Privacy Browser - Feature #208

Calculate SSL certificate fingerprints

09/28/2017 11:16 PM - bill bunter

Status:	New	**Start date:**	09/28/2017
Priority:	4.x	**Due date:**	
Assignee:	Soren Stoutner	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:		**Spent time:**	0.00 hour

Description

Would like to see certificate fingerprint on the certificate dialogue.
Android 4.4.2
WebKit 537.36

History

#1 - 09/28/2017 11:40 PM - Soren Stoutner

- Assignee changed from bill bunter to Soren Stoutner

- Priority changed from 2 to 3.x

I agree that it would be nice to display the certificate fingerprint. Amazingly to me, Google does not make it easy to get access to it.

https://developer.android.com/reference/android/net/http/SslCertificate.html

It should be possible to calculate the certificate myself, but it looks like this would require having access to the entire certificate in DER form.

https://security.stackexchange.com/questions/14330/what-is-the-actual-value-of-a-certificate-fingerprint#14345

My guess is that it won't be possible to get that level of access until after `WebView` is forked to produce Privacy WebView. Accordingly, I will revisit this during the 4.x series.

https://www.stoutner.com/category/roadmap/

#2 - 09/28/2017 11:48 PM - Soren Stoutner

- Subject changed from website certificate info to Calculate SSL certificate fingerprints

#3 - 09/29/2017 01:03 AM - bill bunter

The fingerprint is the only sure way to verify the cert is not a fake one as part of a mitm attack, you can verify it by going to https://www.grc.com/fingerprints.htm
That server has tier 3 internet access and cannot be mitm attacked so when it retrieves the fingerprint you know it is the genuine one. If we see the same fingerprint we know we should pin that cert in Domain pinning.
BTW, I have been using Privacy Browser for the past few months as my default browser I like it a lot you did some nice work on it,thankyou.
I am a member at https://wilderssecurity.com Browser technology and security/privacy issues are some of the main topics of conversation in the forums, we are mostly IT specialists, developers and privacy advocates I hope you might consider joining

#4 - 09/29/2017 11:16 AM - Soren Stoutner

- Priority changed from 3.x to 2

1. I'm glad you enjoy using Privacy Browser. And I appreciate the suggestions you have made for improving it.

2. When I started working on the SSL certificate pinning feature, my original intention was to use the certificate fingerprints to check for matches. I was surprised that Android does not make that easy to do. Digging a bit more into the documentation, it looks like if I can get a handle on the certificate in either `Certificate` or `X509Certificate` form I can use either `getEncoded()` or `getTBSCertificate()`, respectively, to access the DER encoded certificate, and from there calculate the SHA-1 hash. `WebView` does not expose either a `Certificate` or an `X509Certificate`, and it does not appear possible to convert `SslCertificate` to either of these. But it does look like it is possible to retrieve an `X509Certificate` directly from the web server if one is willing to put forth a bit of work, which is easier than I had initially expected. I will dig into this deeper during the second half of the 2.x cycle.

https://developer.android.com/reference/java/security/cert/Certificate.html

https://developer.android.com/reference/java/security/cert/X509Certificate.html

https://developer.android.com/training/articles/security-ssl.html

3. Having a tier 3 internet connection does not make https://www.grc.com/fingerprints.htm impervious to MITM attacks. For example, to connect to another machine on the internet and retrieve the SSL certificate, most packets from grc.com will need to transit through one of the 6 tier 1 providers (Level 3 Communications, Telia Carrier, NTT, Cogent, GTT, and Tata Communications).

https://en.wikipedia.org/wiki/Internet_backbone

It is likely that the NSA has access to most, if not all, tier 1 providers, either with the companies assistance or through tapping of underwater fiber cables. Other large government intelligence agencies have similar programs.

https://thetechjournal.com/internet/web-security/nsa-might-have-directly-wiretapped-tier-1-networks-in-the-u-s.xhtml

https://www.thenewamerican.com/usnews/item/16086-nsa-taps-directly-into-undersea-fiber-optic-data-cables

As another example, most of the web servers that https://www.grc.com/fingerprints.htm is connecting to in order to retrieve their SSL certificates are located in data centers. Typically there are only a few routers that control all traffic into and out of the data centers. If those routers have been compromised, then whoever has illicit access to them can perform a MITM attack on any data passing to the servers in that data center.

4. Thanks for the tip about https://wilderssecurity.com. I have posted a thread requesting feedback and suggestions.

https://www.wilderssecurity.com/threads/privacy-browser-for-android.397013/

#5 - 12/24/2018 03:00 PM - Soren Stoutner

- Priority changed from 2 to 4.x