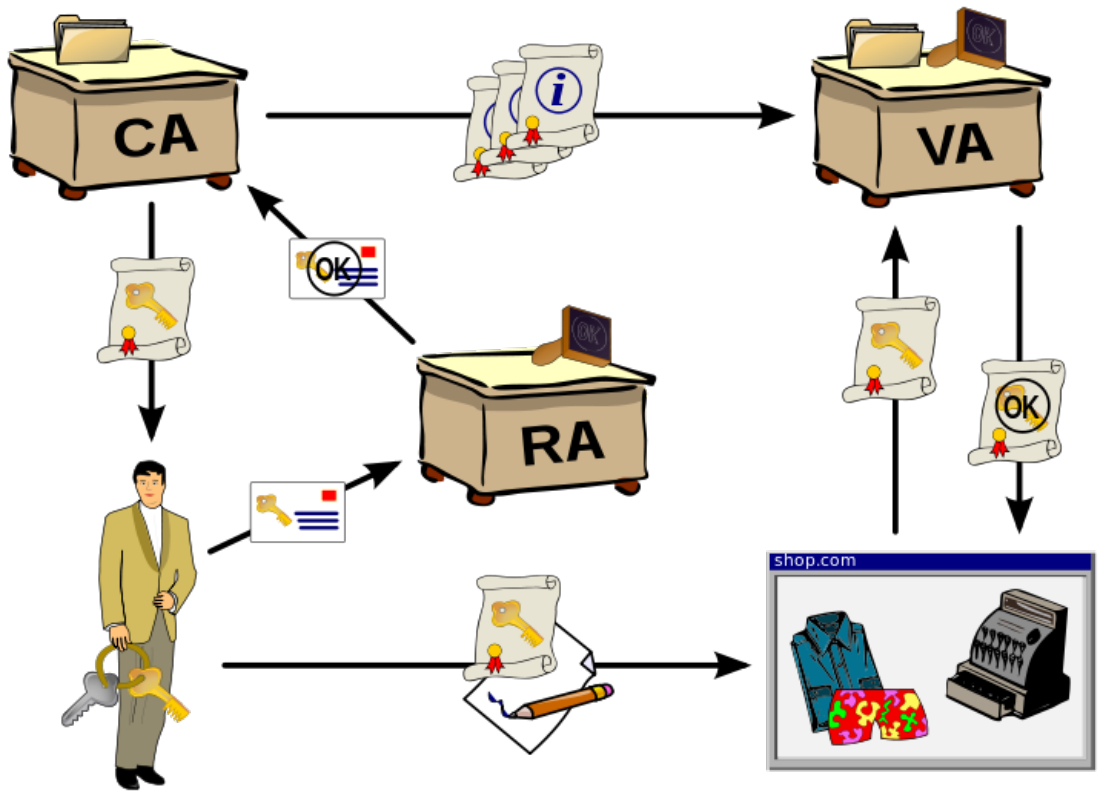
- People snooping on our communications
  - The contents of what we're sending
  - Session tokens (see, e.g., Firesheep)
- Man-in-the-middle attacks
  - An imposter who pretends to be the website we think we're talking to and intercepts our communications to eavesdrop on them, or possibly change them

How do we know whether to trust a certificate?

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

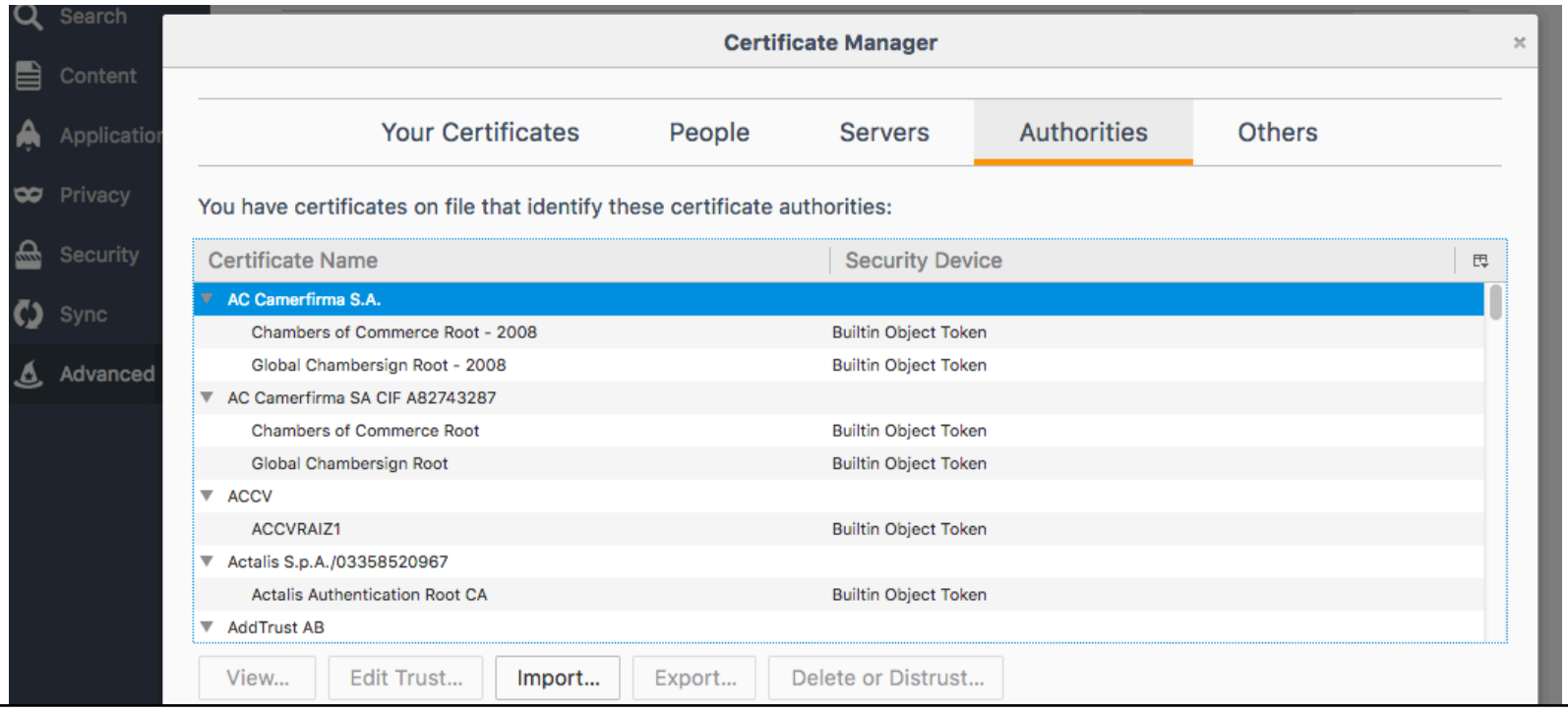
Public-Key Infrastructure

- Binding of keys to identities can be done automatically or by humans



What does PKI look like to browsers?

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



What does PKI look like to sites?

- 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

What does SSL look like?

- Depends on the browser
- Browsers may distinguish between
  - No SSL
  - Regular SSL cert
  - Extended validation (EV) cert
  - Mixed content

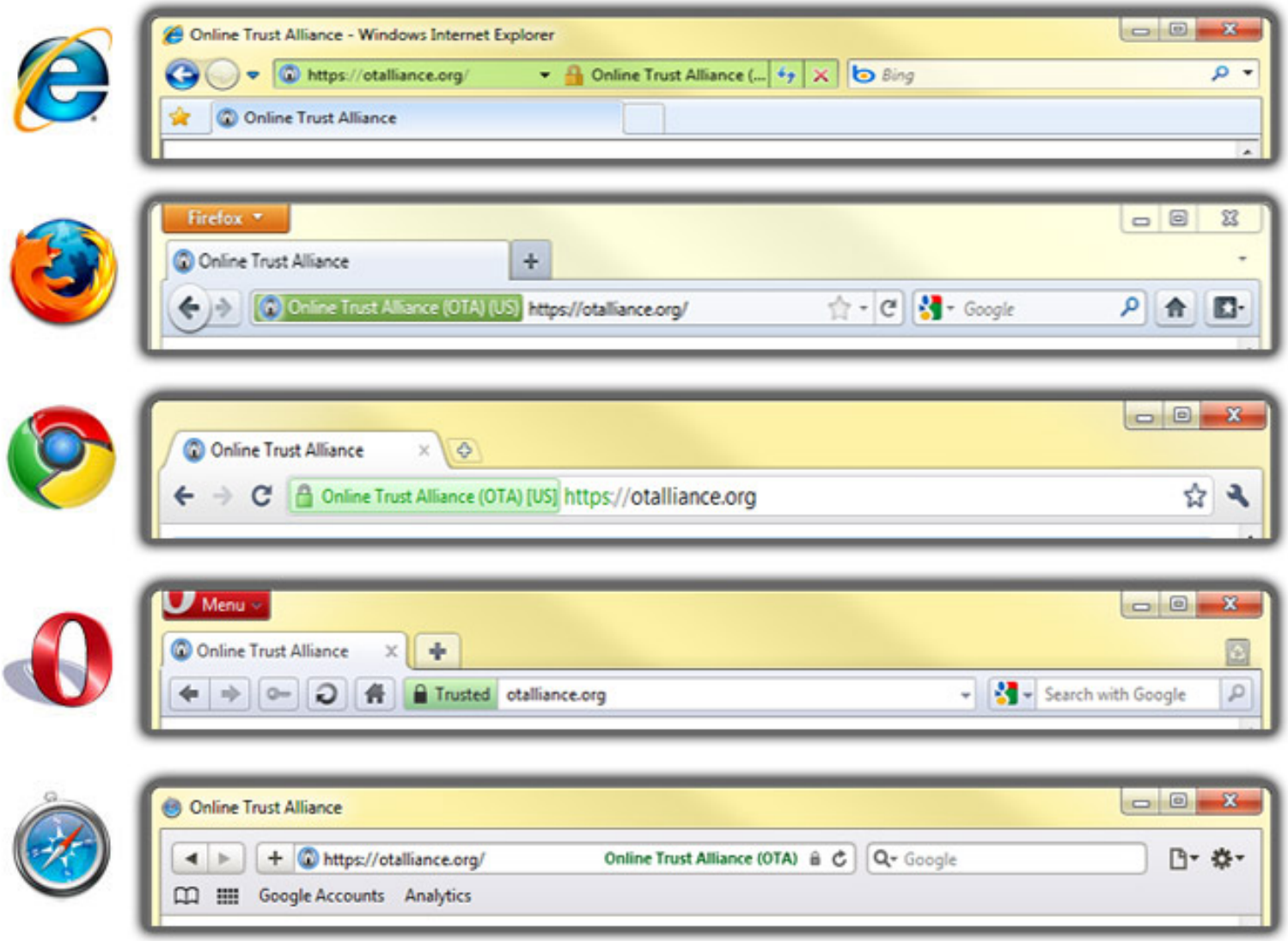
Icons as of 2015

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

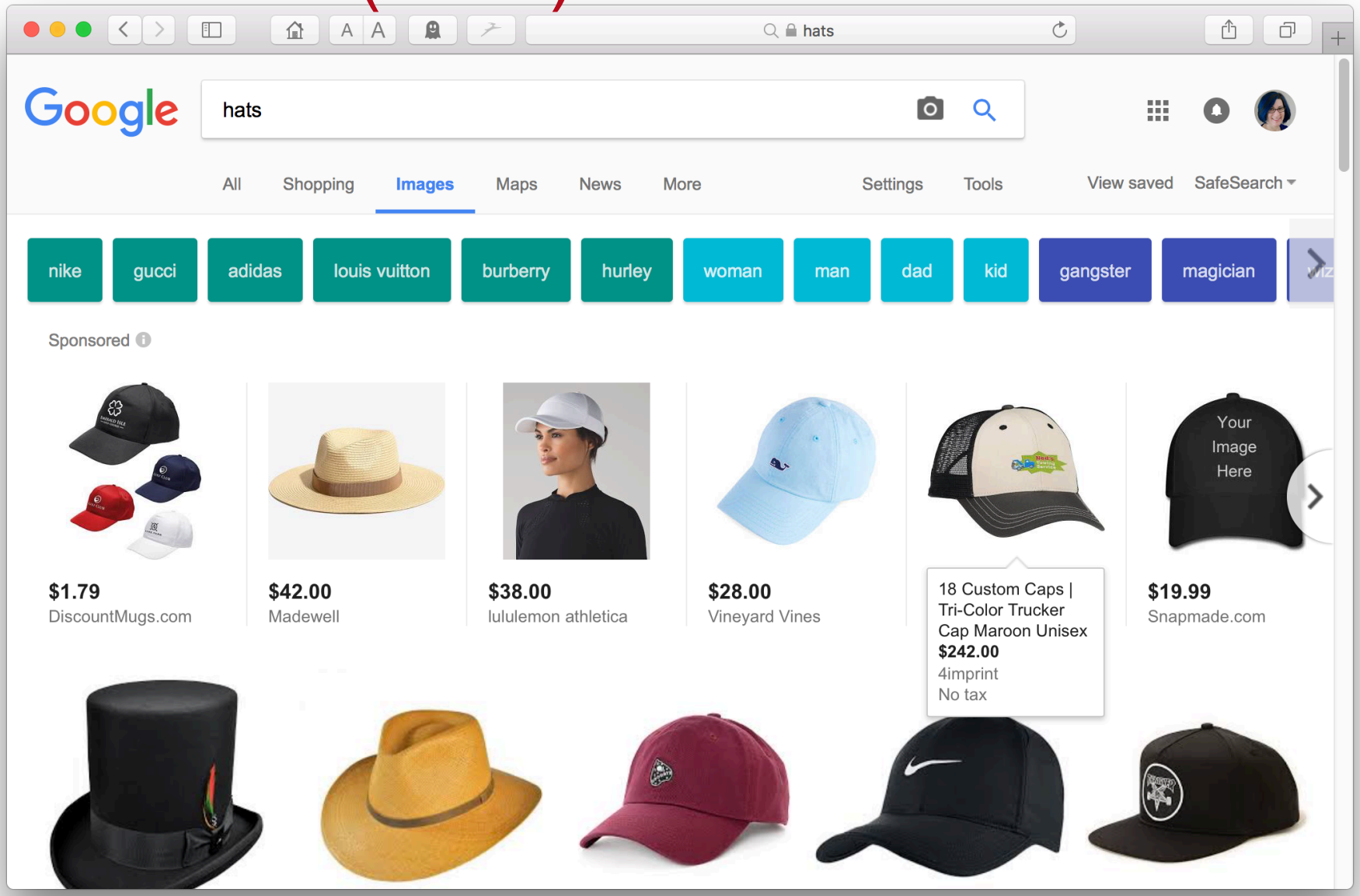
Figure 2: Security indicators for major browsers on Windows (Win), Mac, Android (And), and iOS. For categories that trigger warnings (e.g., malware), we include the security indicator state during the warning.

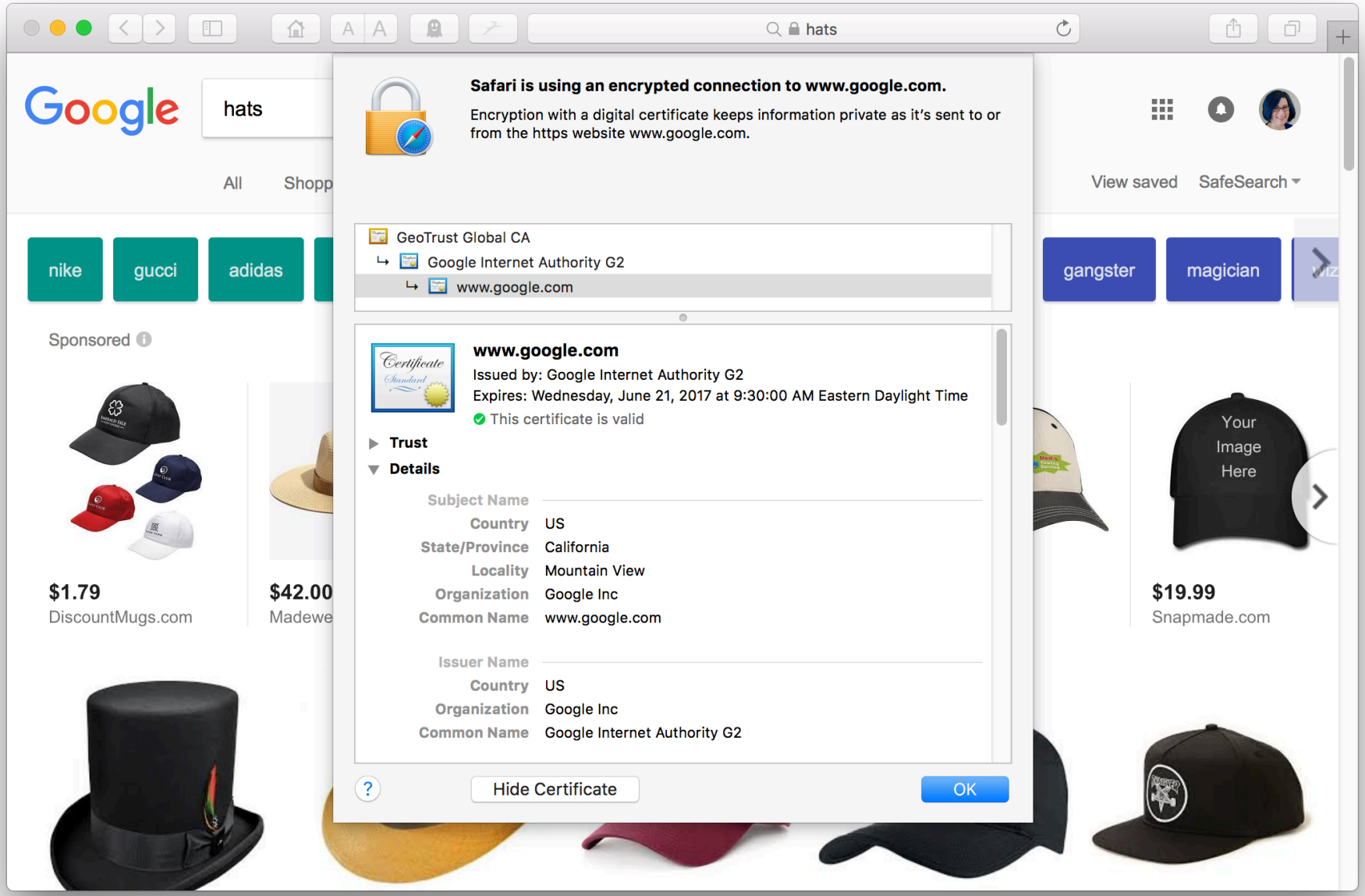
Rethinking Connection Security Indicators
https://www.usenix.org/conference/soups2016/technical-sessions/presentation/porter-felt

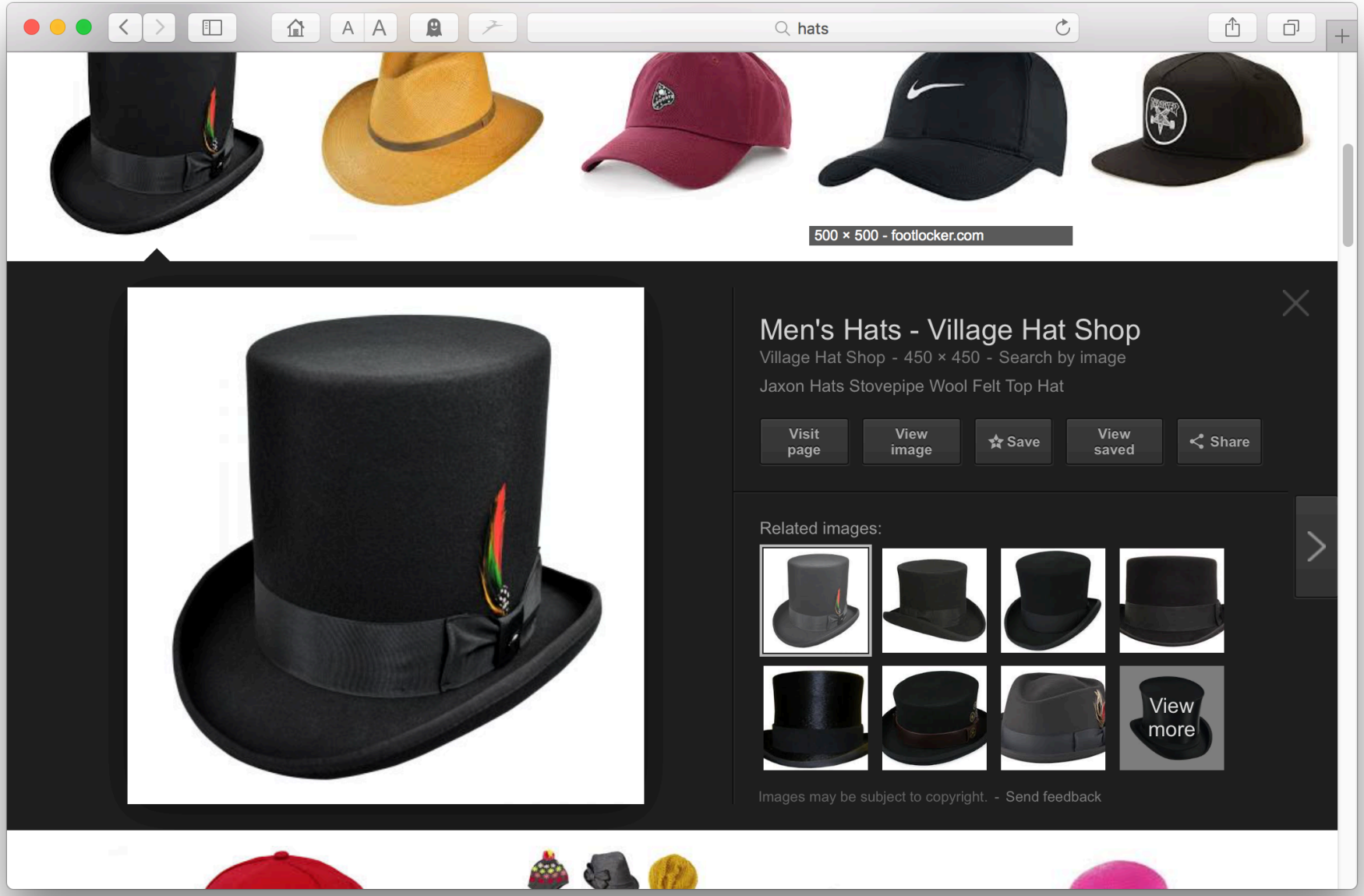
EV cert in 5 browsers

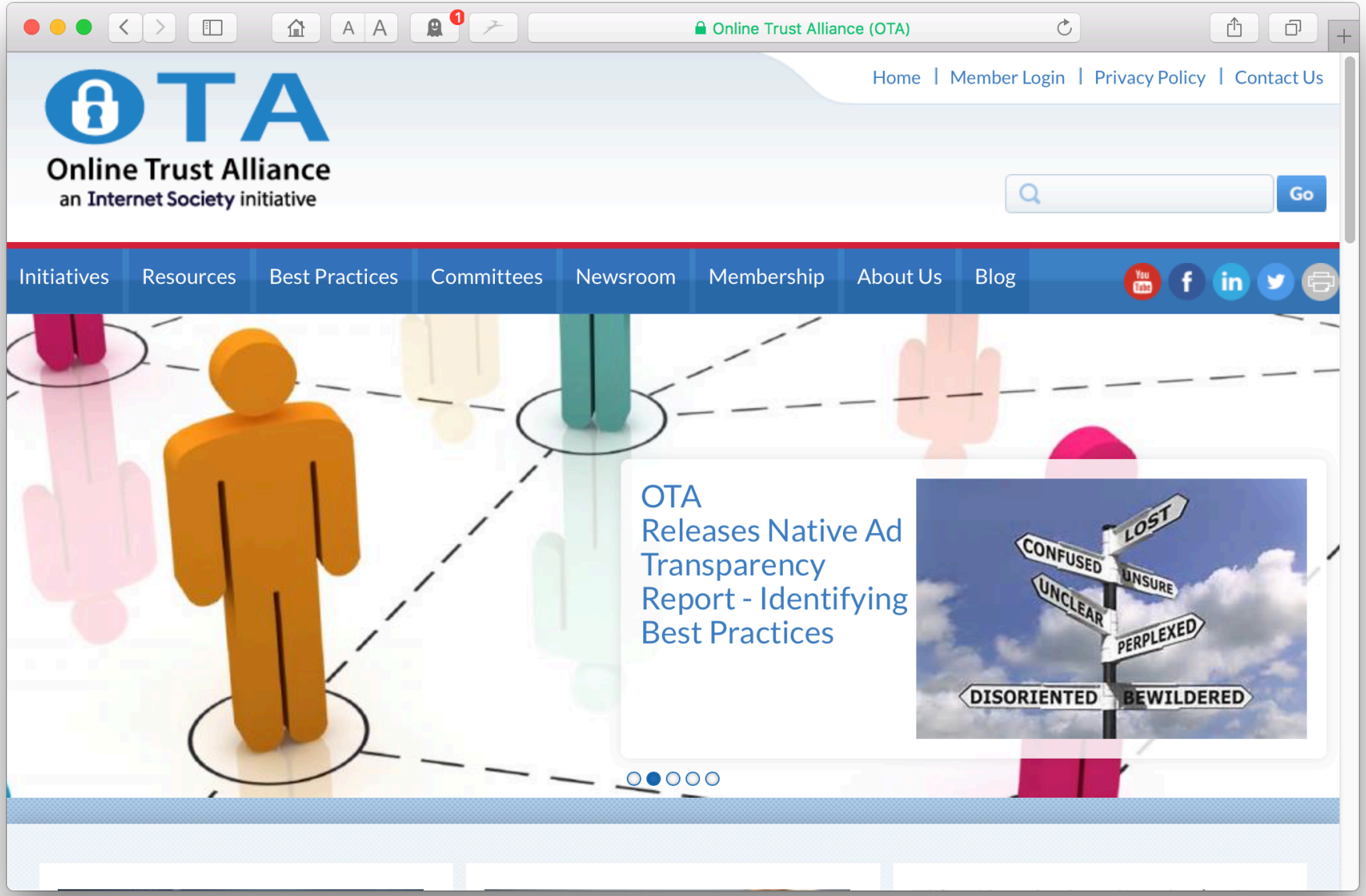


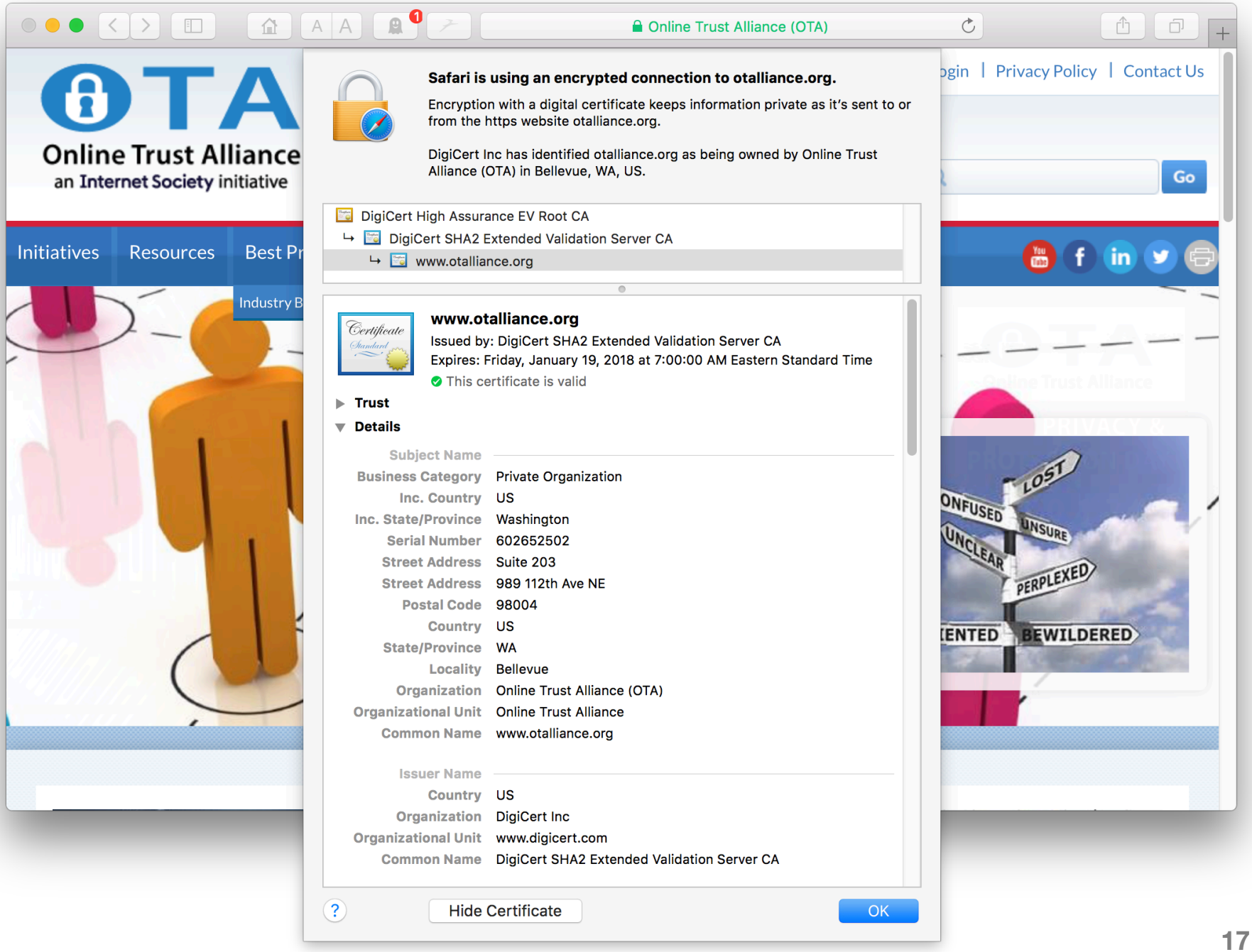
Safari 10 (2017)



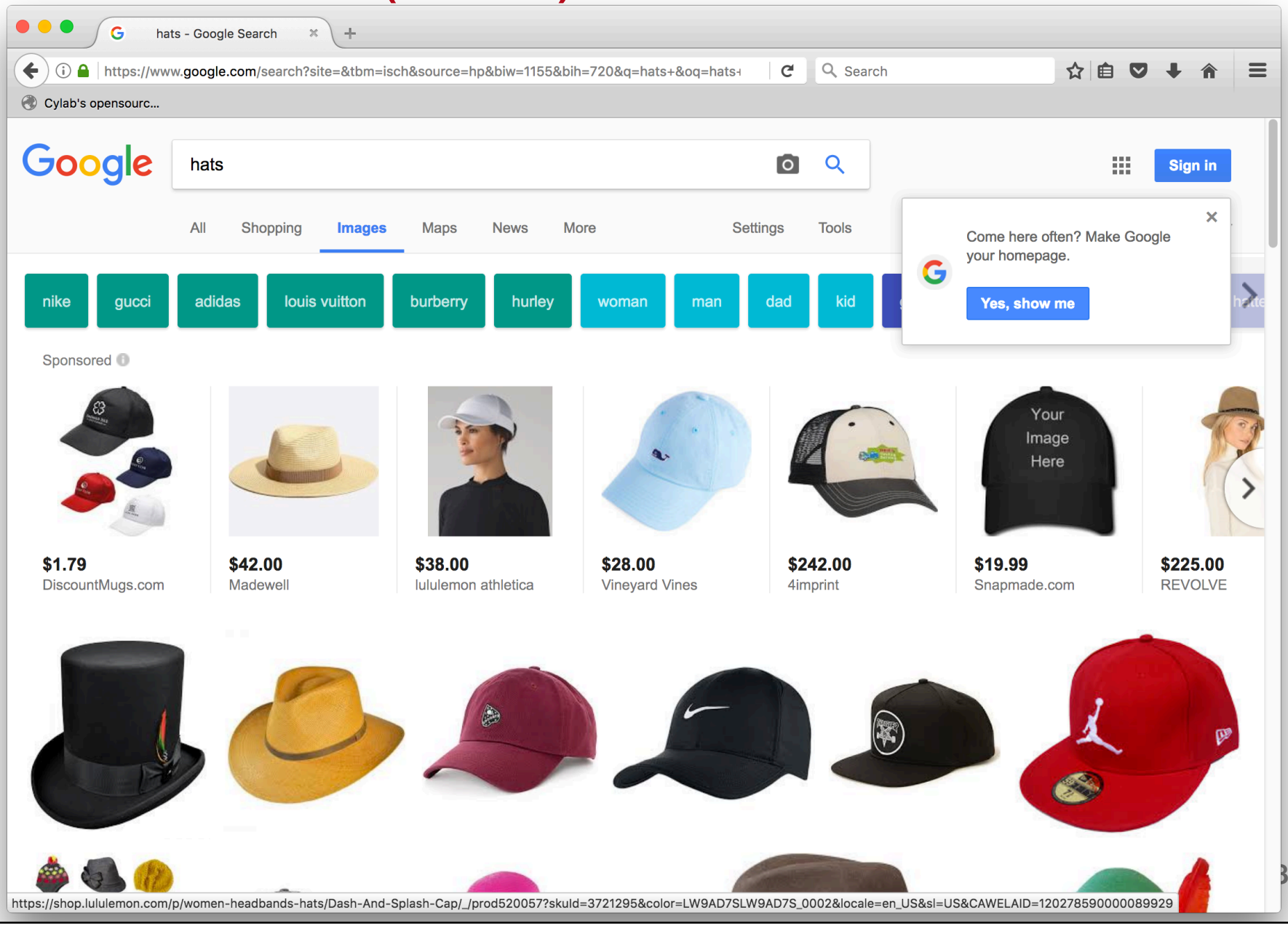

hats
Google
hats
All
Shopp
View saved
SafeSearch
nike
gucci
adidas
gangster
magician
Sponsored
$1.79
DiscountMugs.com
$42.00
Madewe
$19.99
Snapmade.com
Your Image Here
Safari is using an encrypted connection to www.google.com.
Encryption with a digital certificate keeps information private as it's sent to or from the https website www.google.com.
GeoTrust Global CA
Google Internet Authority G2
www.google.com
www.google.com
Issued by: Google Internet Authority G2
Expires: Wednesday, June 21, 2017 at 9:30:00 AM Eastern Daylight Time
This certificate is valid
Trust
Details
Subject Name
Country US
State/Province California
Locality Mountain View
Organization Google Inc
Common Name www.google.com
Issuer Name
Country US
Organization Google Inc
Common Name Google Internet Authority G2
Hide Certificate
OK

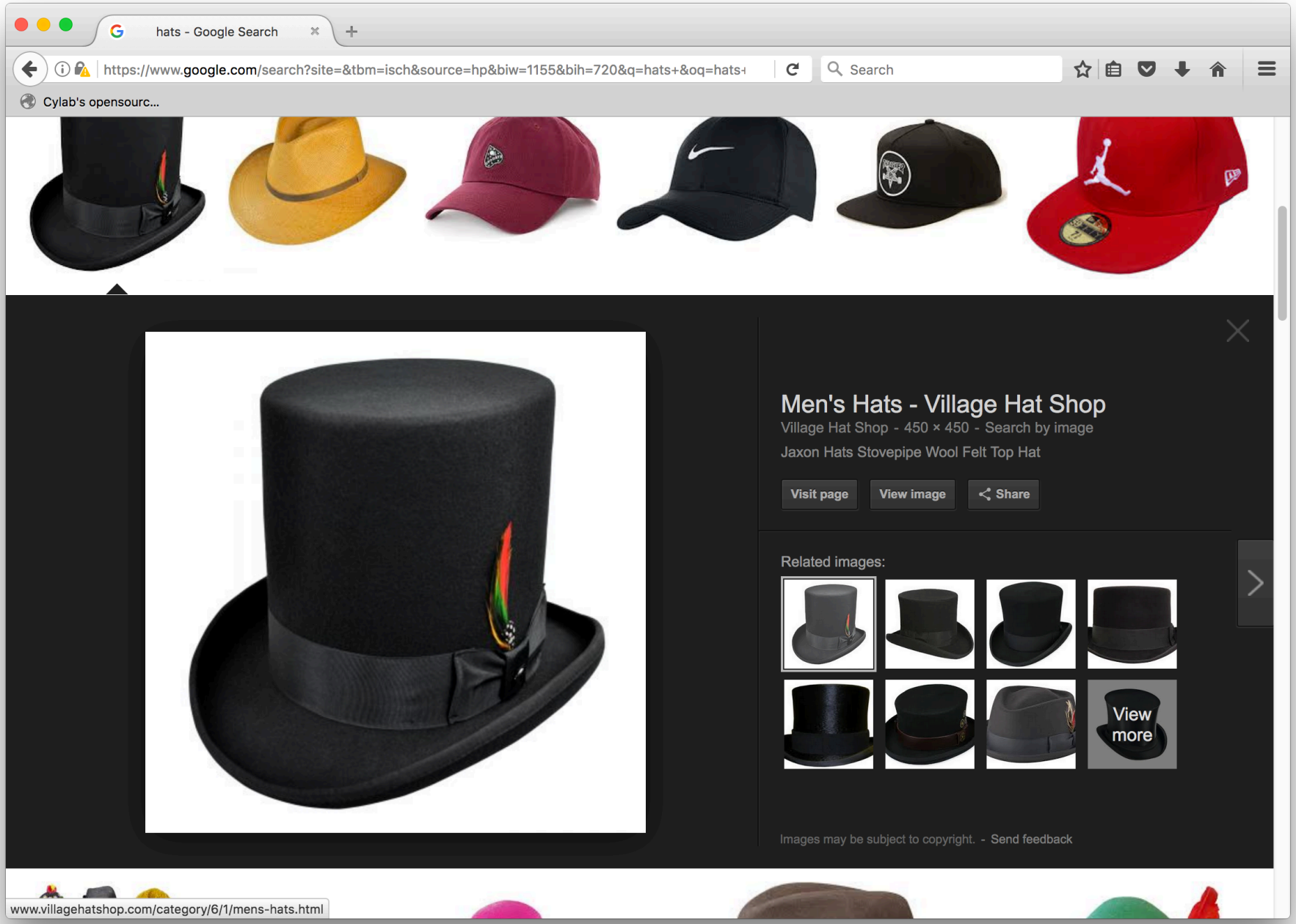

hats
500 × 500 - footlocker.com
Men's Hats - Village Hat Shop
Village Hat Shop - 450 × 450 - Search by image
Jaxon Hats Stovepipe Wool Felt Top Hat
Visit page
View image
Save
View saved
Share
Related images:
View more
Images may be subject to copyright. - Send feedback

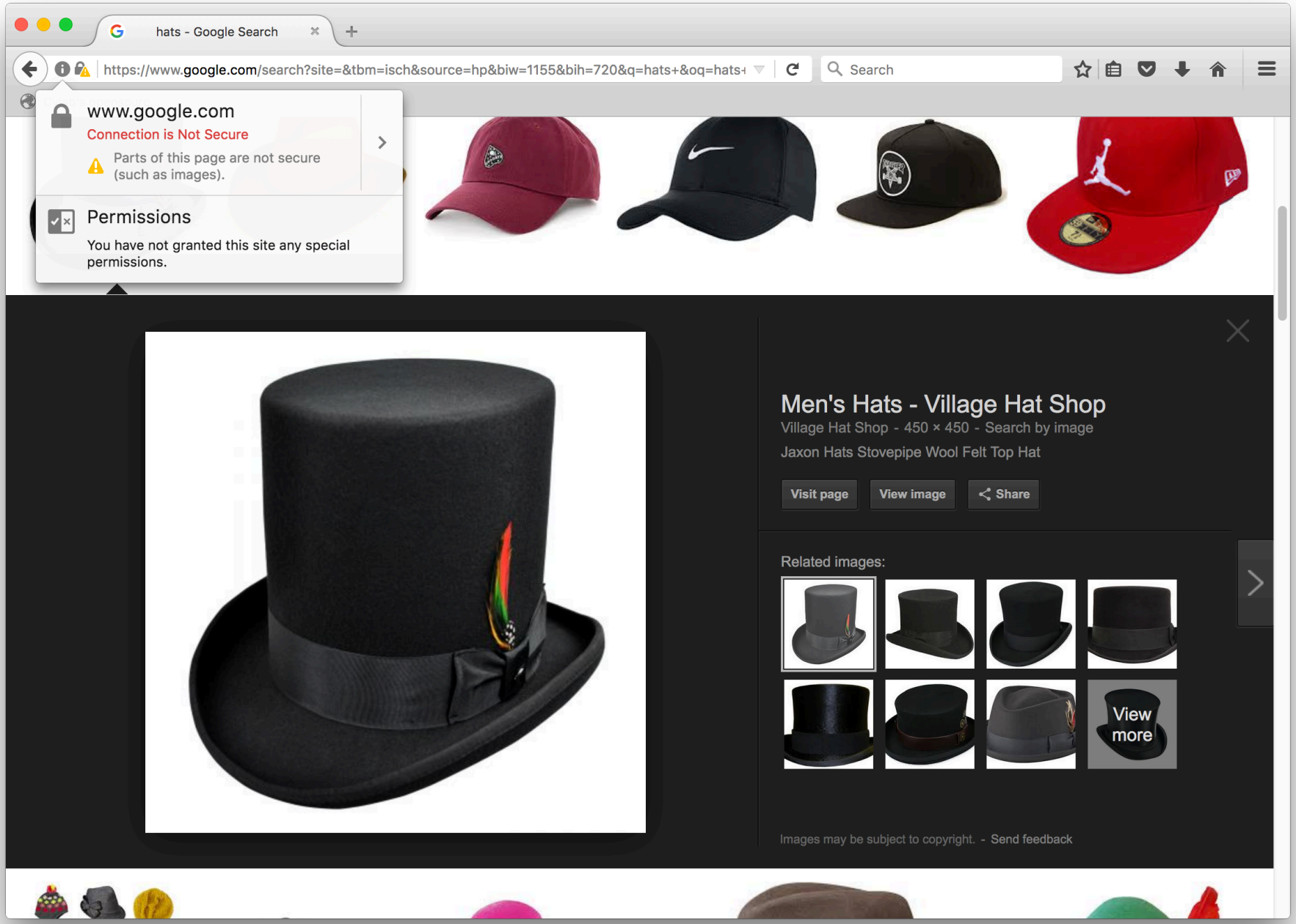

Online Trust Alliance (OTA)
Home | Member Login | Privacy Policy | Contact Us
OTA
Online Trust Alliance
an Internet Society initiative
Go
Initiatives
Resources
Best Practices
Committees
Newsroom
Membership
About Us
Blog
OTA
Releases Native Ad
Transparency
Report - Identifying
Best Practices
LOST
CONFUSED
UNSURE
UNCLEAR
PERPLEXED
DISORIENTED
BEWILDERED

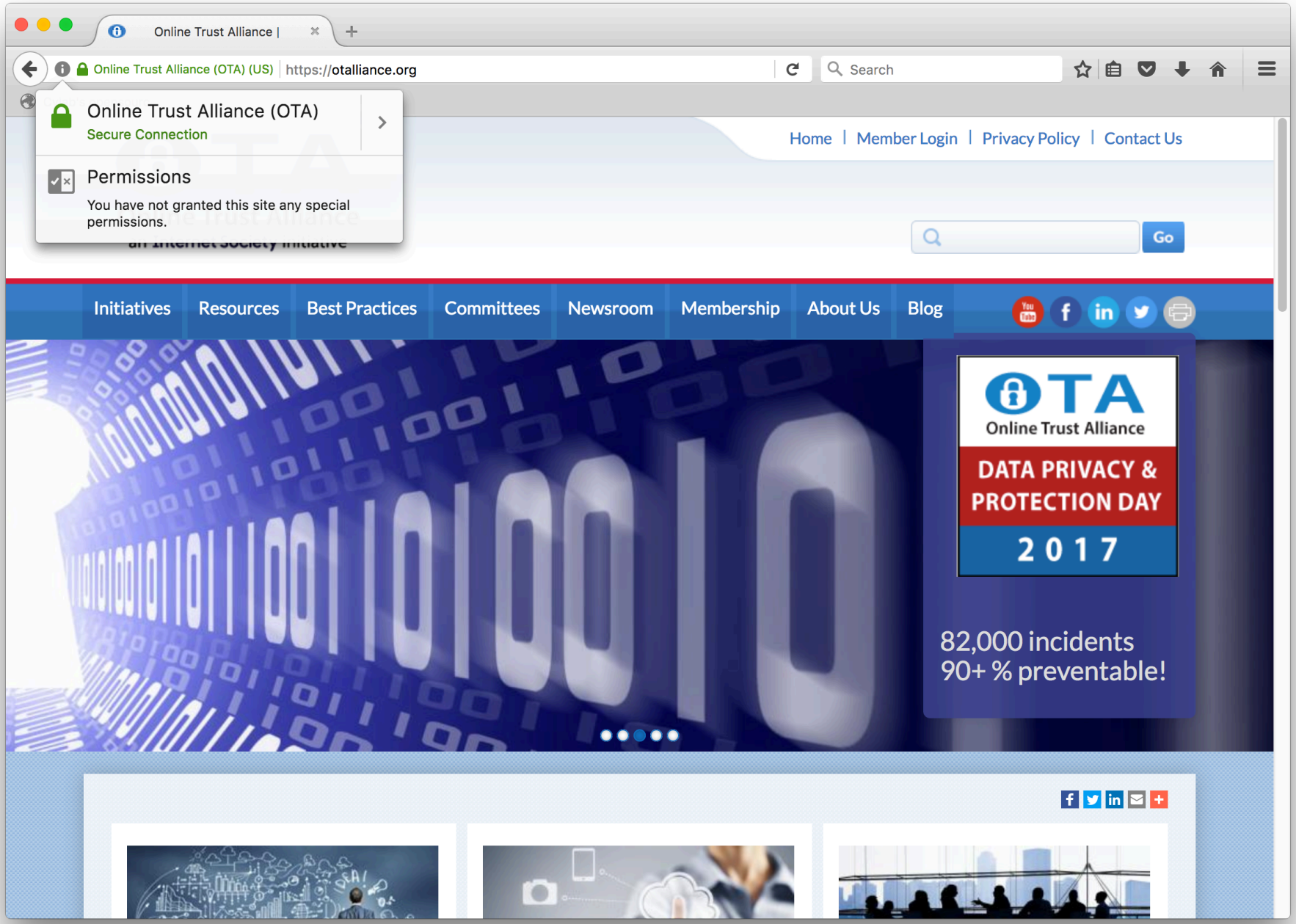

Online Trust Alliance (OTA)
Online Trust Alliance
an Internet Society initiative
Initiatives
Resources
Privacy Policy
Contact Us
Go
Safari is using an encrypted connection to otalliance.org.
Encryption with a digital certificate keeps information private as it's sent to or from the https website otalliance.org.
DigiCert Inc has identified otalliance.org as being owned by Online Trust Alliance (OTA) in Bellevue, WA, US.
DigiCert High Assurance EV Root CA
DigiCert SHA2 Extended Validation Server CA
www.otalliance.org
www.otalliance.org
Issued by: DigiCert SHA2 Extended Validation Server CA
Expires: Friday, January 19, 2018 at 7:00:00 AM Eastern Standard Time
This certificate is valid
Trust
Details
Subject Name
Business Category Private Organization
Inc. Country US
Inc. State/Province Washington
Serial Number 602652502
Street Address Suite 203
Street Address 989 112th Ave NE
Postal Code 98004
Country US
State/Province WA
Locality Bellevue
Organization Online Trust Alliance (OTA)
Organizational Unit Online Trust Alliance
Common Name www.otalliance.org
Issuer Name
Country US
Organization DigiCert Inc
Organizational Unit www.digicert.com
Common Name DigiCert SHA2 Extended Validation Server CA
Hide Certificate
OK
LOST
UNSURE
UNCLEAR
PERPLEXED
BEWILDERED

Firefox 51 (2017)




hats - Google Search
https://www.google.com/search?site=&tbm=isch&source=hp&biw=1155&bih=720&q=hats+&oq=hats+
Search
Cylab's opensourc...
Men's Hats - Village Hat Shop
Village Hat Shop - 450 × 450 - Search by image
Jaxon Hats Stovepipe Wool Felt Top Hat
Visit page
View image
Share
Related images:
View more
Images may be subject to copyright. - Send feedback
www.villagehatshop.com/category/6/1/mens-hats.html


hats - Google Search
https://www.google.com/search?site=&tbm=isch&source=hp&biw=1155&bih=720&q=hats+&oq=hats+
Search
www.google.com
Connection is Not Secure
Parts of this page are not secure (such as images).
Permissions
You have not granted this site any special permissions.
Men's Hats - Village Hat Shop
Village Hat Shop - 450 × 450 - Search by image
Jaxon Hats Stovepipe Wool Felt Top Hat
Visit page
View image
Share
Related images:
View more
Images may be subject to copyright. - Send feedback


Online Trust Alliance |
Online Trust Alliance (OTA) (US)
https://otalliance.org
Search
Online Trust Alliance (OTA)
Secure Connection
Permissions
You have not granted this site any special permissions.
Home | Member Login | Privacy Policy | Contact Us
Go
Initiatives
Resources
Best Practices
Committees
Newsroom
Membership
About Us
Blog
OTA
Online Trust Alliance
DATA PRIVACY & PROTECTION DAY
2017
82,000 incidents
90+ % preventable!

Chrome 56 (2017)

What each security symbol means

These symbols let you know how safe it is to visit and use a site. They tell you if a site has a security certificate, if Chrome trusts that certificate, and if Chrome has a private connection with a site.

- Secure
- Info or Not secure
- Not secure or Dangerous

Self-signed certificates

- What happens if someone signs their own certificate and chooses not to use the PKI infrastructure?
  - You get a warning!

Warnings


http://www.utechsoft.com
This applet was signed by "Unlimi-Tech Software Inc.," and authenticated by "Thawte Consulting cc". Do you trust this certificate?
Click Trust to run this applet and allow it unrestricted access to your computer. Click Don't Trust to run this applet with standard Java restrictions.
?
Show Certificate
Don't Trust
Trust

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

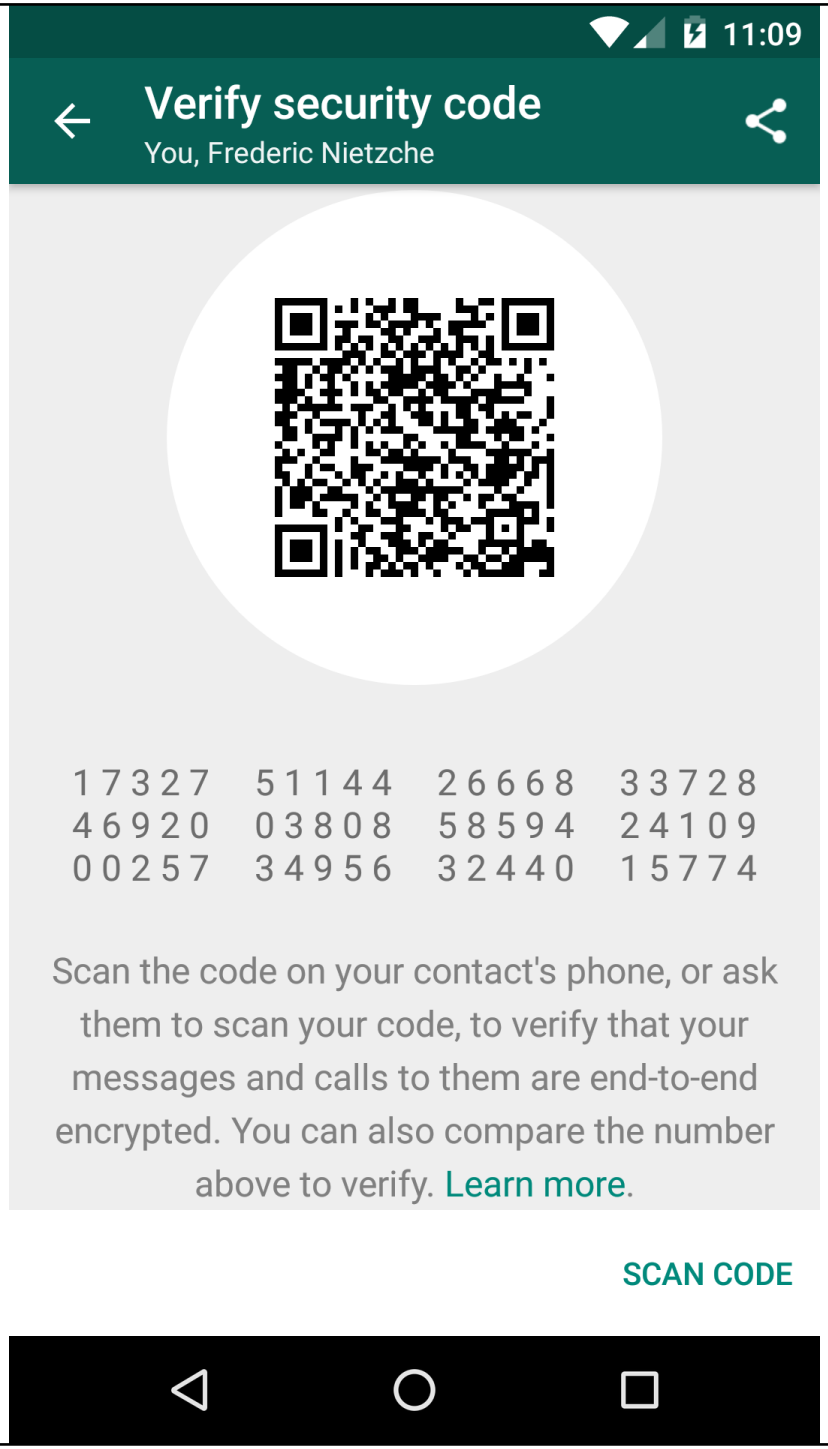
If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

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

Add Exception...

Comparing crypto key fingerprints

- What threat does this defend against?
  - Communicating with someone other than the person you think you are communicating with



Textual Representations

```
6749 1008 6111 3692 5410 1044
1059 5600 3737 5418 5839 2681
```

- Numbers (159.5 bits)
- People used to remembering numbers (e.g. phone numbers, debit card PIN)

```
BC95 4013 2403 4C3A C6FC
3CE3 117F 86A6 8C41 C435
```

- Hexadecimal (160 bits)
- Standard format for cryptographic fingerprints

```
buri padi luya kilo yise rada
deyu sipi hofe hage xata rite
```

- Alternating vowels/consonants (161.1 bits)
- Pseudowords can be pronounced easily

Textual Representations

error seed some stage
skin expansion trousers trouble
thought probable land stone
steel brush self harbor

- Words (155.7 bits)
- May be easier to compare sets of words rather than meaningless text

The nerve gets safely.
Her sick hand offers her open touch fixedly.
His safe request thinks before your flower.
That sun is your black smoke.

- Sentences (159.8 bits)
- Generated using a deterministic sentence generator
- Sentences add more structure, which may help comparison

Graphical Representations

```
+--[ECDSA  256]---+
|         o o.    |
|          = o    |
|         + . .   |
|          o .    |
|         S .     |
|          o E .  |
|           + o +.|
|          . o * +o|
|           o.++*o.|
+-----------------+
```

- Visual host key (≤ 128 bits)
- Used in OpenSSH
- Remembering and comparing visual patterns may be easier than for text

- Vash (≈ 5,438 bits)
- Abstract art created using a PRNG
- Given large entropy, images tend to be more distinctive

Graphical Representations

- Unicorns (≈ 2,854 bits)
- Avatar-like representation
- Generated using a PRNG that determines appearance of different elements (e.g., rainbow location, horn length, unicorn pose)
- May facilitate comparison by providing clear reference points to check
- Also may be easier to memorize image summary for quick comparison

How can these fingerprints be attacked?

- Attacker tries to substitute a similar fingerprint and hopes the user doesn't notice
- Requires attacker to generate a public key that has a similar looking fingerprint
- The more similar it needs to be, the harder it will be for the attacker to generate this
- So how similar does it need to be to fool users?

a1.png a20.png a22.png

a27.png a31.png a3.png

a47.png a63.png a8.png

a12.png

a16.png

a21.png

a22.png

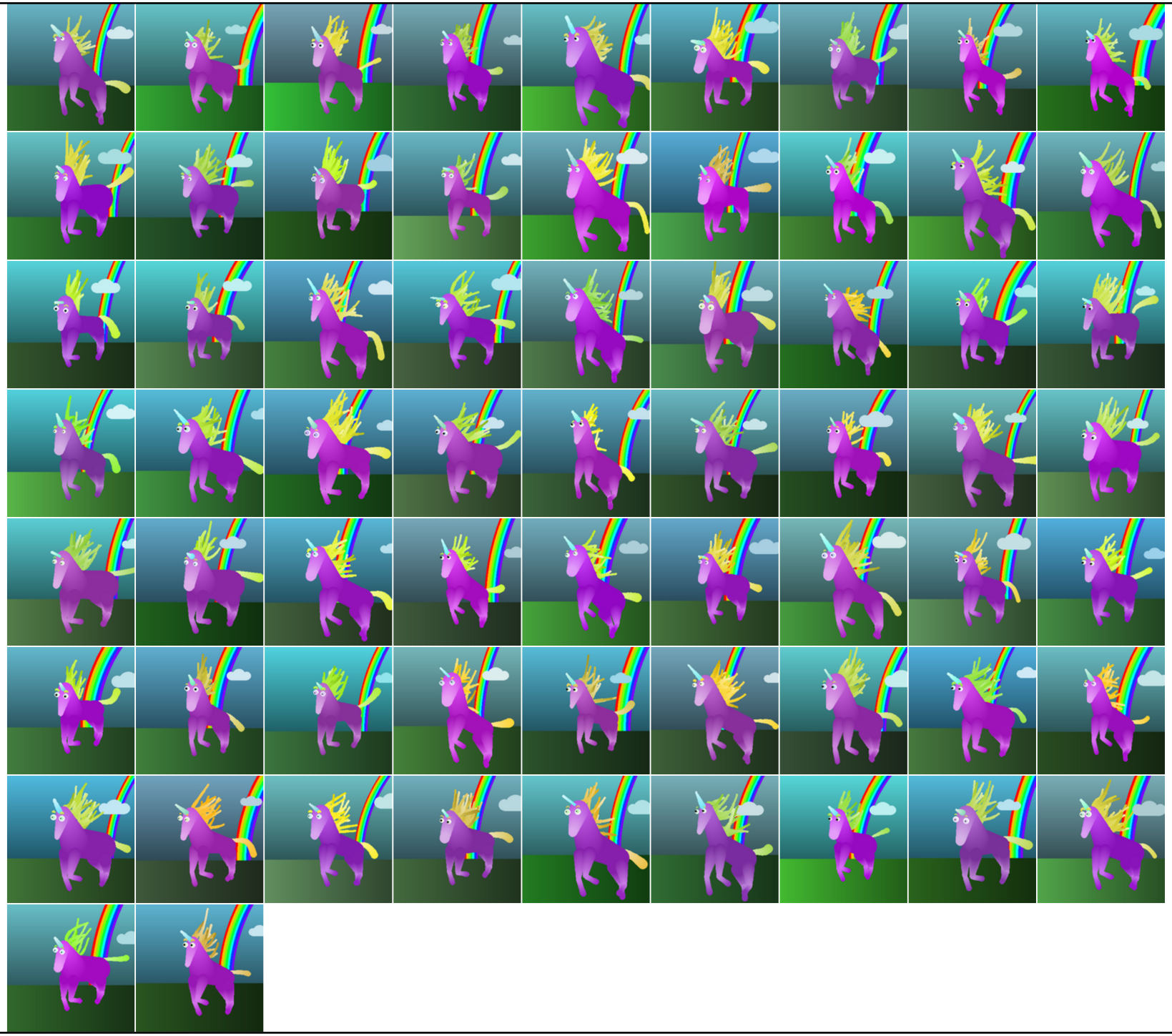
a26.png

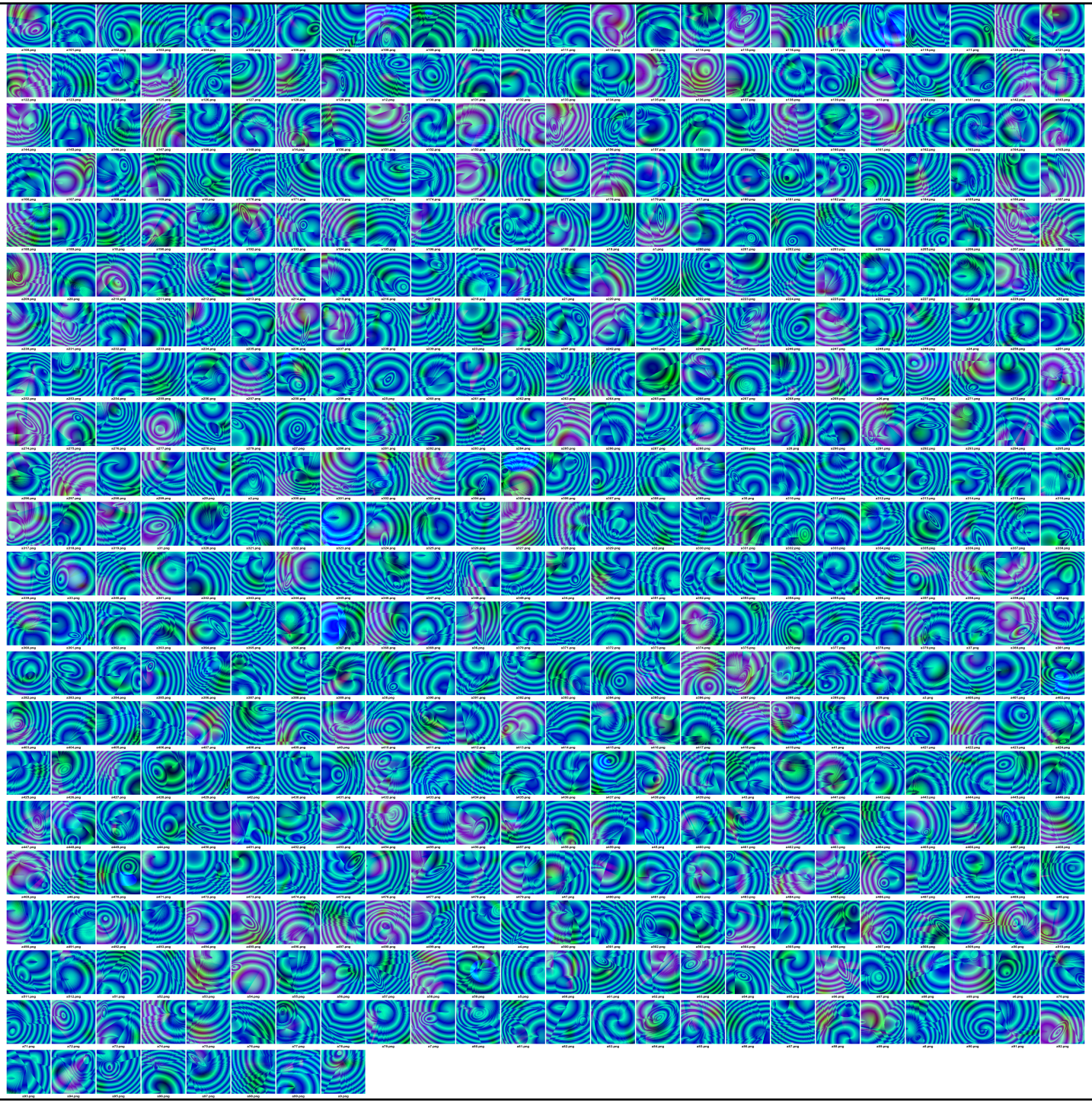
a37.png

a41.png

a47.png

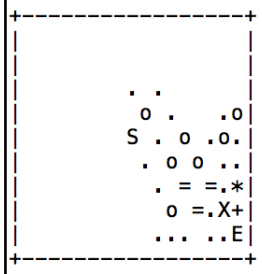
a60.png



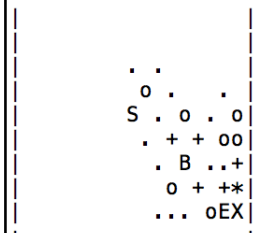


TARGET FINGERPRINT:

71af74bb5a6977e3
4df614d9b81ef6e4

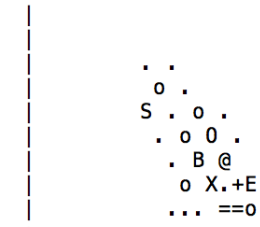


71af74bb5a69275c
fde4eff77db4369e



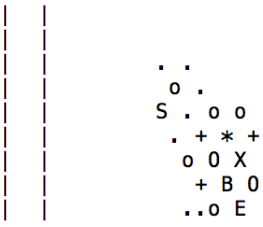
shape: 13.00
marker: 66.87
total: 79.87

71af74bb5a69874f
fbf208974c6ec37e



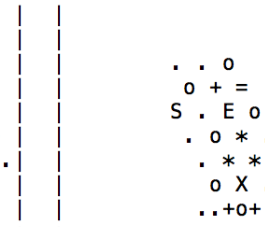
shape: 29.36
marker: 76.08
total: 105.44

71af74bb5a69a7d0
a5bd5c123b291fb3



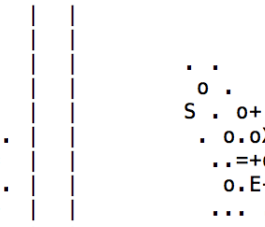
shape: 32.36
marker: 79.93
total: 112.29

71af74bb5a69b704
7cebae255bd0b0b4



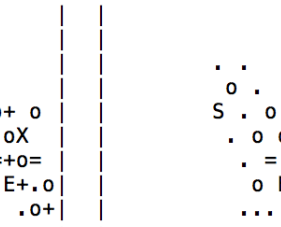
shape: 36.36
marker: 84.10
total: 120.46

71af74bb5a69f7f6
615832a77807ef92



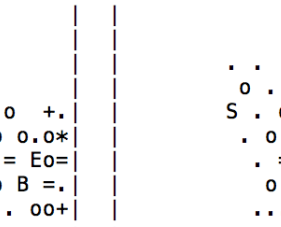
shape: 27.14
marker: 96.93
total: 124.07

71af74bb5a696769
ceef64f614b619a7



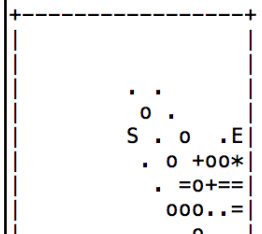
shape: 15.00
marker: 115.42
total: 130.42

71af74bb5a6957cc
6dda2d67d9d8fe2e



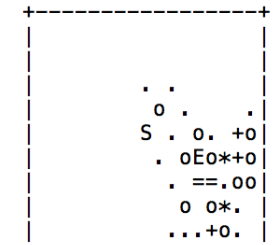
shape: 18.14
marker: 113.21
total: 131.35

71af74bb5a69977c
b7b8643d49b7e557



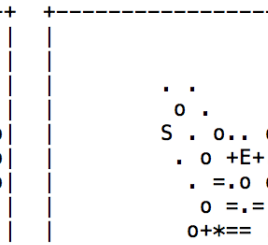
shape: 18.00
marker: 124.27
total: 142.27

71af74bb5a69575e
ae66c4b3548ebe06



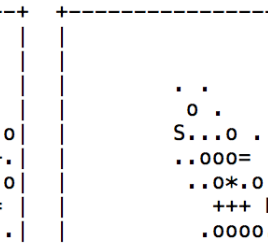
shape: 19.00
marker: 133.44
total: 152.44

71af74bb5a6957e7
e0a7aadf8dda7ac4



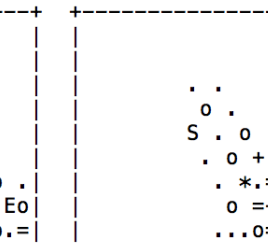
shape: 24.14
marker: 130.80
total: 154.94

71af74bb5a6967a4
3e2478bdf6f7d897



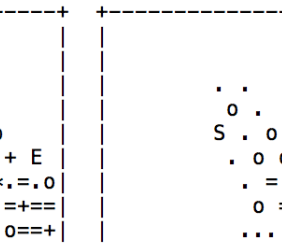
shape: 40.36
marker: 116.02
total: 156.38

71af74bb5a69b76c
fc801f6b6db61763



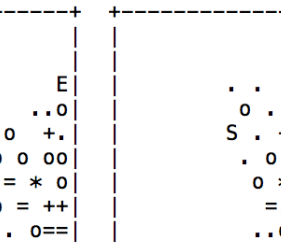
shape: 30.36
marker: 126.62
total: 156.98

71af74bb5a6967b9
f1b657ef4a359c65



shape: 15.00
marker: 145.00
total: 160.00

71af74bb5a69d748
c36b467e082b3f4f



shape: 35.36
marker: 125.65
total: 161.01

Which fingerprint formats are best?

- What makes a good fingerprint format?
- How could we evaluate that?
- What are your predictions?

See forthcoming paper!

- To be presented at CHI 2017 and at CMU privacy seminar April 27, noon, HBH1002
- J. Tan, L. Bauer, J. Bonneau, L. F. Cranor, J. Thomas, and B. Ur. Can unicors help users compare crypto key fingerprints? CHI 2017.