

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 scenes. Consequently, browser extensions seem 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 form 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

Google Cl	nrome	×
<u> </u>	Please close all Google Chrome windows and try again.	
	ОК	



Browsers are the new operating systems



Browsers are the new operating systems









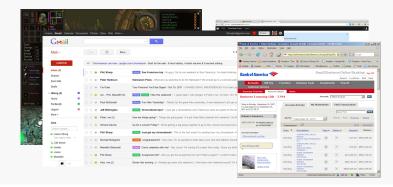


						K V Rgame Nature	Konstanting (Series and Series and Series and Series and Series and Series and Series (Series (Se	1/ One-section and 1	-		¢.
	Gmail	Decor	ieres Phot	is Stes Web Mare+	* Q		hkinglan@gnal.com	Staw	Could have been allowed by a		٥
Davropo 4 Health 45 Energy 25 Defetter 16	Mail -			C Nov			1-15 of 15 < >	¢٠	-	- L-	
Accuracy Det	COMPOSE		10 01	ransebooks are here - google	a convolutionation - Built for the web + 81	hour battery. Instant resume & 8 second	startup.	My the set			
Ban ta ban	Induce (8) Starved		0 * 1	Phil Sharp	Many San Francisco Mp - H g	ays: So for our weekend in San Francisco	. The been thinking about stuff to do .	2:25 pm	-	And a line of the second	
Cab is hars	Sect Mal			Peter Harbison	Halloween Plans - What are you p	lanning to do for Halloween? We should g	je to a costume party	2:23 pm			
Con to have	Drafts			YouTube	Your Personal YouTube Digest - O	et 10, 2011 - CHANGE EMAIL PREFERE	NCES You'lube Logo Your Personal	Oct. 10	- M	Adde New Installation	Pr Ante President Pre
Debadement.	> Hiking (2)		0 * 0	ne . Phil, Meredith (5)	Hilling To Dat Hille this weekeed	r - 1, great ideal I call sholgun in Peters -	our. On Mor. Oct 10, 2011 at 5:23 Ph.	Oct 10		Taken a	
SHEROME IN	Home To De (2)	а.		Paul McDonald	Fun Hike Yesterdayl - The	riks for the great hike yesterday, it was a	wesomel Let's go on another hike nex	Oct. 10	ter B	Advance Draw and Advance contracted	Br Mar
6776 (1976)	Urgent	э.		Jeff Wellington	Chromebook tips7-1)us	t got a Chromebook and I heard you were	an expert on the best web apps. Who	Oct 10		and and a	UT Note:
STAL	More -			Patier, me (2)	How are things going? - Things are	going great. Eve got three hikes planned	this weekend. On Mon, Oct 12, 2011	Oct 10		Diplut Nationary Gala, Gagia Editori	Sector of the se
	Chall			Samone Davids	Up for a concert Priday? - Write on	tling a big group logether to go to this cor	ncert and would lave to have you join.	Oct 10		No.	Contraction of the local division of the loc
14	Search people			Phil Sharp	Jast got my chromebook	d - This is the first email firs sending from	n my chromebook. Heve you thought c	Oct 19		Edge Imperial Internet and American American and American	D4
THE.	Set status here			Michael Bologning	Contract of the second designed a line real	in. I'm so pumped to hear about your new	buin bahima' Sounds like such a same	Oct 10		and a second	IN I
	Call phone			Meredith Blackwell		Her Jasen' I'm turning 25 a week from to		Oct 10	at heads	Colonation Ranager	Fue America
	- Jason			Phi Ship		get the assignment for last Priday's proje		Oct 10			T W Star
	Meredith			Alex, me (2)		colors this weekend 1. How does next w		Oct 10			

Browsers are the new operating systems



Browsers are the new operating systems





Protecting Web Users

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











- 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



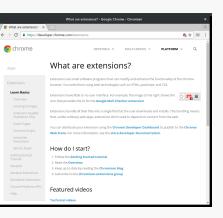


Outline

- 2 What are extensions: user perspective

Browser extensions

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





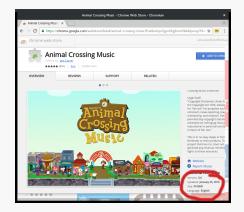
Browser extensions

- 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



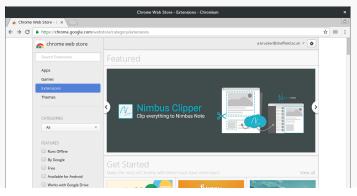




- Add-ons extending your browser
- Google says:
 - small software programs
 - little to no user interface
- What we find:
 complex and large programs
 - sophisticated user interfaces
- What extension can do:
 - modify the user interface (how your browser behaves)
 - modify web pages (what you see)
 -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



Let's search for a simple calculator



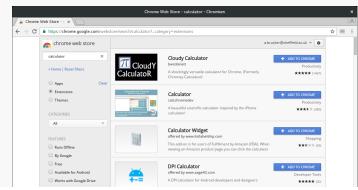
OWASP



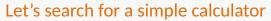
Let's search for a simple calculator



Let's search for a simple calculator



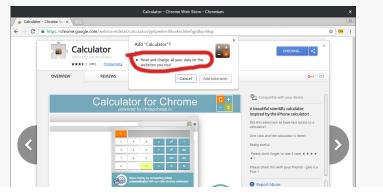








Let's search for a simple calculator

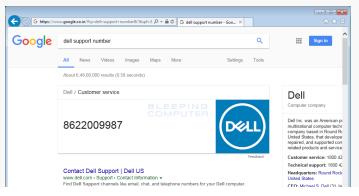


Let's search for a simple calculator





Malicious extensions are a real threat to users (1/2)





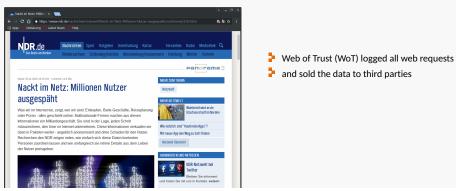
Malicious extensions are a real threat to users (1/2)



Current versions of Crusaders are installed on victims' computers via software bundles. Users

OWASP AppSec EU Belfas

Malicious extensions are a real threat to users (2/2)



Malicious extensions are a real threat to users (2/2)

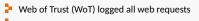


Web of Trust (WoT) logged all web requests



Malicious extensions are a real threat to users (2/2)





- and sold the data to third parties
- A German TV station bought the data



Malicious extensions are a real threat to users (2/2)



- 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 to users (2/2)



Tab

- 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 ÷ ...



Outline

- 3 What are extensions: developer perspective

The architecture of browser extensions

Tab DOM Scripts Textension Formssions Corrent Scripts Corrent Scripts Scrip	<pre>{ "update_url": "https://clients2.google.com/service/update2/ "name": "Test_Extension", "version": "0.1", "manifest_version": 2, "description": "This_uis_uauharmless_uextension", "permissions": ["tabs", "<all_urls>", "webRequest" }, "content_scripts": [{</all_urls></pre>
Operating System Native App Filesystem USB Camera	<pre>"background": { "scripts": ["background.js"] } }</pre>



Security mechanism: Permissions

Content Scripts

Black and white: either injecting script, or not

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

Outline

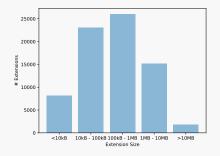
1 Motivation

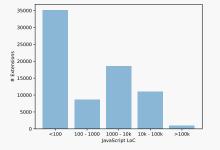
- 2 What are extensions: user perspective
- 3 What are extensions: developer perspective
- 4 Little shop of horrors
- 5 Outlook

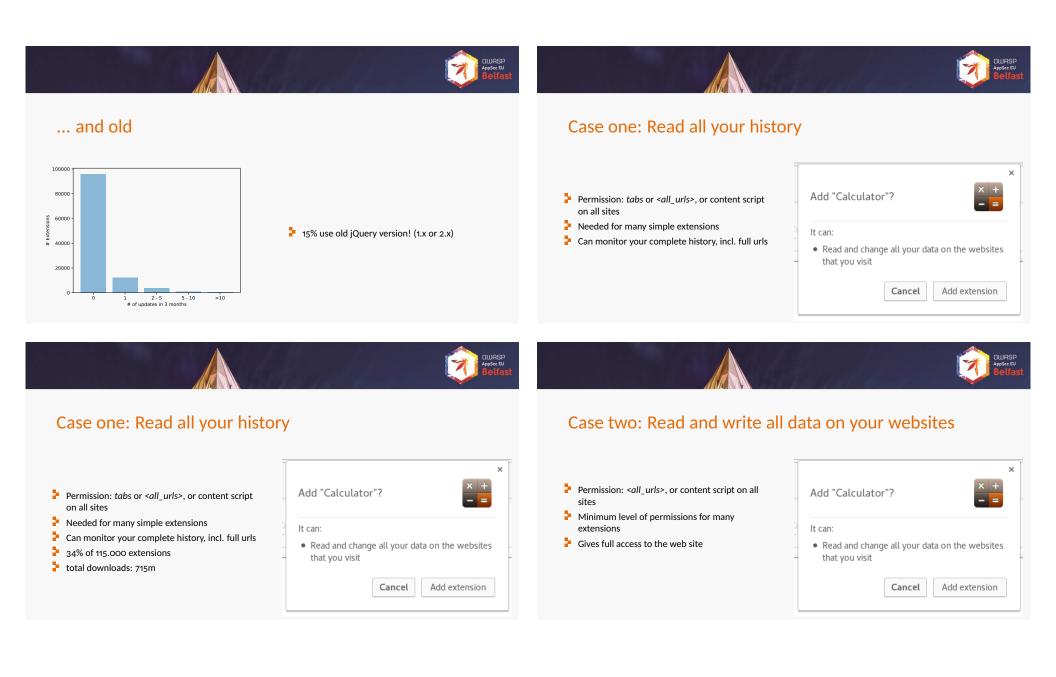
Chrome Web Store

chrome web store Main way of distributing extensions We monitored 115k extensions over 3 months Wide variety of categories: productivity 29.29% fun 11.65% communication 10.24% web_development 9.15% games 7.52% accessibility 7.22%

Extensions are big ...



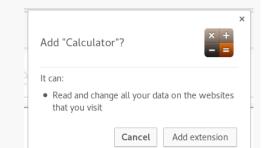






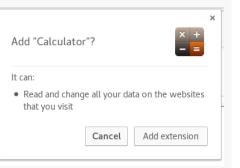
Case two: Read and write all data on your websites

- Permission: <all_urls>, or content script on all sites
- Minimum level of permissions for many extensions
- Gives full access to the web site
- 21% of 115.000 extensions
- total downloads: 615m



Case three: Circumvent security measures

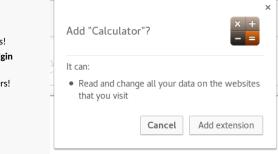
- Permission: <all_urls> and webRequest
- Can intercept and change all HTTP headers!
- Disable Content-Security-Policy, Same-origin Policy, etc.
- Breaks security guarantees of web browsers!



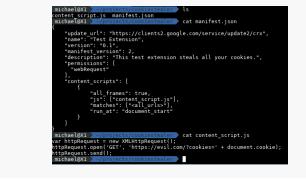
OWASP AppSec EU Belfast

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!
- 6% of 115.000 extensions
- total downloads: 325m



It's that easy...





OWASP AppSec EU



- 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?



Integrity: content modifications layout modifications

- Confidentiality: data storagetransmitted 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)

Outlook: On the short term (2/2)





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).

Be aware of the risk

Check the vendor of the extension carefully

Check the permissions (i.e., active domains)

Use browser profiles





Thank you for your attention! Any questions or remarks?

Contact:

Dr. Achim D. Brucker and Michael Herzberg Department of Computer Science University of Scheffield Regent Court 211 Portobello St. Sheffield S1 40P, UK