23- SSL, PKIs, and Secure Communication

Lorrie Cranor

April 12, 2017
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

<table>
<thead>
<tr>
<th>Browser</th>
<th>HTTPS</th>
<th>HTTPS minor error</th>
<th>HTTPS major error</th>
<th>HTTP</th>
<th>EV</th>
<th>Malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge 20 Win</td>
<td>example.com</td>
<td><a href="https://mix">https://mix</a></td>
<td>wrong.host.bads</td>
<td>example.com</td>
<td>Symantec Co</td>
<td>Unsafe website</td>
</tr>
<tr>
<td>Safari 9 Mac</td>
<td>example.com</td>
<td>mixed.badssl.c</td>
<td>wrong.host.bads</td>
<td><a href="http://www.example">www.example</a></td>
<td>Symantec Corpo</td>
<td>unavailable</td>
</tr>
<tr>
<td>Chrome 48 And</td>
<td><a href="https://v">https://v</a></td>
<td><a href="https://mix">https://mix</a></td>
<td><a href="https://v">https://v</a></td>
<td><a href="http://www.example">www.example</a></td>
<td>Symantec</td>
<td>Blocked</td>
</tr>
<tr>
<td>Opera Mini 14 And</td>
<td><a href="http://www.example">www.example</a></td>
<td>mixed.badssl.c</td>
<td>wrong.host.bads</td>
<td><a href="http://www.example">www.example</a></td>
<td>Endpoint, C</td>
<td>unavailable</td>
</tr>
<tr>
<td>UC Mini 10 And</td>
<td>Example Do</td>
<td>mixed.badssl.c</td>
<td>wrong.host.bads</td>
<td>Example Do</td>
<td>Endpoint, C</td>
<td>Blocked</td>
</tr>
<tr>
<td>UC Browser 2 iOS</td>
<td>Example Do</td>
<td>mixed.badssl.c</td>
<td>wrong.host.bads</td>
<td>Example Do</td>
<td>Symantec</td>
<td>unavailable</td>
</tr>
<tr>
<td>Safari 9 iOS</td>
<td>example.com</td>
<td>mixed.badssl.c</td>
<td>wrong.host.bads</td>
<td>example.com</td>
<td>Symantec</td>
<td>unavailable</td>
</tr>
</tbody>
</table>

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)
OTA Releases Native Ad Transparency Report - Identifying Best Practices
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.

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: 602662502
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
Firefox 51 (2017)
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

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.
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

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

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.
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

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

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

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

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

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

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.
Graphical Representations

- 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?
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