Haketilo - Feature #13

find some way not to require each chrome user to modify manifest.json

07/01/2021 12:26 PM - koszko

Status:	Closed	**Start date:**	07/01/2021
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

Smuggling page's policy setting to content scripts without use of asynchronous APIs like messages system doesn't seem to be doable in a straightforward way. Currently invented hack is to smuggle setting in URL after hash ("#"). A schema to smuggle settings must make it impossible for website operators to trick the extension into assuming arbitrary policy settings for a site. This can be achieved by mungling the URL with a value not known to website. This value must be obtainable in a synchronous fashion from within content script. Under Mozilla, per-session extension id can serve as such value. For Chrome, the only option discovered so far is to add a unique "key" entry to manifest and use it. For that, each Chrome user would hae to edit manifest.json to set a different key.

We need to find some other value that could be used instead of key or better - find another way to smuggle page's policy settings to content scripts. Before this is achieved, it is possible to automate the task when distributing the extension as some distro's package (e.g. as .deb) which we should also do.

History

#1 - 08/03/2021 01:19 AM - koszko

Please note that under Manifest V3 in Chrome we'll be able to dynamically register content scripts which might solve this problem

#2 - 08/27/2021 10:07 AM - koszko

Using a synchronous AJAX call from the content script might allow us to use a bundled file as a secret

#3 - 08/28/2021 02:54 AM - jahoti

> Using a synchronous AJAX call from the content script might allow us to use a bundled file as a secret

Wouldn't that still require each user to build the extension themselves?

#4 - 08/28/2021 08:48 AM - koszko

> Wouldn't that still require each user to build the extension themselves?

It would. It would just be less hacky than using that manifest key

#5 - 09/06/2021 04:53 PM - koszko

> Wouldn't that still require each user to build the extension themselves?

It would. It would just be less hacky than using that manifest key

I realized I didn't explain the actual issue with "key" in the manifest.

Instead of employing synchronous AJAX (which is deprecated and generates lots of annoying warnings plus could get completely disabled in some version of Chrome), I simply moved the unique value to another place in the manifest. The "key" manifest property was required by Chromium to be an actual key in PEM format which meant build.sh would need to depend on, for example, OpenSSL to generate it. Now build.sh can simply read /dev/urandom to get a random value it puts in one of the filenames in "web_accessible_resources".

This is now on koszko branch

#6 - 09/07/2021 12:00 AM - jahoti

> The "key" manifest property was required by Chromium to be an actual key in PEM format

Thank you for explaining! The new setup does seem significantly better with this in mind.

#7 - 09/10/2021 08:49 PM - koszko

I found details regarding the CRX file format:
http://www.dre.vanderbilt.edu/~schmidt/android/android-4.0/external/chromium/chrome/common/extensions/docs/crx.html

Unfortunately, the "Google BSD license" link is dead and I cannot check which of the BSD licenses applied to that shell script... But that's a minor issue. With or without that script, I should be able to set up a service that will serve .crx Chromium builds of Hachette that differ by some secret.

And, of course, tech-aware users will be encouraged to build the extension themselves :)

#8 - 09/11/2021 05:13 AM - jahoti

> Unfortunately, the "Google BSD license" link is dead and I cannot check which of the BSD licenses applied to that shell script...

While rewriting it would not be hard and may in fact be the preferable option, the Internet Archive does have a copy: https://web.archive.org/web/20131114001115/http://code.google.com/google_bsd_license.html (the link died 8 years ago!).

#9 - 09/29/2021 03:03 AM - jahoti

- Status changed from New to Closed

- % Done changed from 0 to 100

This is now in master.