Intercepting Suspicious Chrome Extension Actions

Michael Cypher

Department of Computing
Imperial College London

June 26, 2017

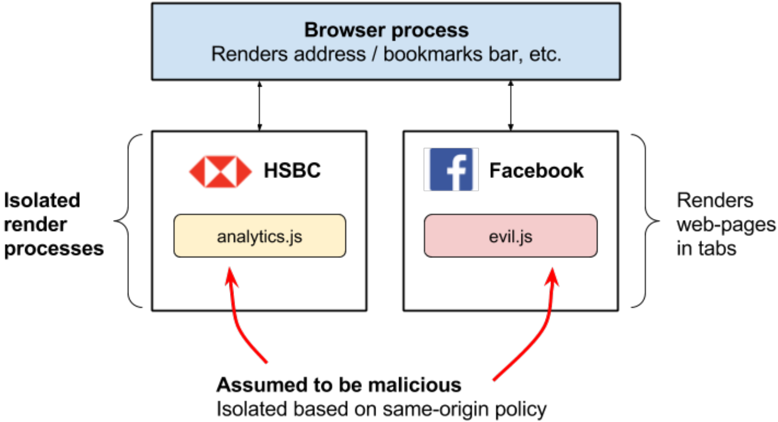
Chrome Browser

User Usage

Most popular desktop browser (62%) and browser in general (52%) and is used to execute **sensitive web applications**

Chrome Browser

Multi-process Architecture


Browser process
Renders address / bookmarks bar, etc.
Isolated render processes
HSBC
analytics.js
Facebook
evil.js
Renders web-pages in tabs
Assumed to be malicious
Isolated based on same-origin policy

Chrome Extensions

The same-origin policy prevents attackers from executing arbitrary code on web-pages, right?

Chrome Extensions

The same-origin policy prevents attackers from executing arbitrary code on web-pages, right? **Not if they're extensions!**

Chrome Extensions

The same-origin policy prevents attackers from executing arbitrary code on web-pages, right? **Not if they're extensions!**

Extensions

- can execute content scripts on pages (if granted permission by users)

Chrome Extensions

The same-origin policy prevents attackers from executing arbitrary code on web-pages, right? **Not if they're extensions!**

Extensions

- can execute content scripts on pages (if granted permission by users)
- have access powerful Chrome extension APIs

Chrome Extensions

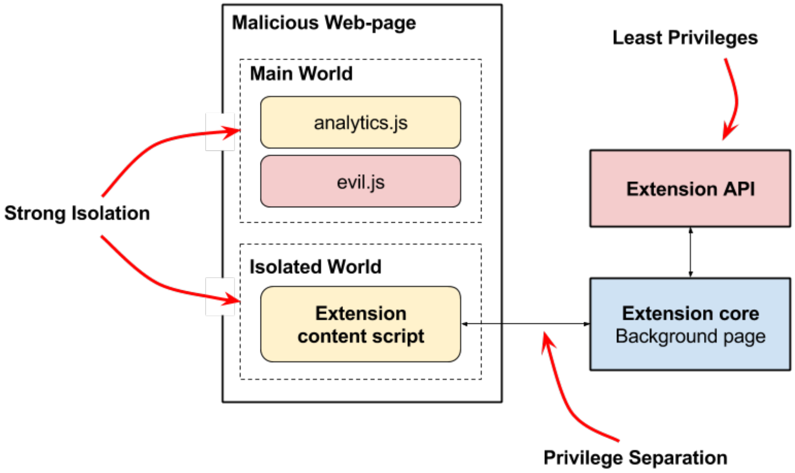
The same-origin policy prevents attackers from executing arbitrary code on web-pages, right? **Not if they're extensions!**

Extensions

- can execute content scripts on pages (if granted permission by users)
- have access powerful Chrome extension APIs
- are assumed to be **benign-but-buggy** and **not malicious**!

Extension System Architecture

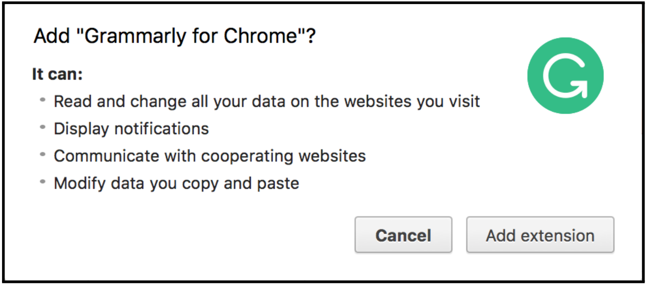
Security Model



Malicious Extensions

Permission model does not protect users from malicious extensions!

- Malicious extensions may provide useful functionality



Add "Grammarly for Chrome"?

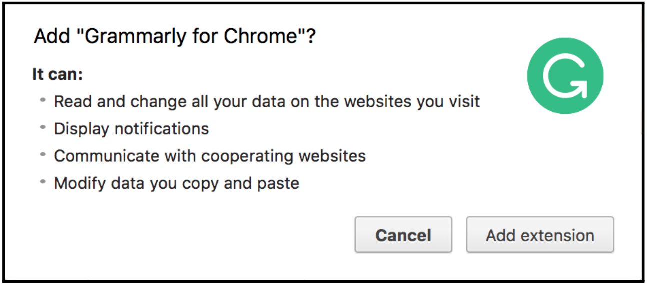
It can:

- Read and change all your data on the websites you visit
- Display notifications
- Communicate with cooperating websites
- Modify data you copy and paste

Malicious Extensions

Permission model does not protect users from malicious extensions!

- Malicious extensions may provide useful functionality
- Content scripts can carry out attacks using standard Web APIs



Add "Grammarly for Chrome"?

It can:

- Read and change all your data on the websites you visit
- Display notifications
- Communicate with cooperating websites
- Modify data you copy and paste

Several threats are widespread on Chrome Web Store

1. **Facebook hijacking** present in 4,809 extensions (2012 - 2015)

Malicious Extensions

Threats

Several threats are widespread on Chrome Web Store

1. **Facebook hijacking** present in 4,809 extensions (2012 - 2015)
2. **Ad Injection** present in 3,496 extensions

Malicious Extensions

Threats

Several threats are widespread on Chrome Web Store

1. **Facebook hijacking** present in 4,809 extensions (2012 - 2015)
2. **Ad Injection** present in 3,496 extensions
3. **User Tracking**

Malicious Extensions

Threats

Several threats are widespread on Chrome Web Store

1. **Facebook hijacking** present in 4,809 extensions (2012 - 2015)
2. **Ad Injection** present in 3,496 extensions
3. **User Tracking**

Google automatically analyzes extensions for malice in sandboxes before publishing them but **provides no guarantees**

Project Goals

1. Protect users from malicious extensions and provide security guarantees

Project Goals

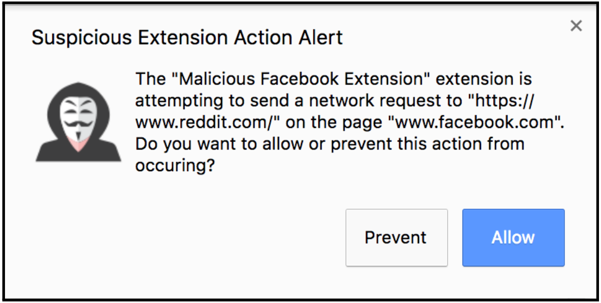
1. Protect users from malicious extensions and provide security guarantees
2. Break minimal benign web applications and extensions

Project Goals

1. Protect users from malicious extensions and provide security guarantees
2. Break minimal benign web applications and extensions
3. Not incur a significant performance overhead

Intercepting Suspicious Chrome Extension Actions

Our approach... **Analyze extension behaviour at run-time and ask users to allow or prevent suspicious actions!**



Suspicious Extension Action Alert

The "Malicious Facebook Extension" extension is attempting to send a network request to "https://www.reddit.com/" on the page "www.facebook.com". Do you want to allow or prevent this action from occuring?

Project challenges

- What extension actions do we consider suspicious?
- Differentiating between extension actions and other script actions
- Improving user experience and suspicious action classification

Suspicious Actions

Focus on **content script operations** and add permissions around **standard Web APIs** that harm users

- `EventTarget.click()`

Suspicious Actions

Focus on **content script operations** and add permissions around **standard Web APIs** that harm users

- `EventTarget.click()`
- `Node.appendChild()` (45% of malware)

Suspicious Actions

Focus on **content script operations** and add permissions around **standard Web APIs** that harm users

- `EventTarget.click()`
- `Node.appendChild()` (45% of malware)
- `XMLHttpRequest.send()` (52% of malware)

Suspicious Actions

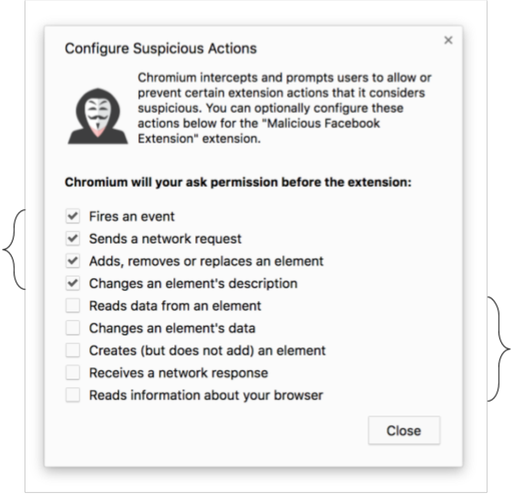
Focus on **content script operations** and add permissions around **standard Web APIs** that harm users

- `EventTarget.click()`
- `Node.appendChild()` (45% of malware)
- `XMLHttpRequest.send()` (52% of malware)

Filter out benign events, or operations on elements not attached to DOM.

Suspicious Actions

Configuring Suspicious Actions



Configure Suspicious Actions

Chromium intercepts and prompts users to allow or prevent certain extension actions that it considers suspicious. You can optionally configure these actions below for the "Malicious Facebook Extension" extension.

Chromium will your ask permission before the extension:

- ☑ Fires an event
- ☑ Sends a network request
- ☑ Adds, removes or replaces an element
- ☑ Changes an element's description
- □ Reads data from an element
- □ Changes an element's data
- □ Creates (but does not add) an element
- □ Receives a network response
- □ Reads information about your browser

Default suspicious actions

Required for top 3 threats

Possible suspicious actions

Could harm users

Project challenges

- What extension actions do we consider suspicious?
- Differentiating between extension actions and other script actions
- Improving user experience and suspicious action classification

Detecting Extension Actions

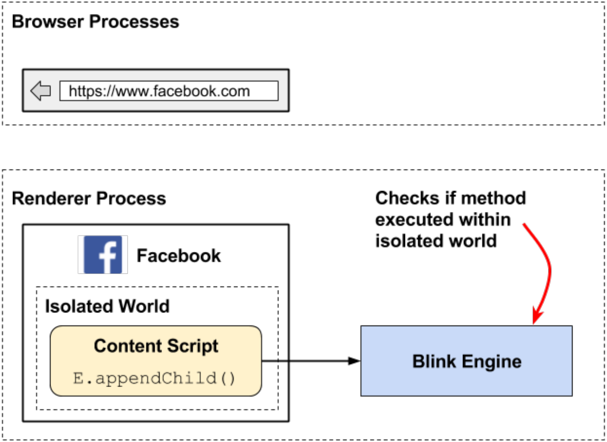
Alternatives

Neither approach provides security guarantees

- Measuring the ordering and frequency of events
- Transforming content script JavaScript to taint methods

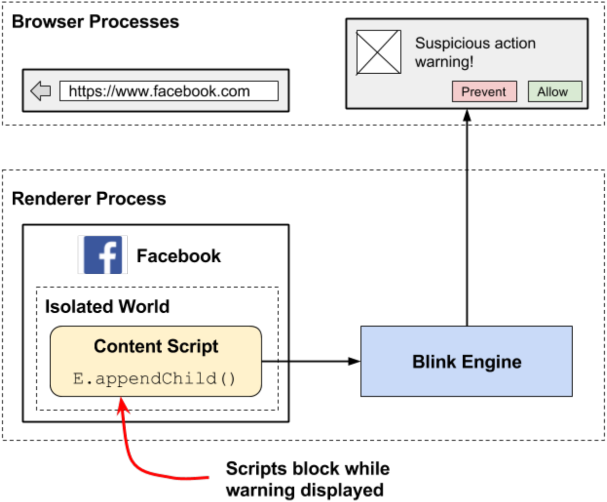
Detecting Extension Actions

Using the Isolated World



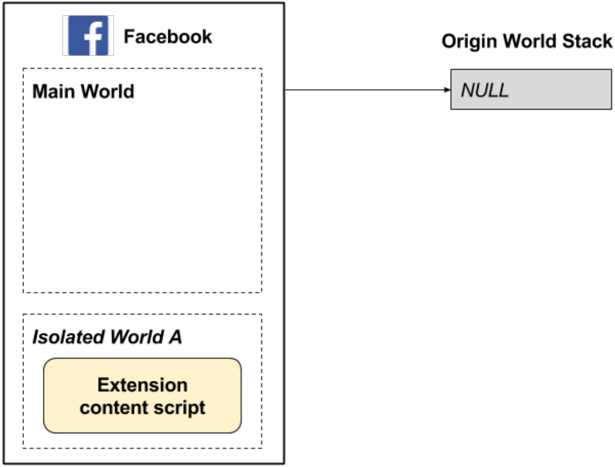
Detecting Extension Actions

Using the Isolated World



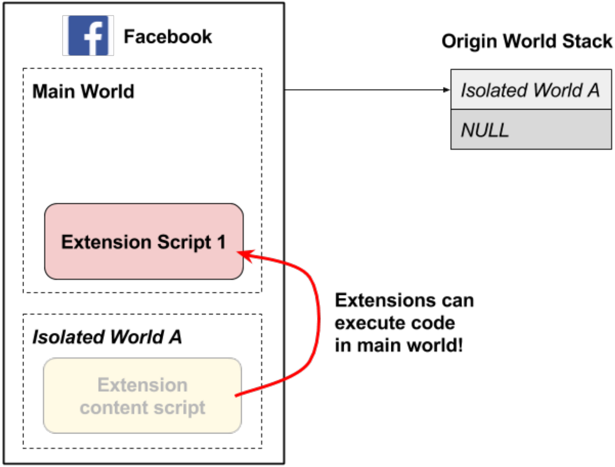
Script Injection

Executing Scripts in the Main World



Script Injection

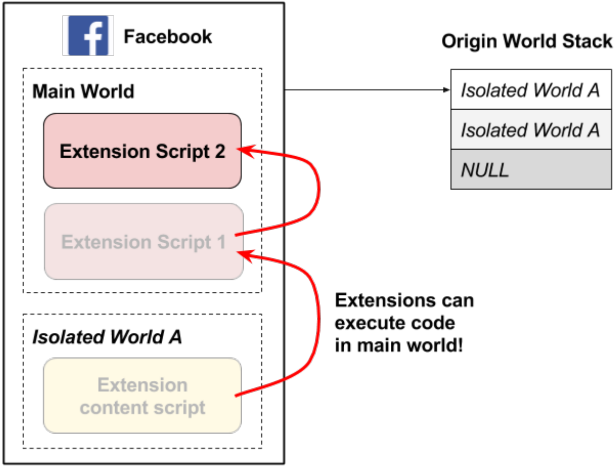
Executing Scripts in the Main World



Extensions can execute code in main world!

Script Injection

Executing Scripts in the Main World



Project challenges

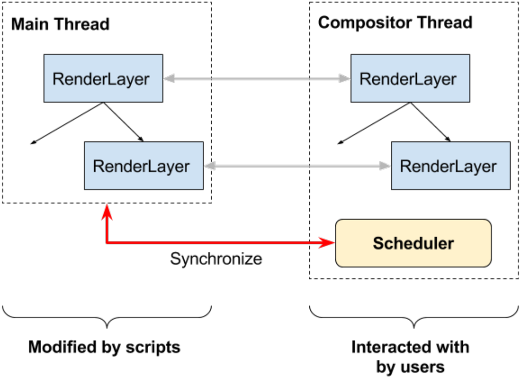
- What extension actions do we consider suspicious?
- Differentiating between extension actions and other script actions
- Improving user experience and suspicious action classification

Describing Suspicious Actions

Improving User Experience

Users need to be able to correctly classify suspicious actions

- Let web-pages describe elements themselves
- **Highlight** or **scroll** to element under question

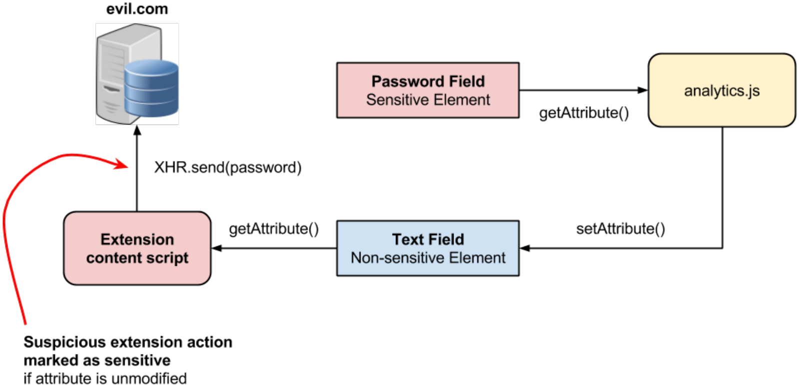


Sensitive Attributes

Improving User Experience

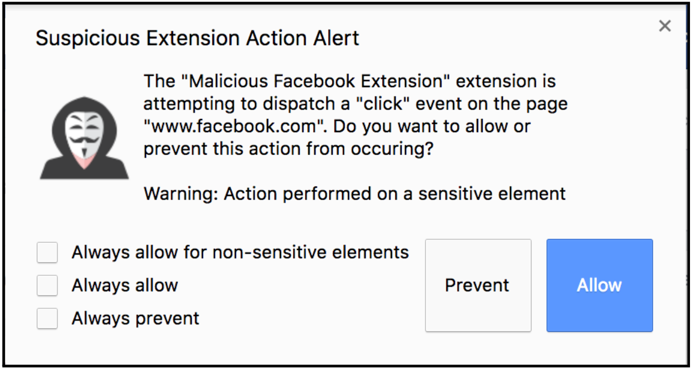
Let web-pages taint elements as sensitive

- Warn users of operations on sensitive elements
- **Precise sensitive data flow tracking**



Remembering User Decisions

Improving User Experience



Suspicious Extension Action Alert

The "Malicious Facebook Extension" extension is attempting to dispatch a "click" event on the page "www.facebook.com". Do you want to allow or prevent this action from occuring?

Warning: Action performed on a sensitive element

☐ Always allow for non-sensitive elements

☐ Always allow

☐ Always prevent

Security Guarantees

Results

- **Guarantee** we alert users if an extension executes a suspicious action!

Security Guarantees

Results

- **Guarantee** we alert users if an extension executes a suspicious action!
- But **security relies on users** correctly classifying malicious actions

Security Guarantees

Results

- **Guarantee** we alert users if an extension executes a suspicious action!
- But **security relies on users** correctly classifying malicious actions
- **False negatives = attacks made possible**

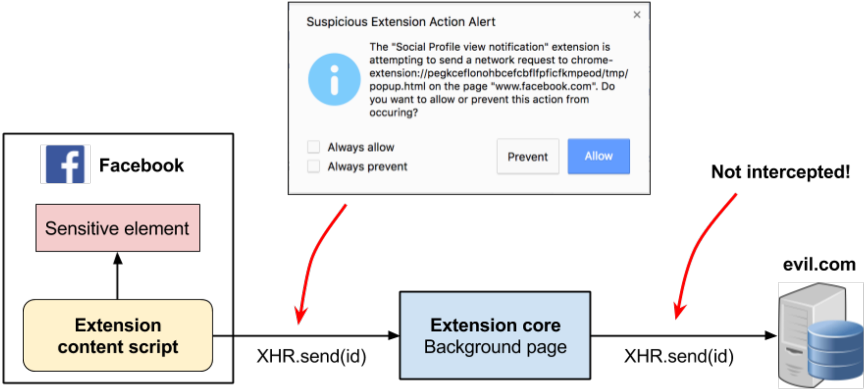
Security Guarantees

Results

- **Guarantee** we alert users if an extension executes a suspicious action!
- But **security relies on users** correctly classifying malicious actions
- **False negatives = attacks made possible**
- **False positives = benign extensions may break**

Discovered Malicious Extension

Leaked sensitive data to third-party



Suspicious Extension Action Alert

The "Social Profile view notification" extension is attempting to send a network request to chrome-extension://pegkceflonohbcefcbflfpficfkmpeod/tmp/popup.html on the page "www.facebook.com". Do you want to allow or prevent this action from occuring?

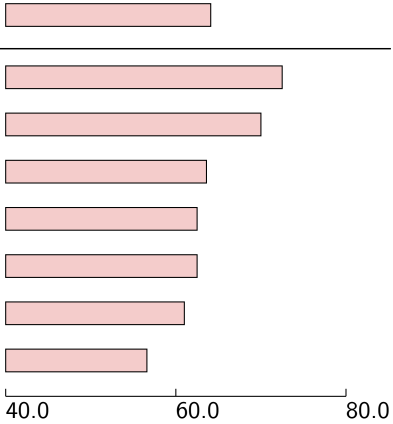
□ Always allow

□ Always prevent

User Experience Survey

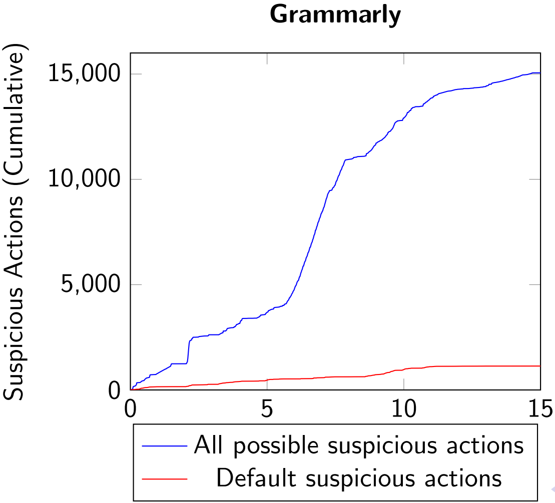
Results

Action Group	Size	Prevented (%)	Bar Chart: Prevented (%)
Total	839	64.1	
Change Attr	120	72.5	
Event	80	70.0	
DOM	280	63.6	
Request	80	62.5	
Response	80	62.5	
Create	100	61.0	
Read Attr	99	56.6	



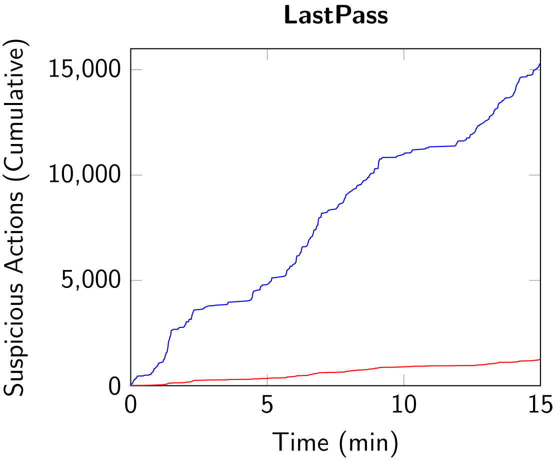
Suspicious Actions Triggered By Popular Benign Extensions

The quantity of suspicious actions executed during 15 minutes of extension use



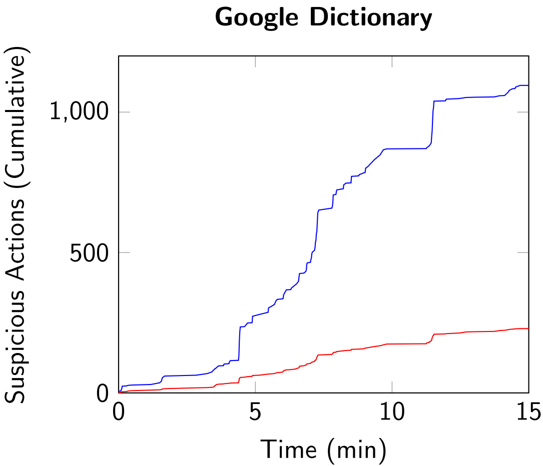
Suspicious Actions Triggered By Popular Benign Extensions

The quantity of suspicious actions executed during 15 minutes of extension use



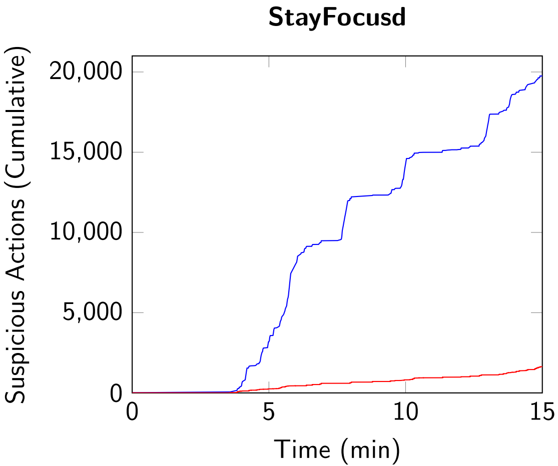
Suspicious Actions Triggered By Popular Benign Extensions

The quantity of suspicious actions executed during 15 minutes of extension use



Suspicious Actions Triggered By Popular Benign Extensions

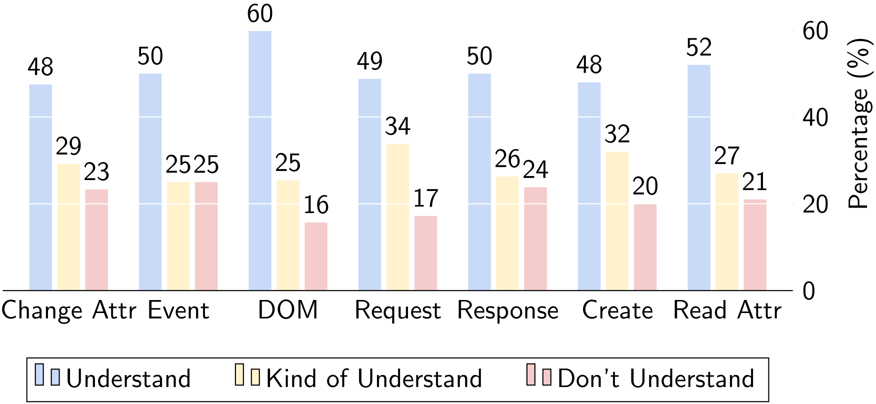
The quantity of suspicious actions executed during 15 minutes of extension use



User Experience Survey

Results

Do users understand suspicious extension action pop-ups?



Performance Impact

Results

Modified browser sometimes has significant performance overhead

- **DOM:** 50%, 380% increase when creating elements, setting attributes

Performance Impact

Results

Modified browser sometimes has significant performance overhead

- **DOM:** 50%, 380% increase when creating elements, setting attributes
- **Events:** 70% increase when dispatching click events

Demonstration and Questions

For Further Reading I

N. Jagpal, E. Dingle, J. P. Gravel, P. Mavrommatis, N. Provos, M. A. Rajab and K. Thomas
Trends and Lessons from Three Years Fighting Malicious Extensions
Proceedings of the USENIX Security Symposium, 2015.

A. Kapravelos, C. Grier, N. Chachra, C. Kruegel, G. Vigna and V. Paxson
Hulk: Eliciting malicious behavior in browser extensions
Proceedings of the USENIX Security Symposium, 2014.

Top 9 Browsers
StatCounter 2017.

Telemetry Benchmarking

DOM Operations

Name	Original Browser	Modified Browser	
	Avg (ms)	Avg (ms)	Δ Avg (%)
modify-element-classname	4,489.4 ± 42.0	4,797.5 ± 100.4	+6.9
addRange	3,821.9 ± 13.8	3,852.6 ± 21.1	+0.8
modify-element-id	1,720.3 ± 11.6	1,764.1 ± 10.1	+2.5
modify-element-title	1,499.8 ± 11.1	1,512.1 ± 7.3	+0.8
select-multiple-add	141.3 ± 0.9	70.9 ± 0.5	-49.9
remove_child_with_selection	57.6 ± 0.7	140.8 ± 1.2	+144.6
select-single-add	26.0 ± 0.1	21.5 ± 0.1	-17.2
inner_html_with_selection	24.5 ± 0.6	24.9 ± 0.6	+1.2
select-long-word	14.4 ± 0.3	14.4 ± 0.2	-0.1
long-sibling-list	13.9	12.0 ± 0.1	-13.7
select-single-remove	8.5 ± 0.1	6.1	-28.0
textarea-dom	3.4	3.0	-14.0
div-editable	0.3	0.2	-4.7
textarea-edit	0.2	0.2	-3.5

Telemetry Benchmarking

Events

Name	**Original Browser**	**Modified Browser**	
	Avg (ms)	Avg (ms)	Δ Avg (%)
...ShadowTrees	601.9 ± 2.9	579.5 ± 13.0	-3.7
...DeeplyNestedShadowTrees	235.3 ± 0.9	233.3 ± 0.9	-0.8
EventsDispatching	25.2 ± 0.1	20.3 ± 0.1	-19.3
SimpleClickDispatch	56.2 ± 0.7	95.3 ± 0.9	+69.5

Telemetry Benchmarking

Network Requests

Name	Original Browser	Modified Browser	
	Avg (ms)	Avg (ms)	Δ Avg (%)
send	1,173.8 ± 57.1	1,208.5 ± 59.2	+3.0
read-response	1,208.1 ± 56.0	1,245.5 ± 56.1	+3.1