A Security analysis of Browser Extensions

Abhay Rana
Rushil Nagda
SDSLabs, IIT Roorkee

Presentation flow

Introduction to extensions.
Extension Security
Threat model
Methodology
Demos
Statistics
Solution and Conclusions

Browser Extensions

Add functionality to a browser

Written by a third party

Improve the browser experience

Extension security

Google Chrome uses a three step model:

- *Isolated worlds* : An extension's content scripts cannot access the direct DOM (Document Object Model) of the current running page, but access a copy of it. The javascript execution of content-scripts is kept completely separate from the execution of the page's actual javascript code, if any.
- *Privilege separation* : Core extension scripts have access to the chrome native APIs. Content scripts do not.
- *Permissions* : Extensions are required to pre-declare their needed privileges, and are limited to those by the browser.

Opera provides limited (common) privileges to all extensions.

Chrome Extension Model

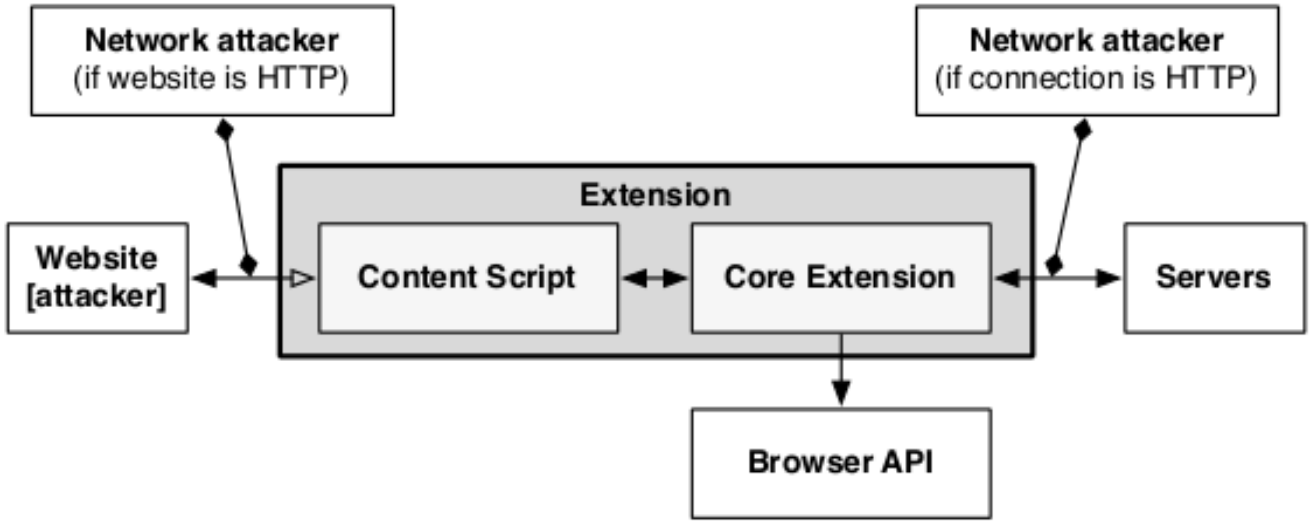


Figure 1: The architecture of a Google Chrome extension.

Threats

Malicious Extensions: An attacker could install a malicious extension in the browser that could, theoretically, cause a lot of damage.

Extension Vulnerabilities: The extension could in itself be vulnerable.

- Insecure Coding practices
- Developer negligence or incompetence

Method of analysis

Silent extension installation

Source code analysis

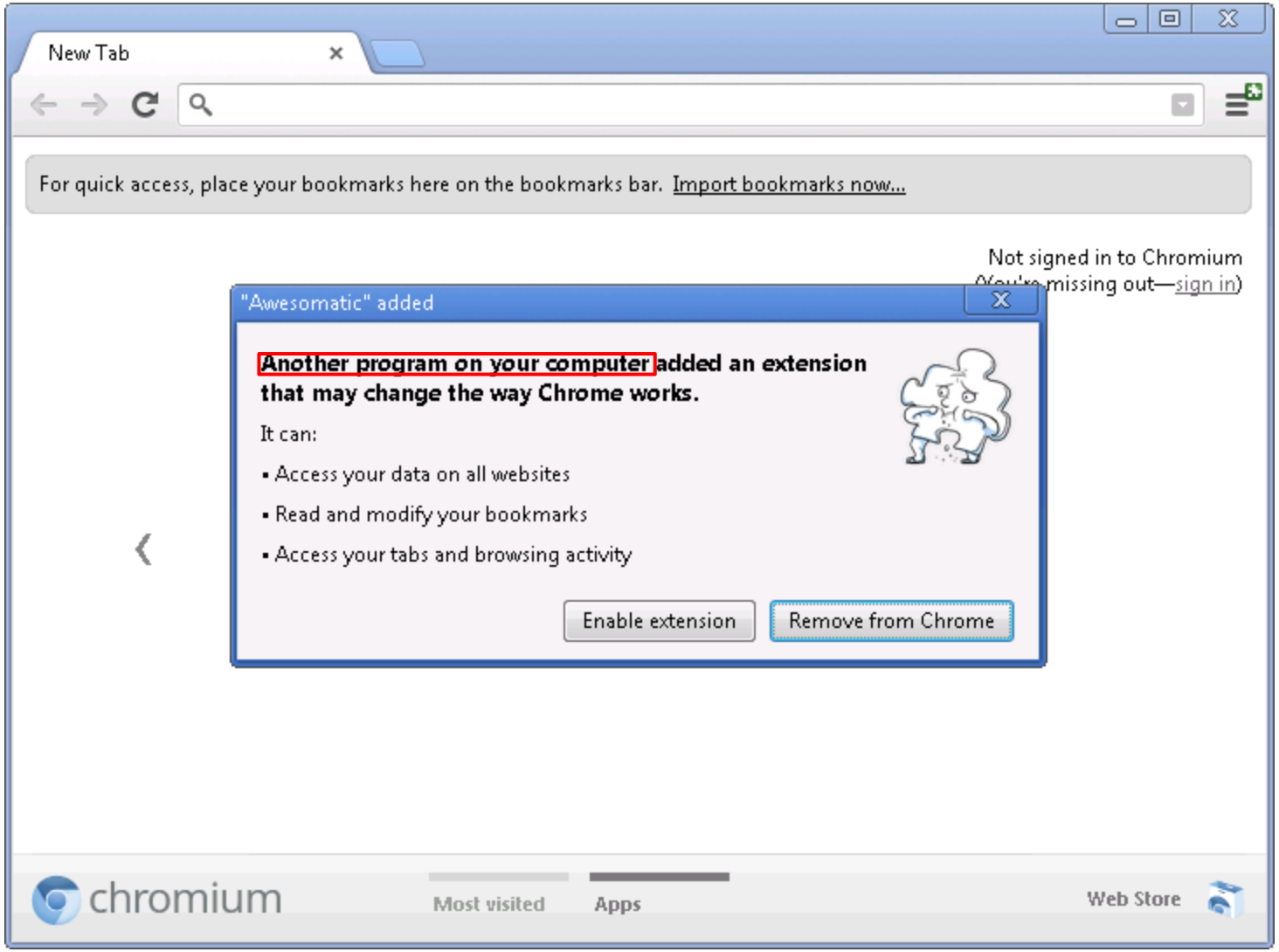
Pre-install analysis of extensions

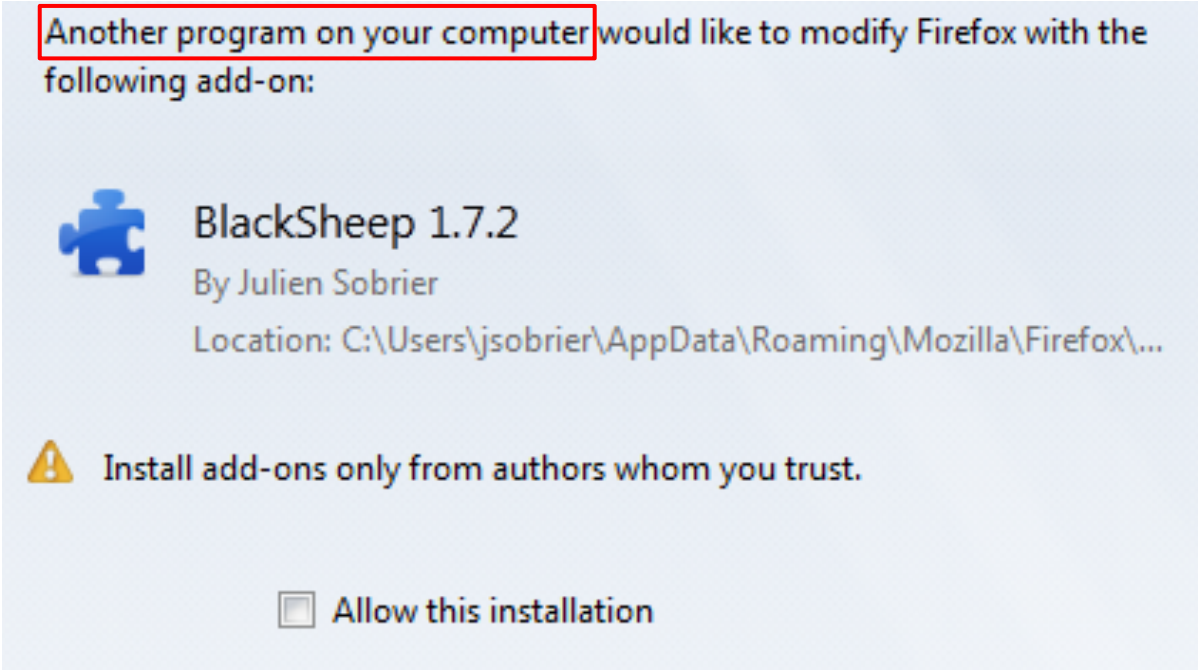
Silent Installation

Browsers allow third party application developers to *silently* install extensions in the browser. (Think Ask Toolbar)

Both Google Chrome & Firefox make the user confirm the installation by giving a UI prompt on next restart.

We work-around this prompt to prove that *complete silent installation* is possible.


New Tab
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
Not signed in to Chromium
(You're missing out—sign in)
"Awesomatic" added
Another program on your computer added an extension that may change the way Chrome works.
It can:
• Access your data on all websites
• Read and modify your bookmarks
• Access your tabs and browsing activity
Enable extension
Remove from Chrome
chromium
Most visited
Apps
Web Store


Another program on your computer would like to modify Firefox with the following add-on:
BlackSheep 1.7.2
By Julien Sobrier
Location: C:\Users\jsobrier\AppData\Roaming\Mozilla\Firefox\...
Install add-ons only from authors whom you trust.
Allow this installation

DEMO

Silent Extension Installation

Statistics: Content-Security Policy

Content-Security Policy is known to reduce extension vulnerabilities by enforcing stronger coding practices.

It is only available on a *"setting"* called Manifest Version=2 on Chrome, though.

It will get deployed to every extension on Chrome by September 2013.

We found 4079/9558 extensions using CSP

Statistics: Privilege abuse

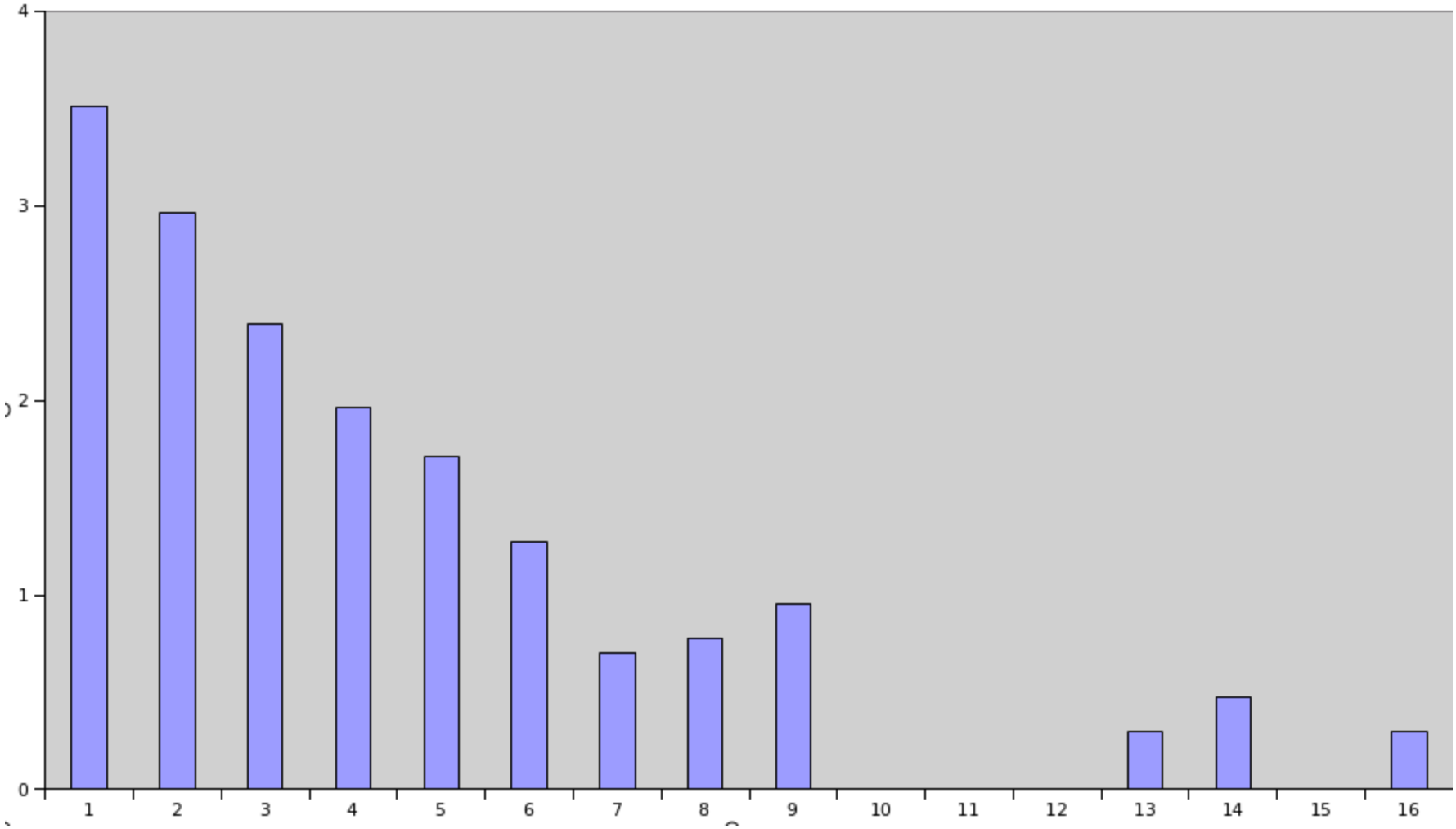
Principle of least privileges

Match Permissions sought by an extension by those actually used

Almost 50% of analysed extensions asked for at least one extra permission

Very sensitive information, like browser cookies, were sought in multiple instances.

Number of extra privileges sought	Number of violating extensions
1	3237
2	923
3	250
4	92
5	52
6	19
7	5
8	6
9	9
10	0
11	0
12	1
13	2
14	3
15	1
16	2


4
3
2
1
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16

Statistics: Network vulnerability

We found at-least 146 extensions making a network request to javascript files over HTTP.

HTTP requests can be attacked by a MitM attack and replaced with malicious javascript.

Furthermore extensions could be making XHR or other network requests over HTTP that we are not aware of.

Extension checker

Pre-checks the extension's API usage and reports it to the user.

Chrome Webstore Extension Analysis

Permissions Being Asked:

```
Array
(
    [0] => bookmarks
    [1] => chrome://favicon/
    [2] => clipboardRead
    [3] => clipboardWrite
    [4] => contextMenus
    [5] => cookies
    [6] => fileBrowserHandler
    [7] => geolocation
    [8] => history
    [9] => idle
    [10] => management
    [11] => notifications
    [12] => tabs
    [13] => tts
    [14] => unlimitedStorage
    [15] => webNavigation
    [16] => webRequest
    [17] => *://*/*
    [18] => http://*/*
    [19] => https://*/*
)
```

Permissions Being Used:

```
Array
(
    [0] => extension
)
```

Difference

```
Array
(
    [0] => bookmarks
    [1] => chrome://favicon/
```

Solution and Conclusion

- Our extensions checker provides information about the authenticity of an extension.
- Any extension with more than 6 permissions sought should be manually reviewed.
- Content-Security-Policy be made mandatory for all extensions.
-