The Evil Friend in Your Browser

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

OWASP Benelux-Day
November 24, 2017
Tilburg, The Netherlands

Outline

- Motivation
- What are extensions: user perspective
- What are extensions: developer perspective
- Real world extensions
- Outlook

Browsers are the new operating systems

Google Chrome
Please close all Google Chrome windows and try again.

OK
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
  - 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

Outline

- **Motivation**
- **What are extensions: user perspective**
- **What are extensions: developer perspective**
- **Real world extensions**
- **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

- 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
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 (2/2)

- Adware replaces phone numbers for security firms returned in search results

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 Extension.
Malicious extensions are a real threat (2/2)

Browser Bully? Malicious Google Chrome Extension Pushes User Buttons

Malicious extensions are a real threat (2/2)

Forced into installing a Chrome extension

Forced into installing a Chrome extension
Malicious extensions are a real threat (2/2)
The architecture of browser extensions

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
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 1.88%

Our "Big Data" extension archive

Daily snapshots of over 125'000 artifacts
Over 3TB in size
Over 23GB JavaScript (over 3'9 billion LOC)

Download numbers

Extensions can be big
Observe our browsing behaviour

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

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!
Mining Monero (an AltCoin – think Bitcoin)

First extension:
- Large press coverage
- Less than 24 hours in Chrome store (before removed by Google)

Two days after press releases:
- At least 16 other mining extensions
- Most of them seemed un-maintained
- Updates to permissions (required by the mining code)
- Different wallets, but extensions from same author use same wallet

Dynamic Analysis for Detecting Privacy Violations

Our Dynamic analysis detected extensions that:
- inject benign analytics in all websites
- monitor the complete browsing behavior
- can observe all data entered into websites

In total:
- Running each extensions on 10 websites
- 18 extensions use this attack (over 250k users affected)
**Outline**

- Motivation
- What are extensions: user perspective
- What are extensions: developer perspective
- Real world extensions
- Outlook

---

**How can we make web browsing great* again?**

- **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...

---

*great = ensuring the security, integrity, and privacy of the user of a web browser*
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:
Department of Computer Science
University of Sheffield
Regent Court
311 Portobello St.
Sheffield S1 4DP, UK