CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

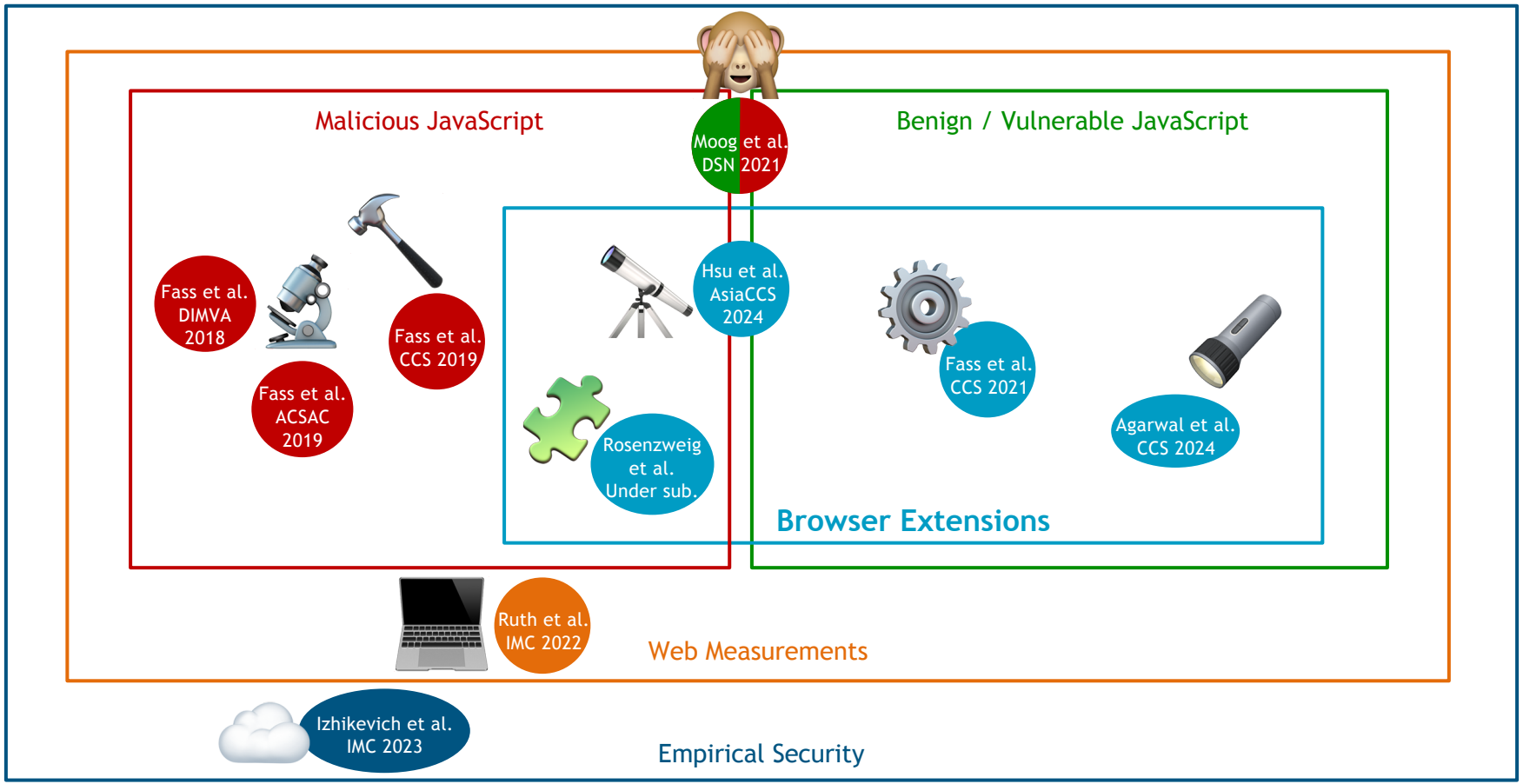
Browser Extension (In)Security

Aurore Fass

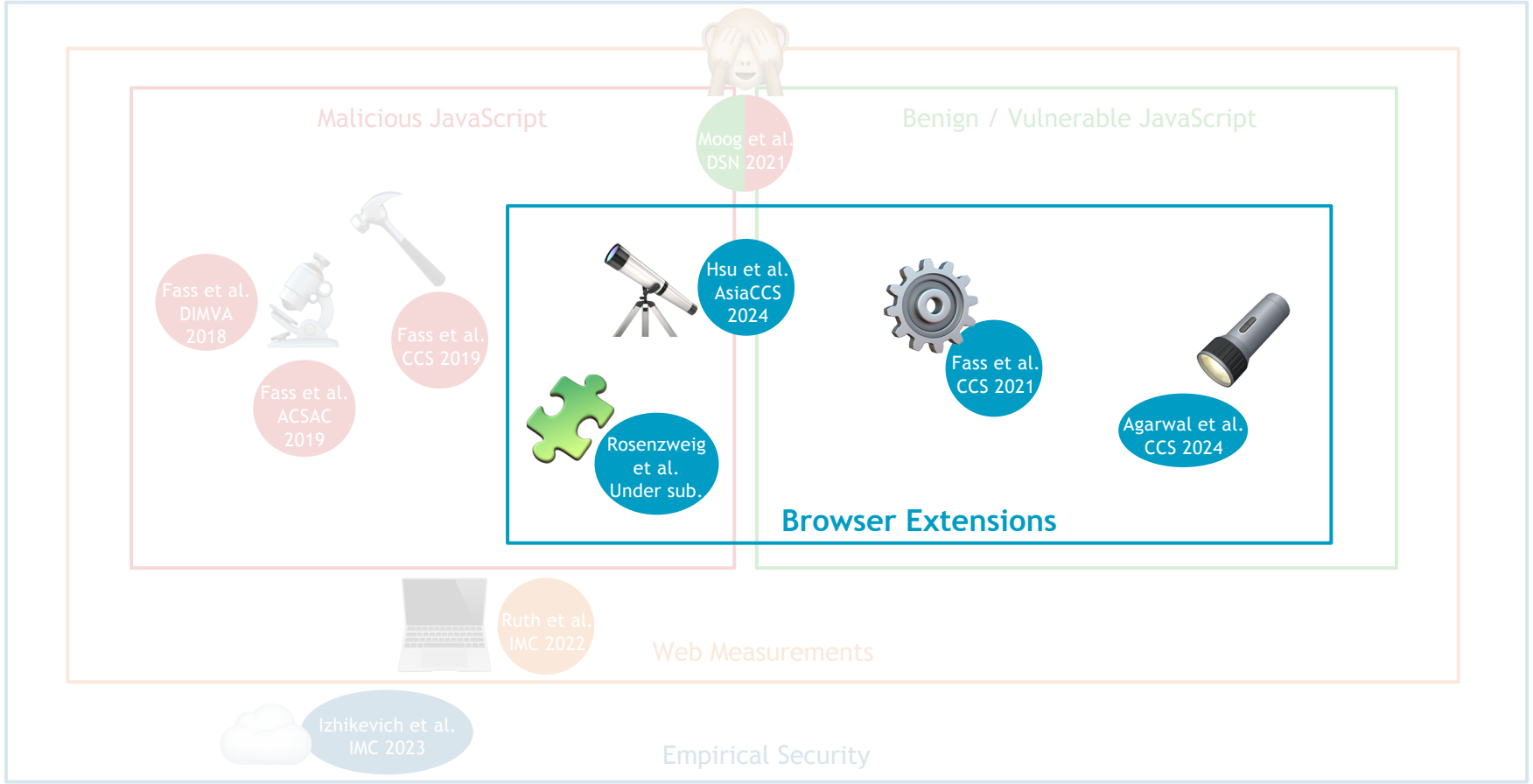
Tenure-Track Faculty at CISPA — Helmholtz Center for Information Security

GDR Sécurité Informatique, Rennes, June 11th, 2024

Research Work



Research Work



What are Browser Extensions?

- Third-party programs to **improve user browsing experience**

AdBlock — best ad blocker

Offered by: getadblock.com

Adblock Plus - free ad blocker

Offered by: adblockplus.org

Adobe Acrobat

Offered by: Adobe Inc.

Avast Online Security

Offered by: https://www.avast.com

Cisco Webex Extension

Offered by: webex.com

Google Translate

Offered by: translate.google.com

Grammarly for Chrome

Offered by: grammarly.com

Honey

Offered by: https://www.joinhoney.com

Pinterest Save Button

Offered by: pinterest.com

Skype

Offered by: www.skype.com

uBlock Origin

Offered by: Raymond Hill (gorhill)

LastPass: Free Password Manager

Offered by: LastPass

- **125k** Chrome extensions totaling over **1.6B** active users

How Safe are Browser Extensions?

- Browser extensions provide additional functionality…

- … so browser extensions need additional & elevated privileges compared to web pages

➢ Browser extensions are an attractive target for attackers 😈

Security-Noteworthy Extensions (SNE)

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

→ Extensions can put their users' security & privacy at risk

- **Contain malware**
  - Designed by malicious actors to harm victims
  - E.g., propagate malware, steal users' credentials, track users
- **Violate the Chrome Web Store policies**
  - E.g., deceive users, promote unlawful activities, lack a privacy policy
- **Contain vulnerabilities**
  - Designed by well-intentioned developers… but contain some vulnerabilities
  - E.g., can lead to user-sensitive data exfiltration

Did you know that…

- **350M users** installed **Security-Noteworthy Extensions** in the last 3 years?

- These **dangerous extensions** stay in the Chrome Web Store ***for years***?

- **60%** of extensions have **never received a single update**?

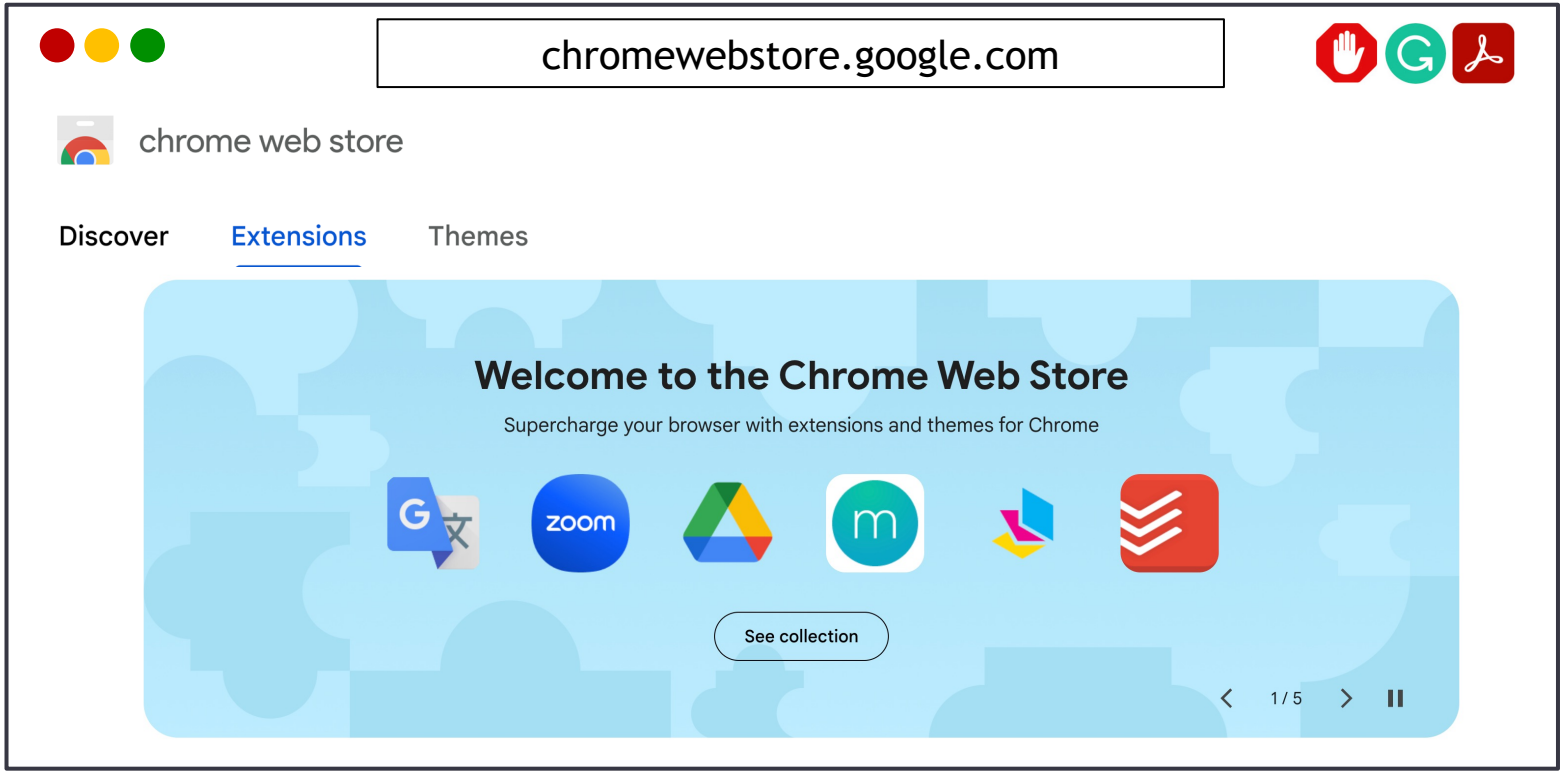

What is in the Chrome Web Store?
Sheryl Hsu, Stanford University
Manda Tran, Stanford University
Aurore Fass, Stanford University, CISPA Helmholtz Center for Information Security

> What is in the Chrome Web Store?

Hsu et al. AsiaCCS 2024

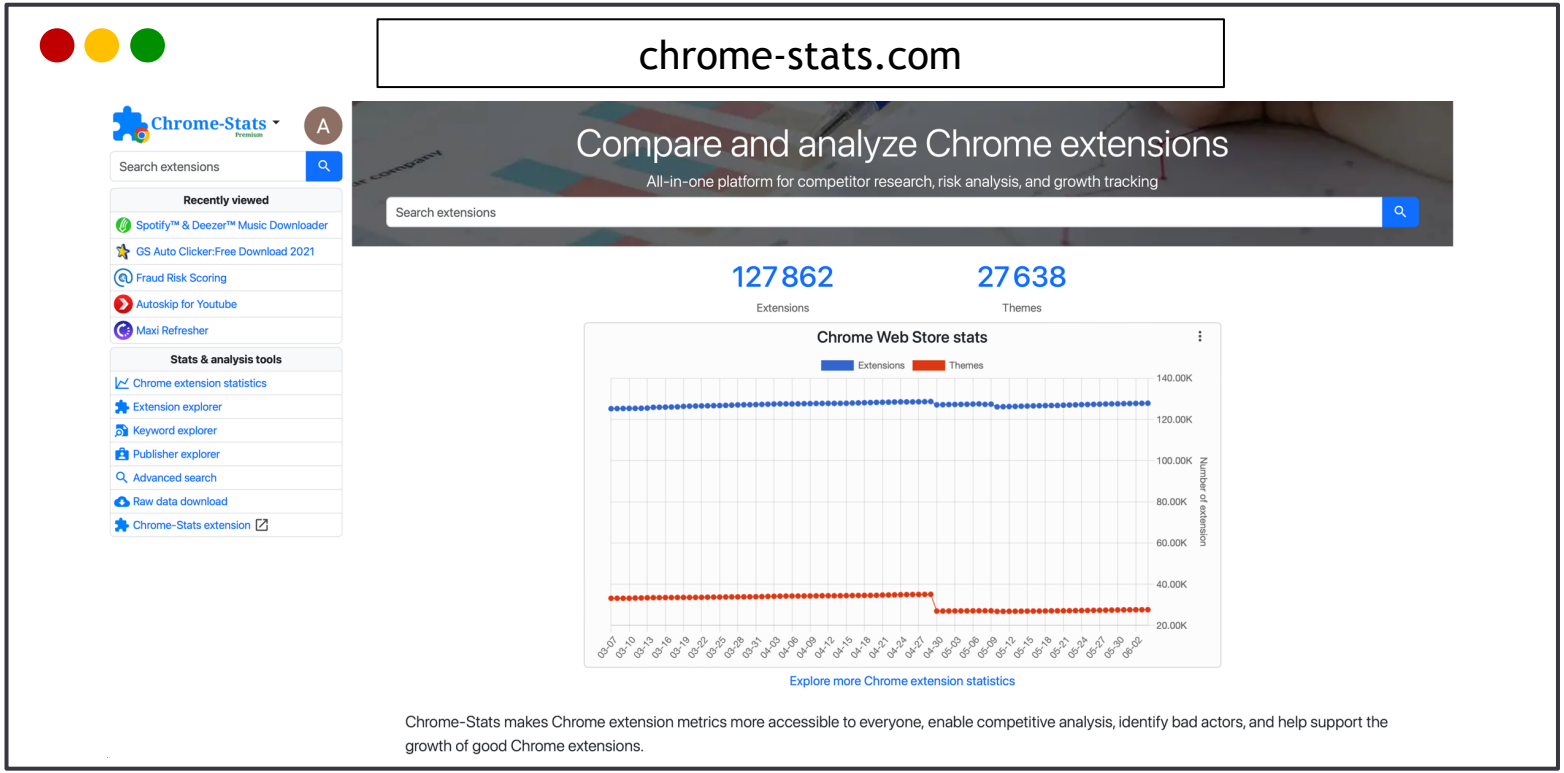
In *ACM AsiaCCS* 2024. Sheryl Hsu, Manda Tran, and Aurore Fass

How to Install Extensions or SNE?

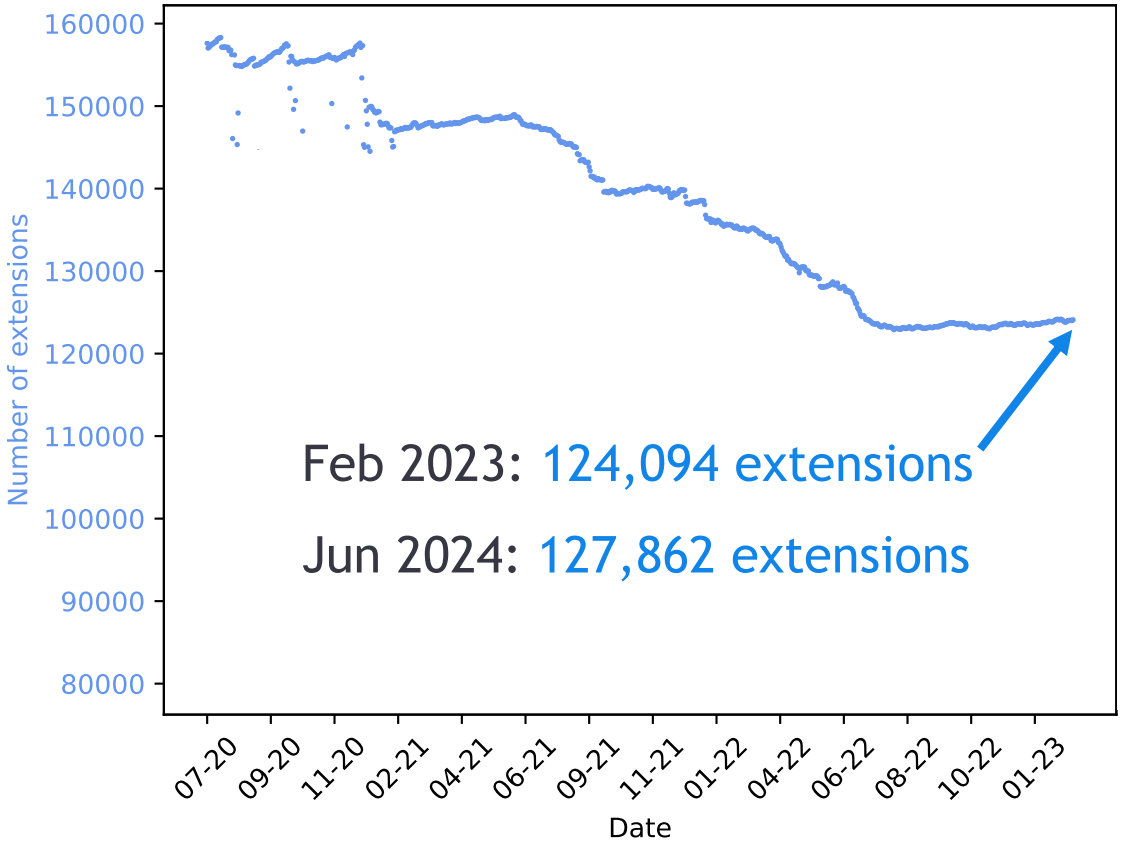


How to Install Extensions or SNE?

Browser Extension Collection: Chrome-Stats



Number of Extensions in the Chrome Web Store

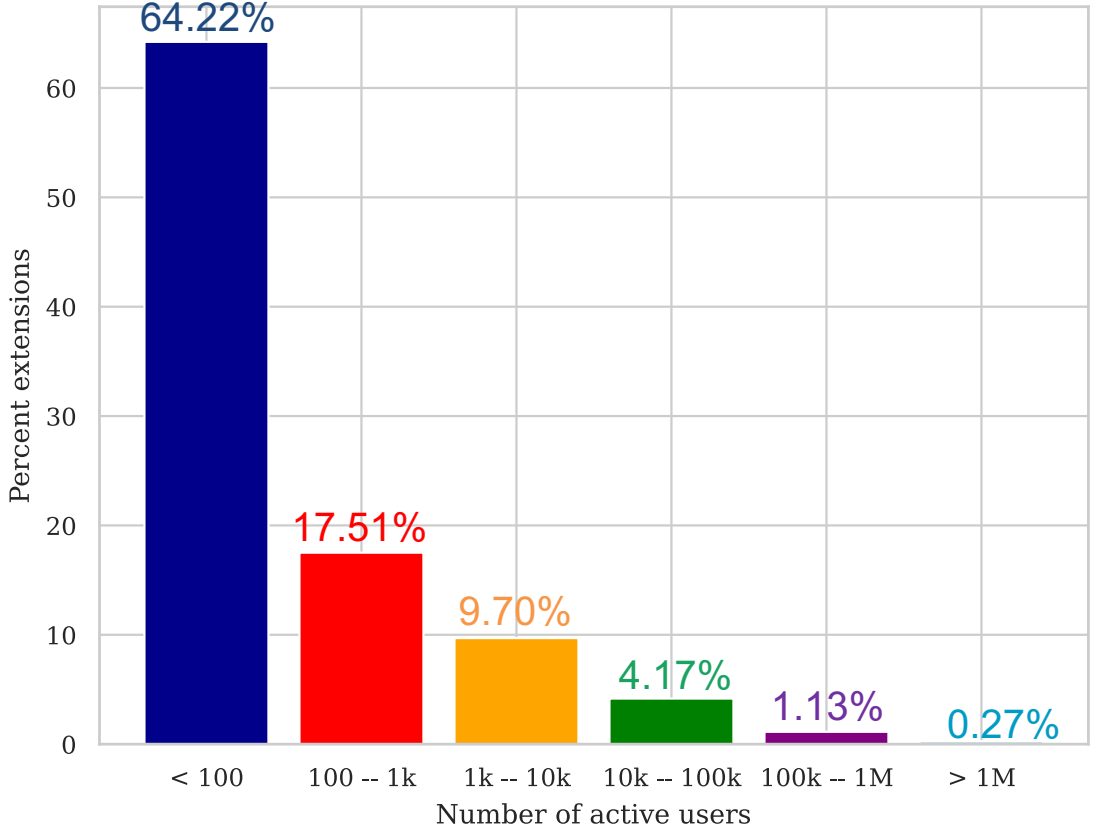


Every month:

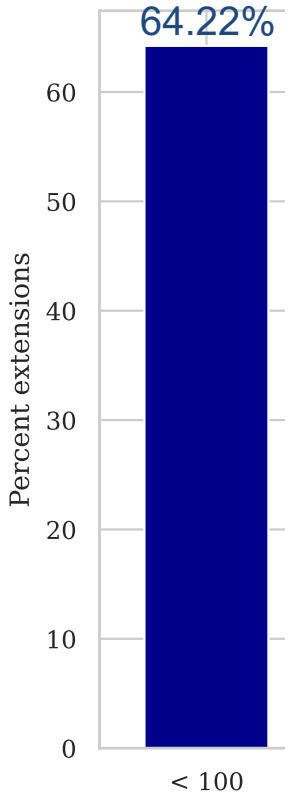
- -3,775 extensions removed
- +2,687 extensions added

➢ Analyses on the CWS should be **run regularly**

Breakdown of Extension Users



Breakdown of Extension Users



- > 1M users: 500 extensions
- > 10M users: 34 extensions

Extension Users

The "**number of users**" on the CWS for a given extension corresponds to:

> *"the number of Chromes with the extension installed that are active and checking in to [their] update servers over the previous seven days only, not for all time. It is not equal to the sum of historic installs minus the sum of historic uninstalls"*

~ Chrome Web Store Developer Support

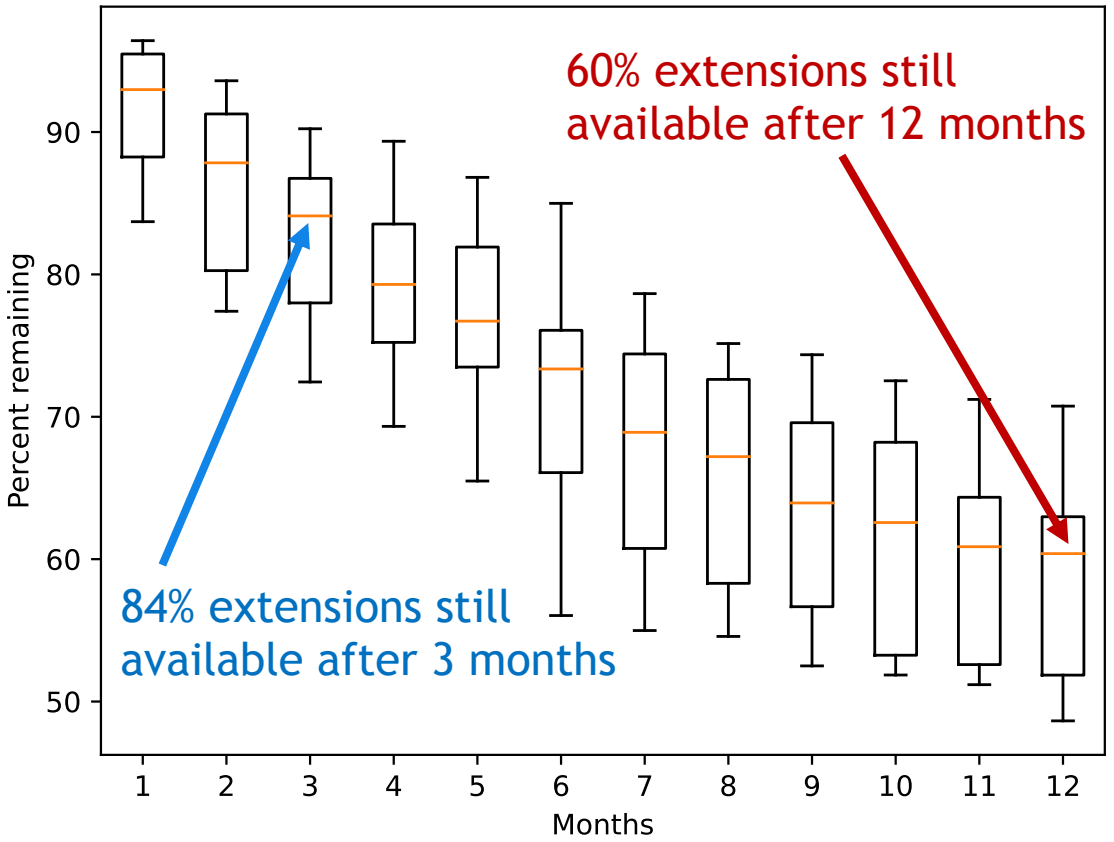
Life Cycle of Extensions

Methodology:

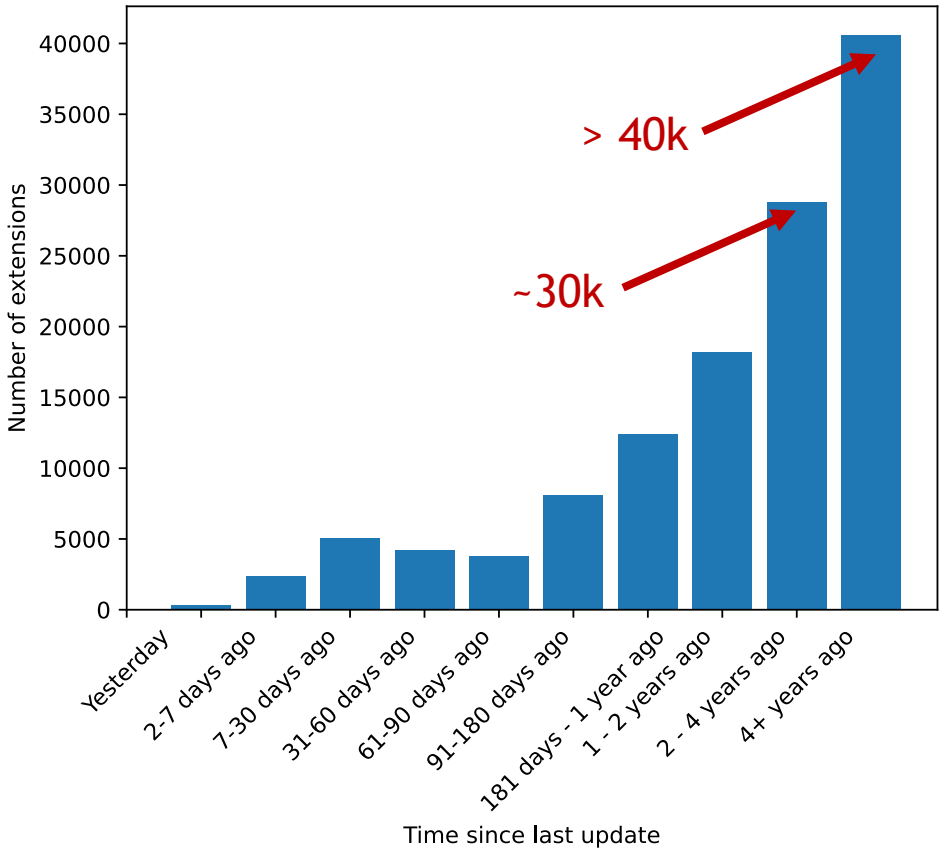
- Collected extensions added to the CWS in Jan—Dec 2021
- Computed the percentage of those extensions still in the CWS 1, 2, …, 12 months later

➢ **Extensions have a very short life cycle**

➢ Analyses on the CWS should be **run regularly**

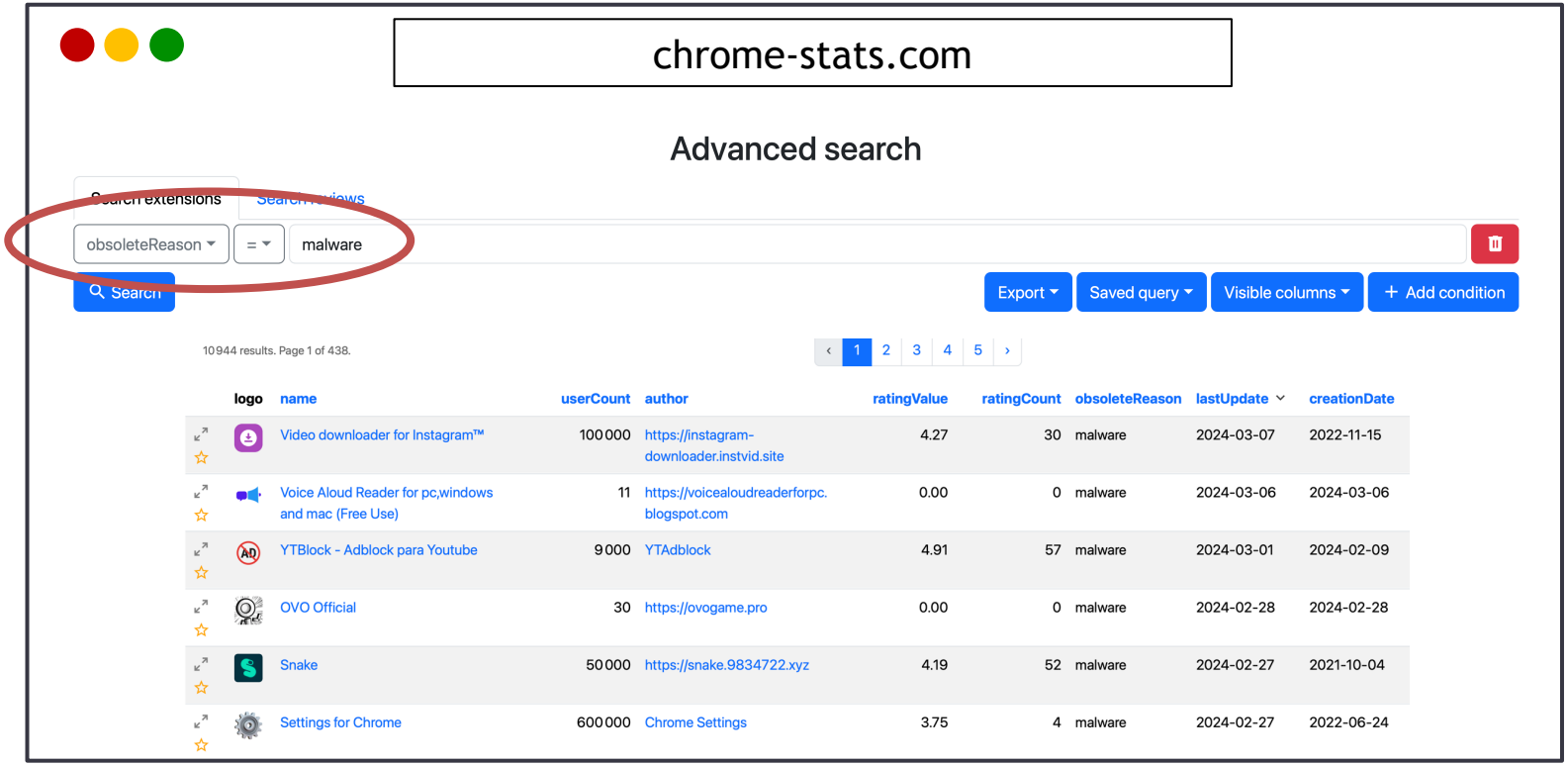


Extension Maintenance and Security



- Critical **lack of maintenance** in the CWS
- **60%** of the extensions have **never been updated**
- Security & privacy implications

Malicious Extension Collection: Chrome-Stats



logo	name	userCount	author	ratingValue	ratingCount	obsoleteReason	lastUpdate	creationDate
	Video downloader for Instagram™	100000	https://instagram-downloader.instvid.site	4.27	30	malware	2024-03-07	2022-11-15
	Voice Aloud Reader for pc,windows and mac (Free Use)	11	https://voicealoudreaderforpc.blogspot.com	0.00	0	malware	2024-03-06	2024-03-06
	YTBlock - Adblock para Youtube	9000	YTAdblock	4.91	57	malware	2024-03-01	2024-02-09
	OVO Official	30	https://ovogame.pro	0.00	0	malware	2024-02-28	2024-02-28
	Snake	50000	https://snake.9834722.xyz	4.19	52	malware	2024-02-27	2021-10-04
	Settings for Chrome	600000	Chrome Settings	3.75	4	malware	2024-02-27	2022-06-24

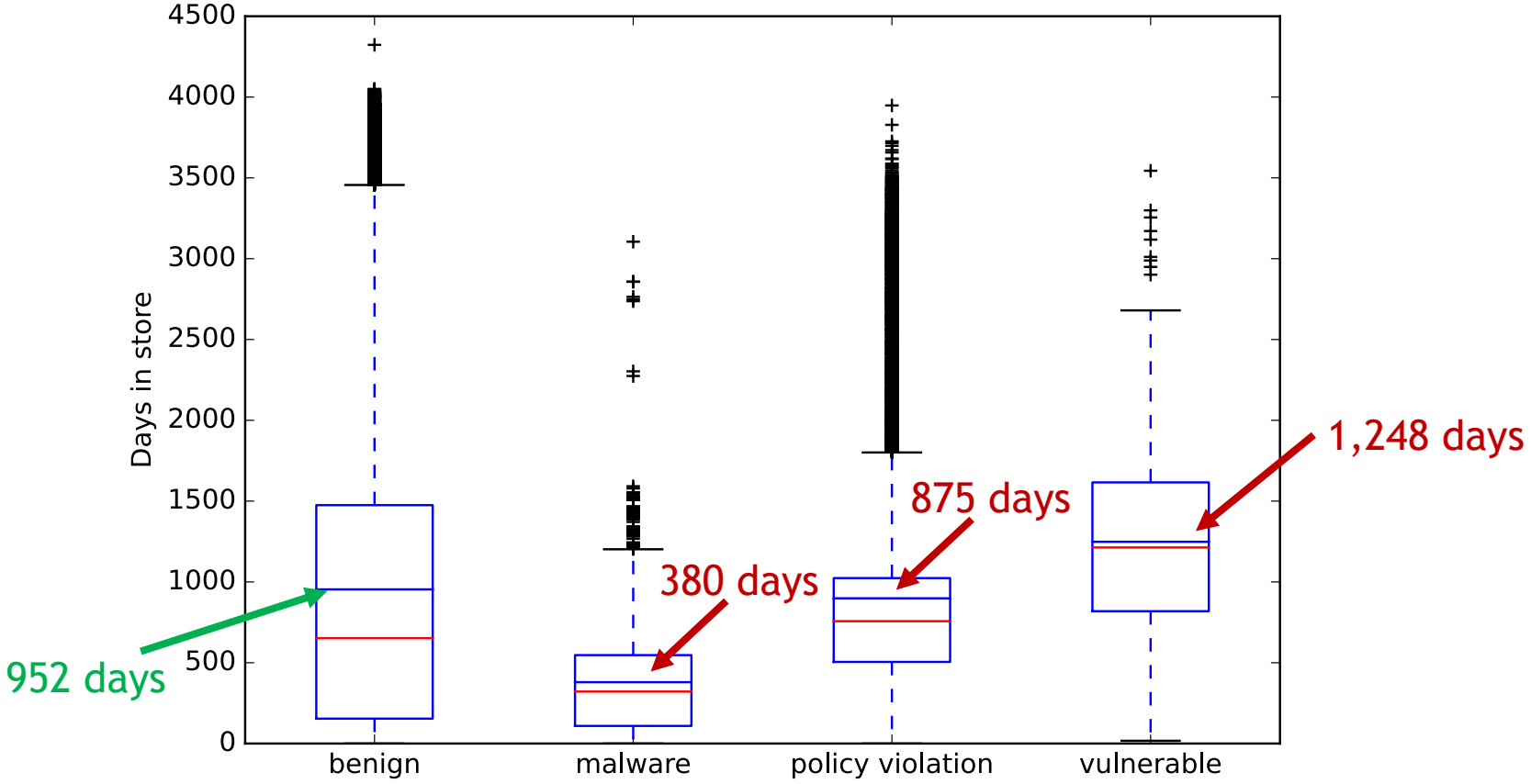
Browser Extension Collection: Chrome-Stats

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

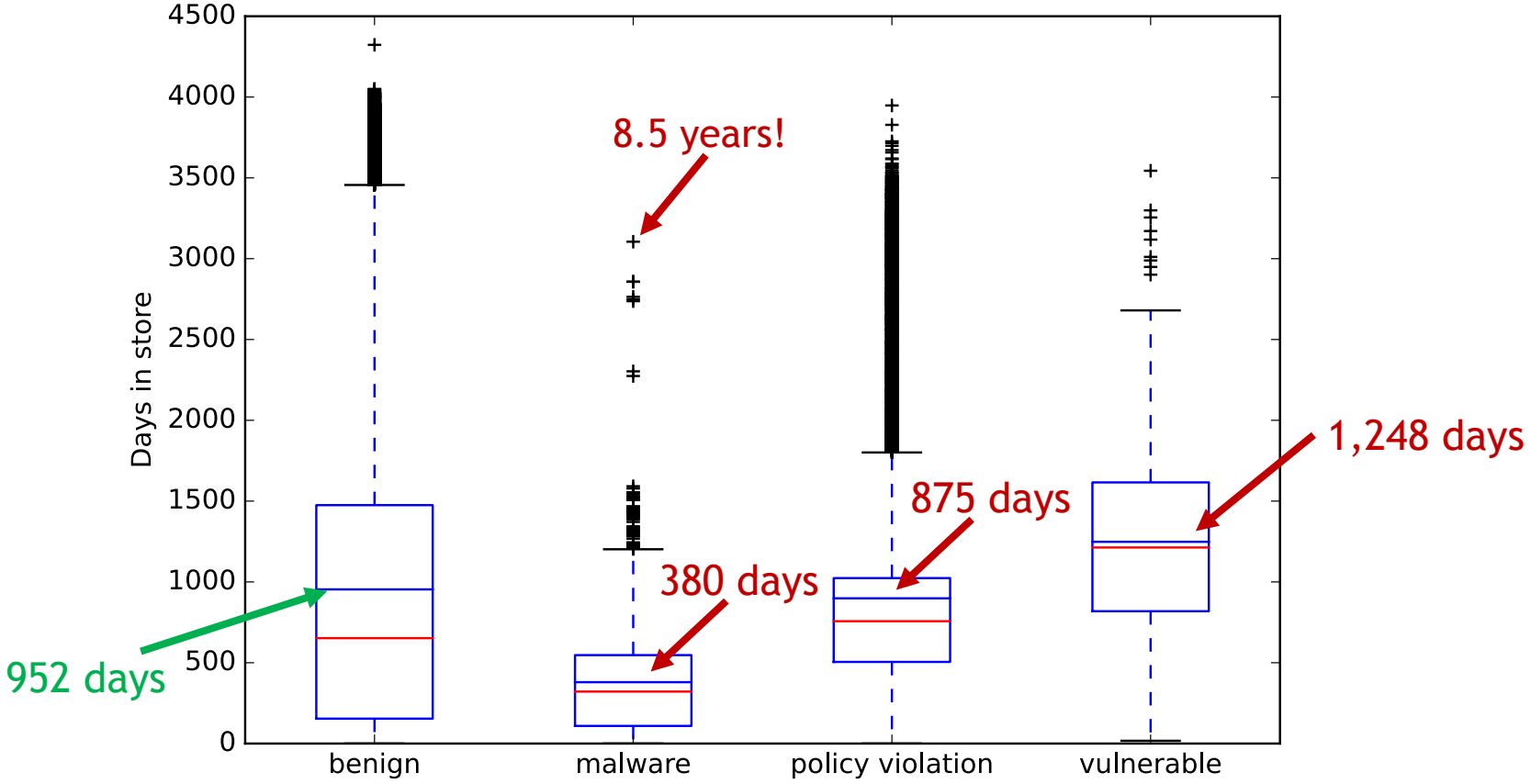
Category	#Extensions Metadata collected	#Extensions Code collected	When collected
SNE	26,014	16,377	Before May 1, 2023
- Malware-containing	10,426	6,587	Before May 1, 2023
- Policy-violating	15,404	9,638	Before May 1, 2023
- Vulnerable [1]	184	152	March 16, 2021
Benign extensions	226,762	92,482	Before May 1, 2023

[1] Fass et al., CCS 2021

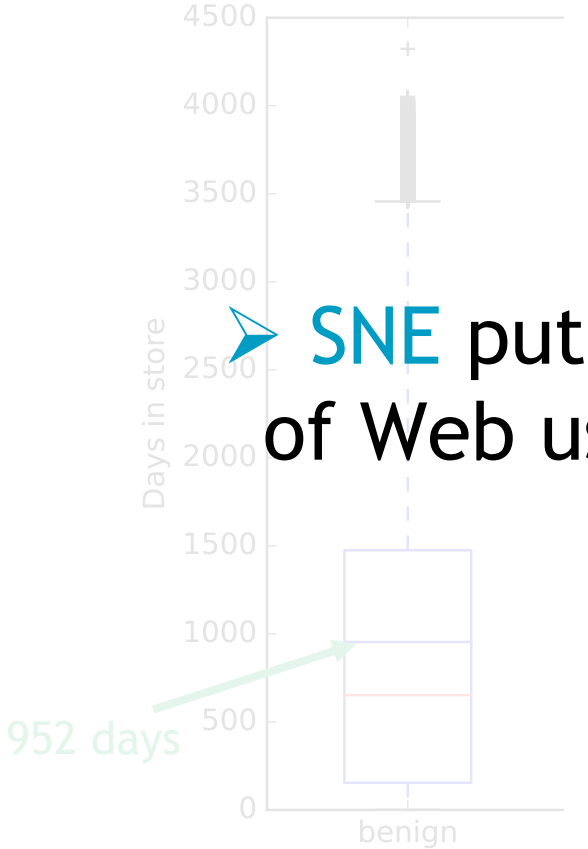
Number of Days in the CWS



Number of Days in the CWS



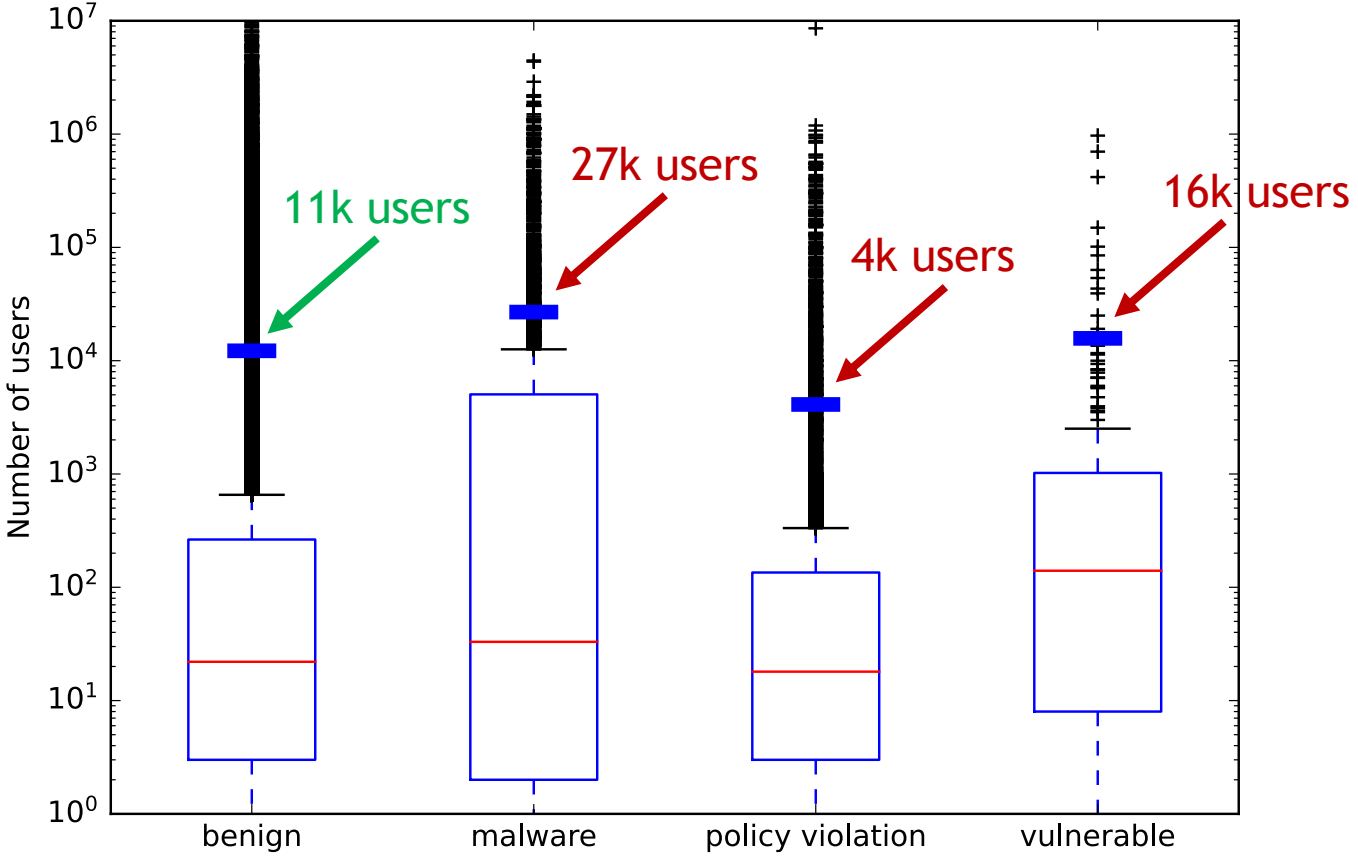
Number of Days in the CWS



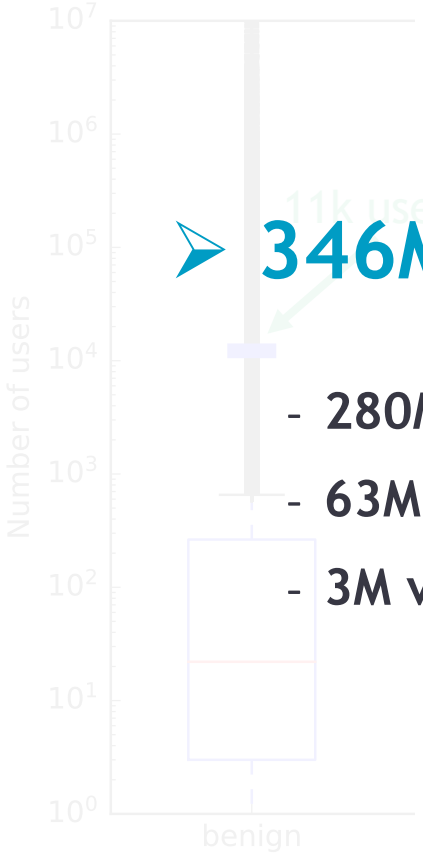
- SNE put the security & privacy of Web users **at risk *for years***

,248 days

Number of Users



Number of Users



- **346M users installed SNE**
  (in the last 3 years):
  - **280M malware-containing**
  - **63M policy-violating**
  - **3M vulnerable extensions**

Detecting SNE with Clustering-based Approaches

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

- Source-code comparison across extensions (*ssdeep* fuzzy hash)
- Clustering similar extensions together (i.e., 100% *ssdeep* overlap)
- 3,270 clusters with $[\![2; 1{,}397]\!]$ extensions (20,822 extensions clustered)

Detecting SNE with Clustering-based Approaches

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

- 3,270 clusters:
  - 2,296 clusters contain just benign extensions
  - 321 clusters only SNE
    - 14 clusters with > 100 SNE and 2 with > 863 SNE each
    - ➢ Analyzing extensions for similarities could enable to **detect SNE**
  - 653 clusters of benign (5,552 extensions) and SNE (5,126)
    - ➢ Extensions in a cluster with SNE should be **flagged for more analyses**

How to Detect Security-Noteworthy Extensions?

- **Contain malware**
  - Designed by malicious actors to harm victims
  - E.g., steal user-sensitive data, track users, propagate malware
- **Violate the Chrome Web Store policies**
  - E.g., deceive users, promote unlawful activities, lacking a privacy policy
- **Contain vulnerabilities**
  - Designed by well-intentioned developers… but contain some vulnerabilities
  - E.g., can lead to user-sensitive data exfiltration

How to Detect Security-Noteworthy Extensions?

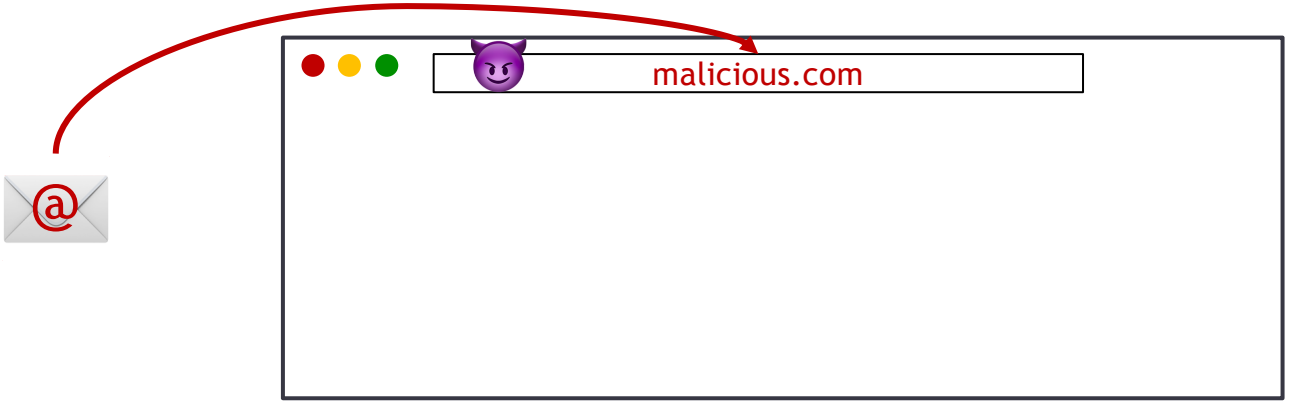
- Contain malware
  - Designed by malicious actors to harm victims
  - E.g., steal user-sensitive data, track users, propagate malware
- Violate the Chrome Web Store policies
  - E.g., deceive users, promote unlawful activities, lacking a privacy policy
- **Contain vulnerabilities**
  - Designed by well-intentioned developers… but contain some vulnerabilities
  - E.g., can lead to user-sensitive data exfiltration

Analysis of Vulnerable Extensions

Challenging to detect due to their inherently benign intent (*benign-but-buggy*)

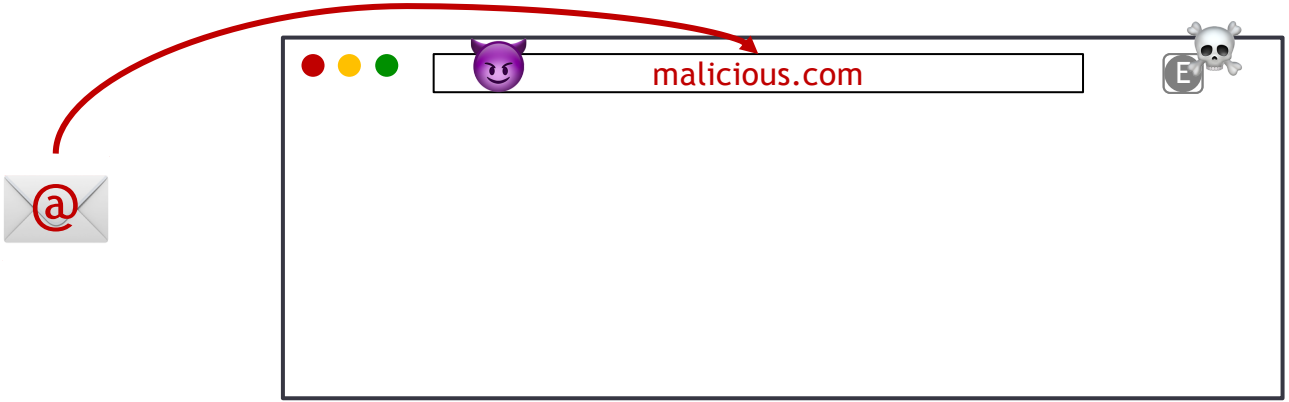
Analysis of Vulnerable Extensions

Challenging to detect due to their inherently benign intent (*benign-but-buggy*)



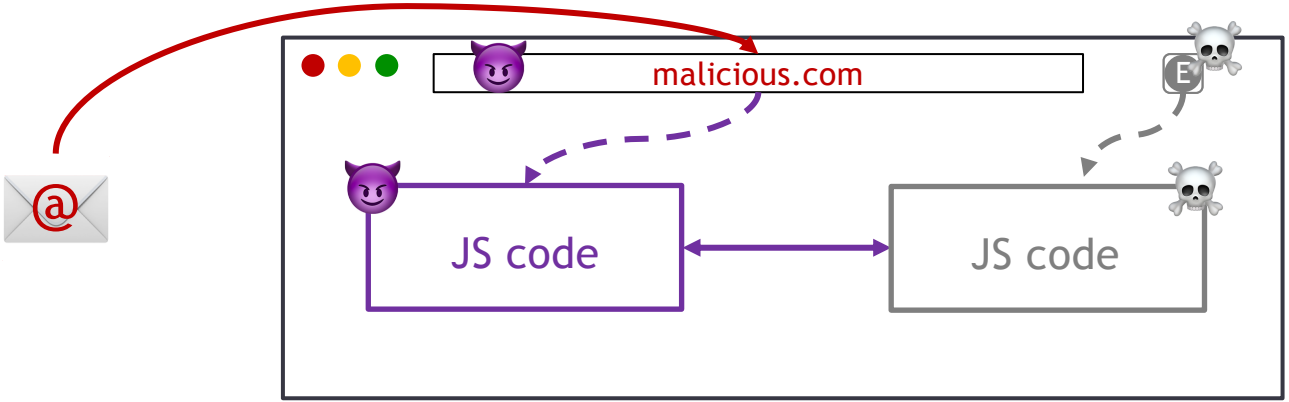
Analysis of Vulnerable Extensions

Challenging to detect due to their inherently benign intent (*benign-but-buggy*)



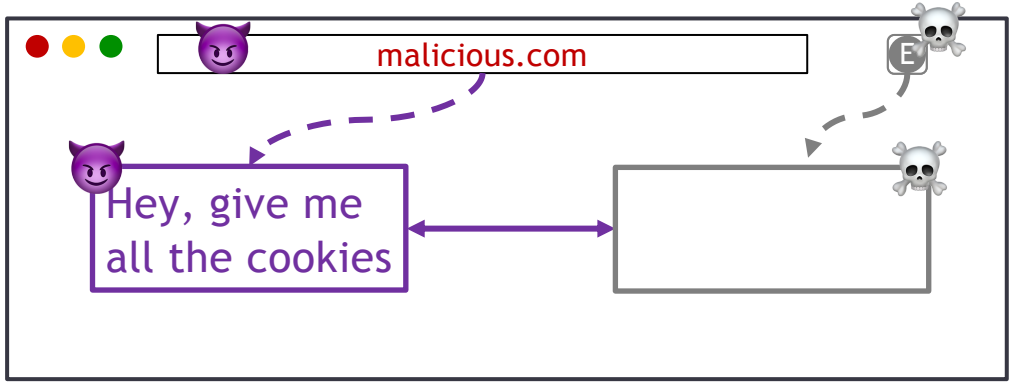
Analysis of Vulnerable Extensions

Challenging to detect due to their inherently benign intent (*benign-but-buggy*)



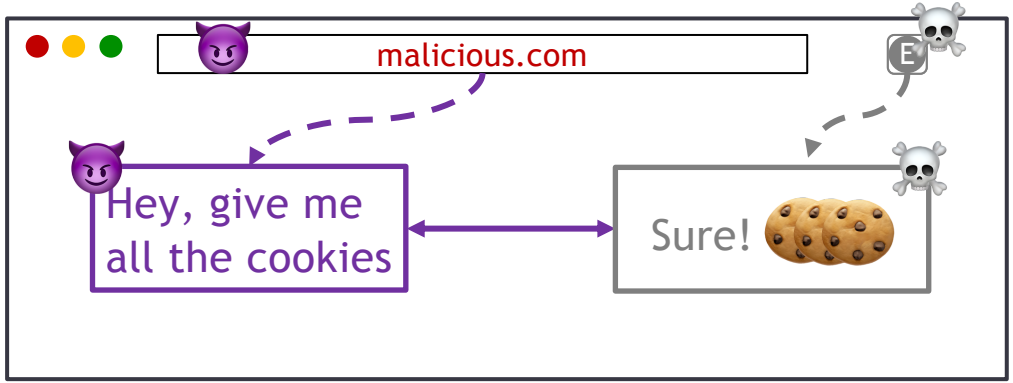
Analysis of Vulnerable Extensions

Challenging to detect due to their inherently benign intent (*benign-but-buggy*)



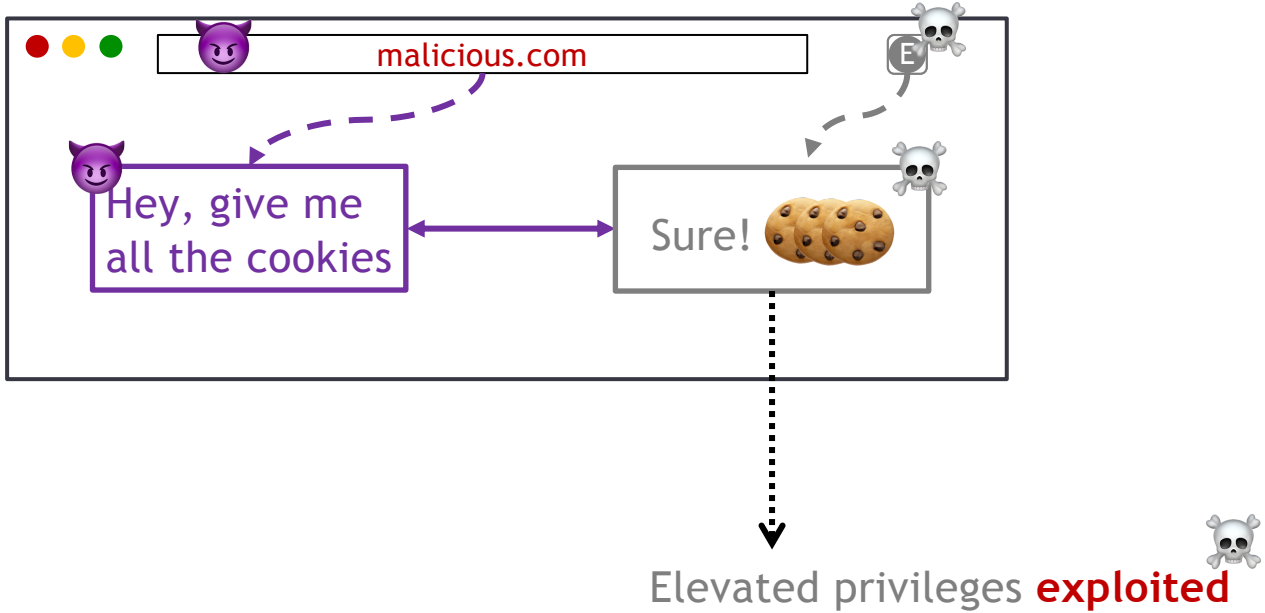
Analysis of Vulnerable Extensions

Challenging to detect due to their inherently benign intent (*benign-but-buggy*)



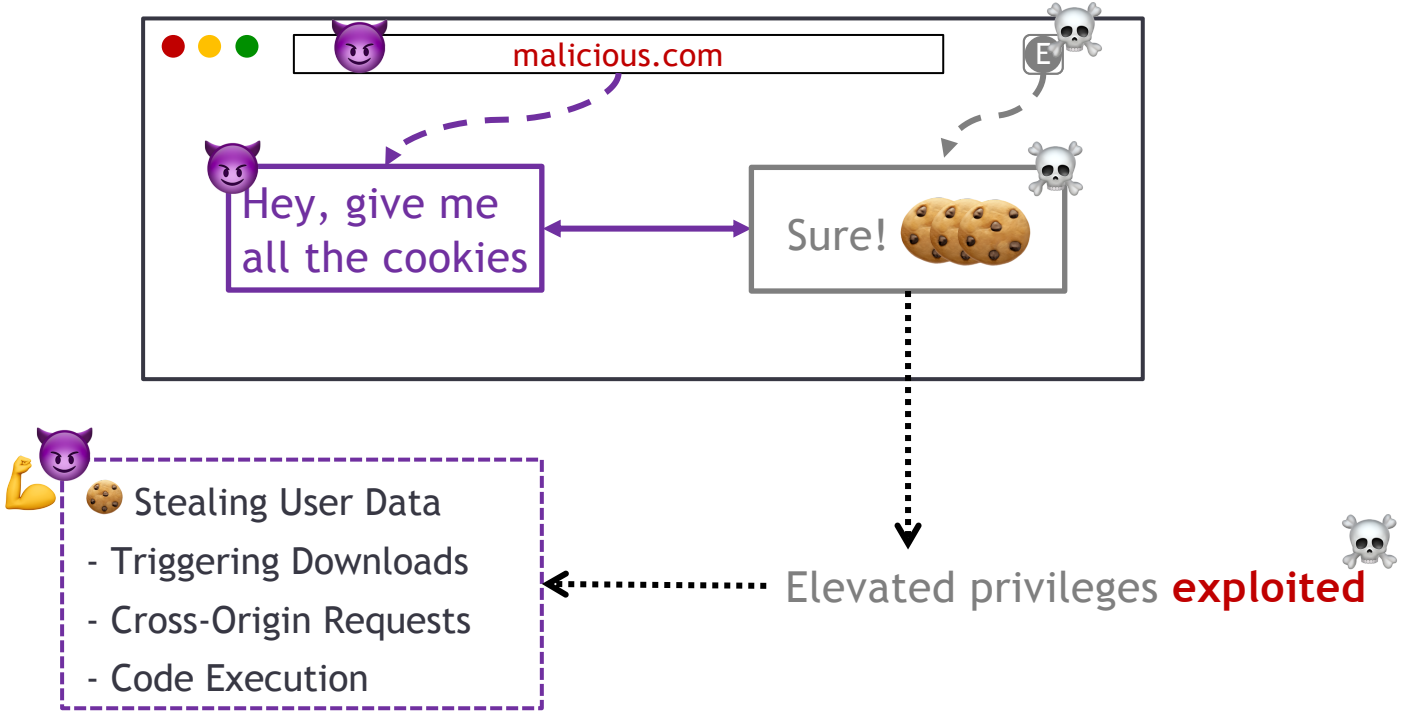
Analysis of Vulnerable Extensions

Challenging to detect due to their inherently benign intent (*benign-but-buggy*)



Analysis of Vulnerable Extensions

Challenging to detect due to their inherently benign intent (*benign-but-buggy*)



Detecting Vulnerable Extensions

Fass et al.
CCS 2021

CISPA
HELMHOLTZ CENTER FOR
INFORMATION SECURITY

> DOUBLEX: Statically Detecting Vulnerable Data Flows in Browser Extensions

In *ACM CCS* 2021. Aurore Fass, Dolière Francis Somé, Michael Backes, and Ben Stock

Detecting Vulnerable Extensions

Fass et al.
CCS 2021


DoubleX: Statically Detecting Vulnerable Data Flows in Browser Extensions at Scale

Aurore Fass, Dolière Francis Somé, Michael Backes, and Ben Stock
CISPA Helmholtz Center for Information Security

> DOUBLEX: Statically Detecting Vulnerable Data Flows in Browser Extensions

In *ACM CCS* 2021. Aurore Fass, Dolière Francis Somé, Michael Backes, and Ben Stock

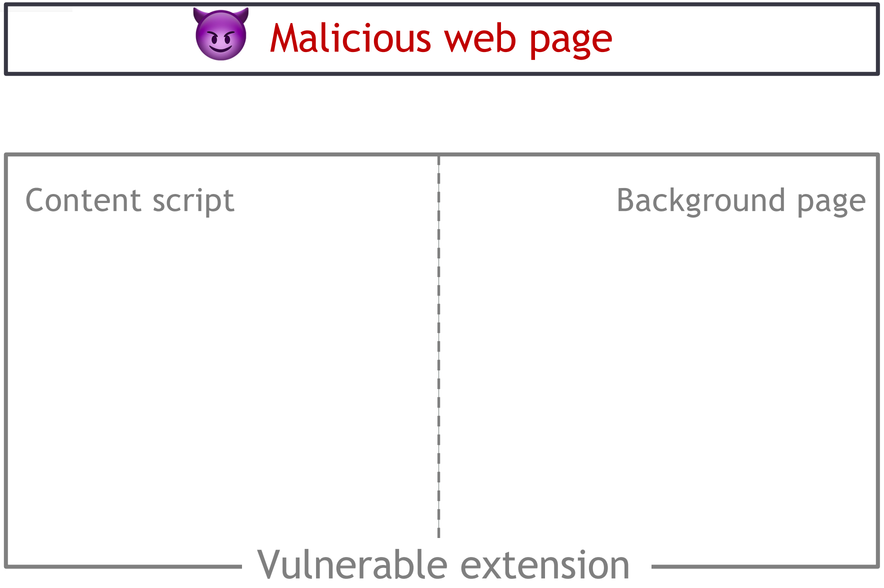
Detecting Vulnerable Extensions

Fass et al.
CCS 2021


DoubleX: Statically Detecting Vulnerable Data Flows in Browser Extensions at Scale
Aurore Fass, Dolière Francis Somé, Michael Backes, and Ben Stock
CISPA Helmholtz Center for Information Security

> DOUBLEX: Statically Detecting Vulnerable Data Flows in Browser Extensions

In *ACM CCS* 2021. Aurore Fass, Dolière Francis Somé, Michael Backes, and Ben Stock



Detecting Vulnerable Extensions


DoubleX: Statically Detecting Vulnerable Data Flows in Browser Extensions at Scale

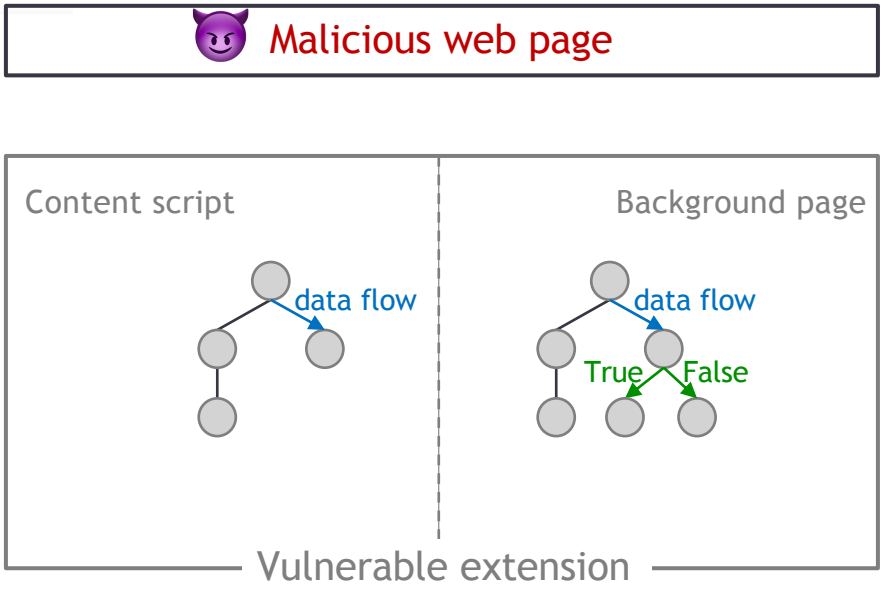
Aurore Fass, Dolière Francis Somé, Michael Backes, and Ben Stock

CISPA Helmholtz Center for Information Security

Fass et al. CCS 2021

> DOUBLEX: Statically Detecting Vulnerable Data Flows in Browser Extensions

In *ACM CCS* 2021. Aurore Fass, Dolière Francis Somé, Michael Backes, and Ben Stock



Per-component JS code abstraction

- AST (Abstract Syntax Tree)
- Control flow
- Data flow
- Pointer analysis

Detecting Vulnerable Extensions

Fass et al. CCS 2021

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY


DoubleX: Statically Detecting Vulnerable Data Flows in Browser Extensions at Scale

Aurore Fass, Dolière Francis Somé, Michael Backes, and Ben Stock

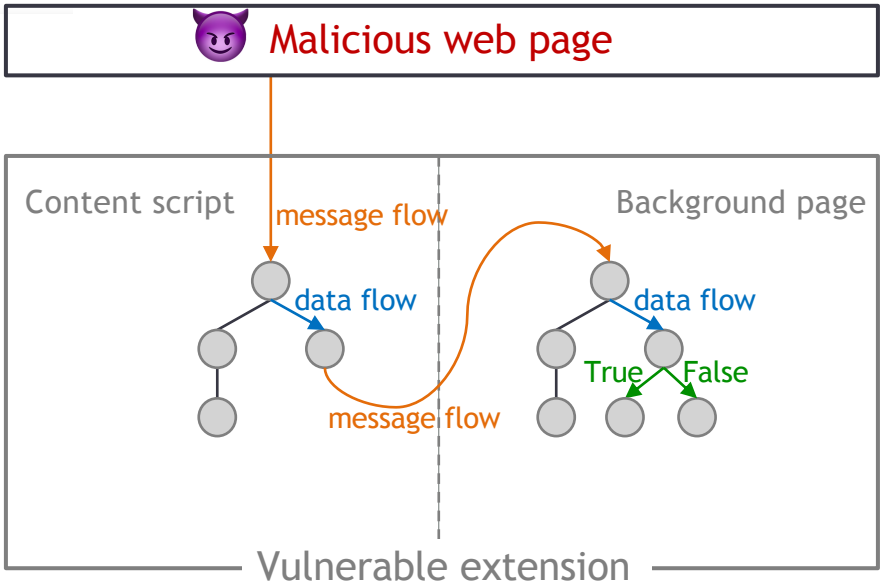
CISPA Helmholtz Center for Information Security

Abstract

Introduction

> DOUBLEX: Statically Detecting Vulnerable Data Flows in Browser Extensions

In *ACM CCS* 2021. Aurore Fass, Dolière Francis Somé, Michael Backes, and Ben Stock



Per-component JS code abstraction

- AST (Abstract Syntax Tree)
- Control flow
- Data flow
- Pointer analysis

Extension Dependence Graph (EDG)

➢ Message interactions

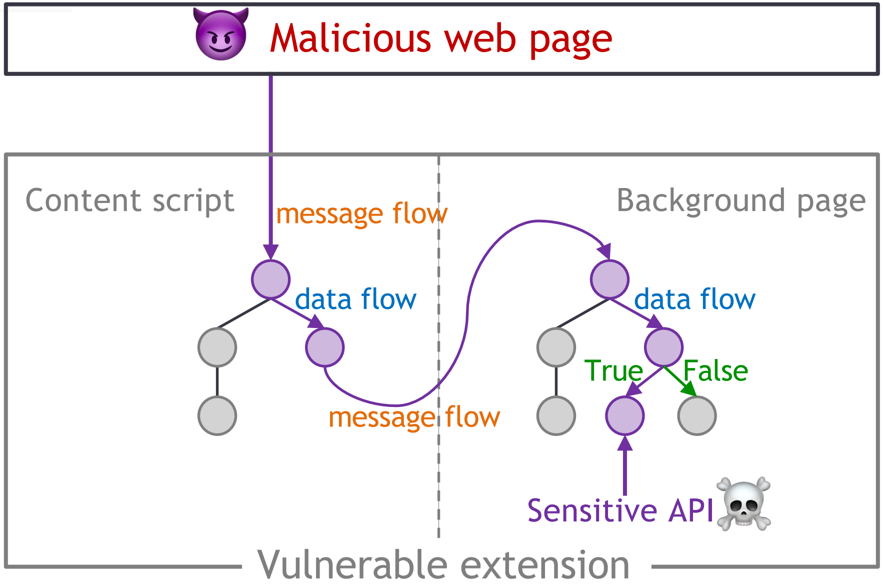
Detecting Vulnerable Extensions

Fass et al.
CCS 2021


DoubleX: Statically Detecting Vulnerable Data Flows in Browser Extensions at Scale
Aurore Fass, Dolière Francis Somé, Michael Backes, and Ben Stock
CISPA Helmholtz Center for Information Security

> DOUBLEX: Statically Detecting Vulnerable Data Flows in Browser Extensions

In *ACM CCS* 2021. Aurore Fass, Dolière Francis Somé, Michael Backes, and Ben Stock



Per-component JS code abstraction

- AST (Abstract Syntax Tree)
- Control flow
- Data flow
- Pointer analysis

Extension Dependence Graph (EDG)

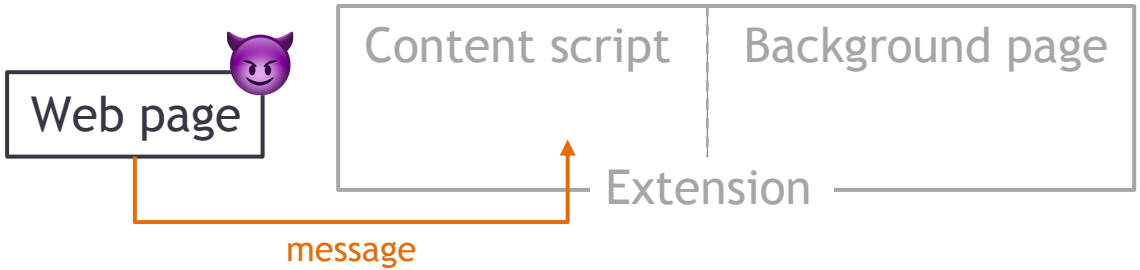
➤ Message interactions

Suspicious data flow tracking

➤ Detects any path between an attacker & sensitive APIs

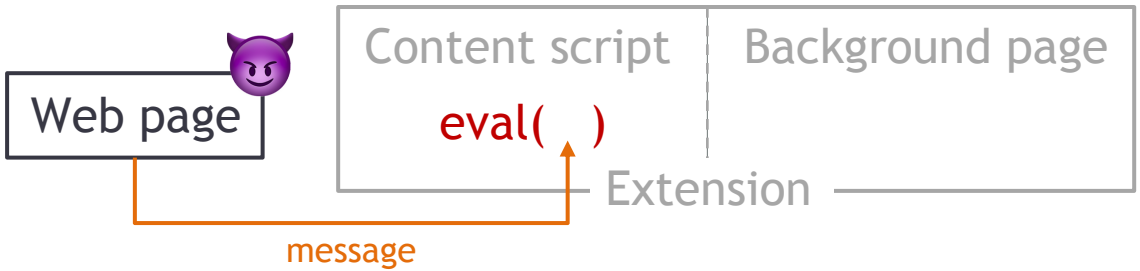
Simplified Example of a Vulnerability

```
// Content script code
window.addEventListener("message", function(event) {




})
```



Simplified Example of a Vulnerability

```
// Content script code
window.addEventListener("message", function(event) {

    eval(event.data);

})
```



Detecting Vulnerable Extensions with DOUBLEX

Analyzed 155k Chrome extensions from 2021 with DOUBLEX

- **184 vulnerable Chrome extensions**
- Impacting **3M users**

Life Cycle of Vulnerable Chrome Extensions

- Analyzed 165k extensions from 2020 with DOUBLEX
  - 193 vulnerable extensions (184 in 2021)
  - vulnerability disclosure for 35 extensions (48 extensions when including 2021)

- Comparison of vulnerable extensions in 2020 vs. 2021
  - not in the CWS anymore: 30 / 193
  - vulnerability fixed: 3 / 193
  - turned vulnerable: 5 / 184
  - new vulnerable: 19 / 184

➢ **still vulnerable: 160 (83%!)**

➢ **Need to prevent vulnerable extensions from entering the CWS → DOUBLEX**

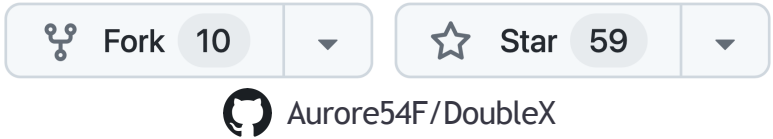
Detecting Vulnerable Extensions with DOUBLEX

Analyzed 155k Chrome extensions from 2021 with DOUBLEX

- **184 vulnerable Chrome extensions**
- Impacting **3M users**

- **Precision: 89%** of the flagged extensions are vulnerable
- **Recall: 93%** of known vulnerabilities [2] are detected

- **Integration** in the **vetting process** conducted by Google
- **Available online**, for developers
  (even in other fields!)



[2] Somé, IEEE S&P 2019

Security-Noteworthy Extensions

- Contain malware
  - Designed by malicious actors to harm victims
  - E.g., steal user-sensitive data, track users, propagate malware
- Violate the Chrome Web Store policies
  - E.g., deceive users, promote unlawful activities, lacking a privacy policy
- Contain vulnerabilities
  - Designed by well-intentioned developers, but contain some vulnerabilities
  - E.g., can lead to user-sensitive data exfiltration

- Can be fingerprinted
  - Designed by well-intentioned developers…
  - … but can lead to, e.g., tracking users across sites, inferring sensitive user information

Security-Noteworthy Extensions

- Contain malware
  - Designed by malicious actors to harm victims
  - E.g., steal user-sensitive data, track users, propagate malware
- Violate the Chrome Web Store policies
  - E.g., deceive users, promote unlawful activities, lacking a privacy policy
- Contain vulnerabilities
  - Designed by well-intentioned developers… but contain some vulnerabilities
  - E.g., can lead to user-sensitive data exfiltration

- Can be fingerprinted
  - Designed by well-intentioned developers…
  - … but can lead to, e.g., tracking users across sites, inferring sensitive user information

Takeaways — Browser Extension (In)Security

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Browser Extensions are Popular

AdBlock — best ad blocker (Offered by: getadblock.com)
Adblock Plus - free ad blocker (Offered by: adblockplus.org)
Adobe Acrobat (Offered by: Adobe Inc.)
Avast Online Security (Offered by: https://www.avast.com)
Cisco Webex Extension (Offered by: webex.com)
Google Translate (Offered by: translate.google.com)
Grammarly for Chrome (Offered by: grammarly.com)
Honey (Offered by: https://www.joinhoney.com)
Pinterest Save Button (Offered by: pinterest.com)
Skype (Offered by: www.skype.com)
uBlock Origin (Offered by: Raymond Hill (gorhill))
LastPass: Free Password Manager (Offered by: LastPass)

- **125k** Chrome extensions totaling over **1.6B** active users

Security-Noteworthy Extensions (SNE)

- Contain **malware**
- **Violate** the Chrome Web Store **policies**
- Contain **vulnerabilities**

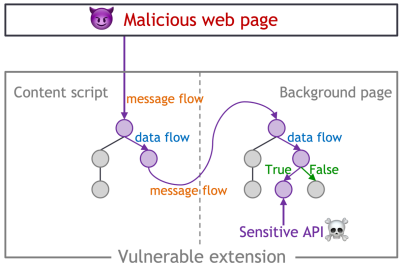
- Can be **fingerprinted**

Thank you

What is in the Chrome Web Store?

- **350M users** installed **SNE** in the last 3 years
- These **SNE** stay in the Chrome Web Store *for years*
- Extensions have a **short life cycle** in the CWS (60% stay 1 year)
- Critical **lack of maintenance** in the CWS (60% received no update)

Detecting Vulnerable Extensions with DOUBLEX



Fass et al.
CCS 2021

Aurore54F/DoubleX

➢ DOUBLEX detects suspicious data flows in browser extensions

184 vulnerable extensions | **Precision: 89%** | **Recall: 93%**

fass@cispa.de
https://aurore54f.github.io
@AuroreFass

Corresponding Publications

- What is in the Chrome Web Store?

Sheryl Hsu, Manda Tran, and Aurore Fass. In *ACM AsiaCCS* 2024

- DoubleX: Statically Detecting Vulnerable Data Flows in Browser Extensions at Scale

Aurore Fass, Dolière Francis Somé, Michael Backes, and Ben Stock. In *ACM CCS* 2021

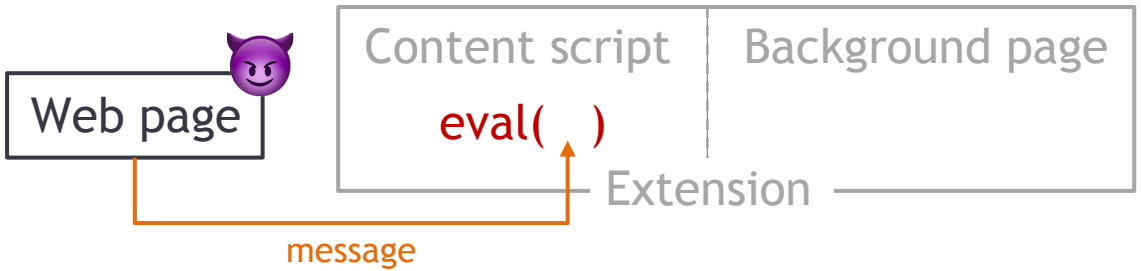
- Peeking through the window: Fingerprinting Browser Extensions through Page-Visible Execution Traces and Interactions

Shubham Agarwal, Aurore Fass, and Ben Stock. In *ACM CCS* 2024

Additional slides about some questions asked

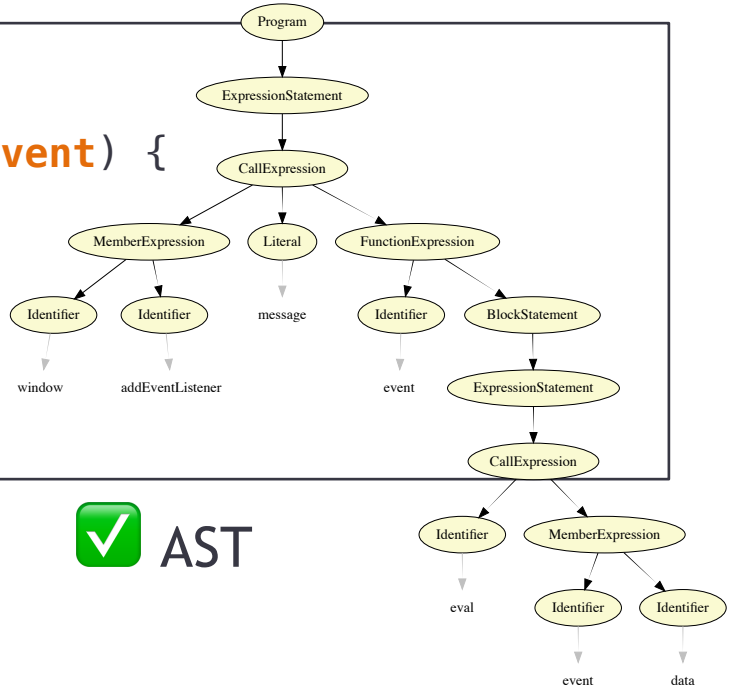
Per-Component JavaScript Code Abstraction

```
// Content script code
window.addEventListener("message", function(event) {

    eval(event.data);

})
```



Per-Component JavaScript Code Abstraction

```
// Content script code
window.addEventListener("message", function(event) {

    eval(event.data);

})
```



Abstract code representation → ✅ AST

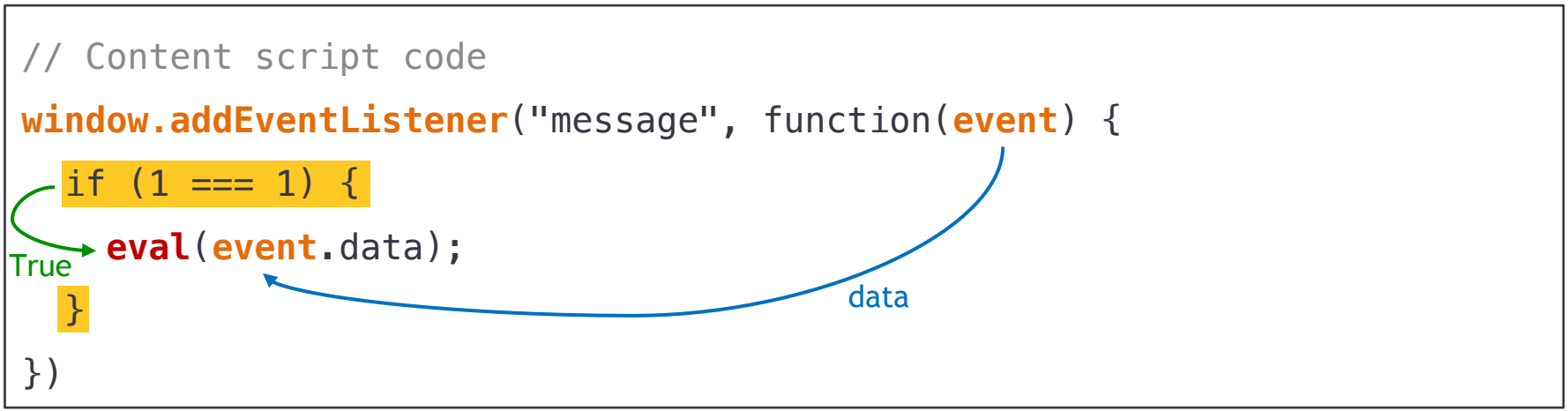
Per-Component JavaScript Code Abstraction

```
// Content script code
window.addEventListener("message", function(event) {

    eval(event.data);

})
```

Abstract code representation → ✅ AST

– variable dependencies → ✅ data flow

Per-Component JavaScript Code Abstraction



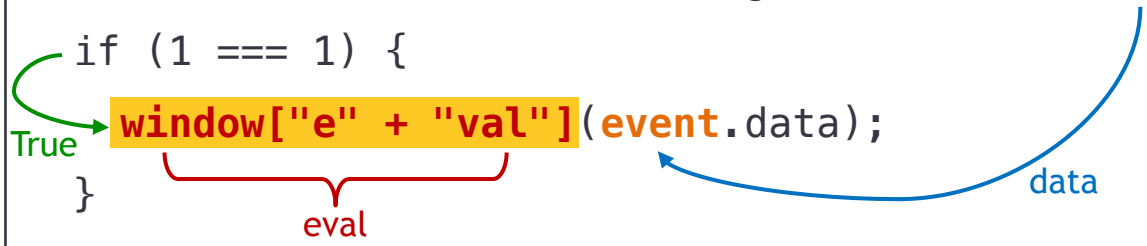
Abstract code representation → ✅ AST

– conditions → ✅ control flow

– variable dependencies → ✅ data flow

Per-Component JavaScript Code Abstraction

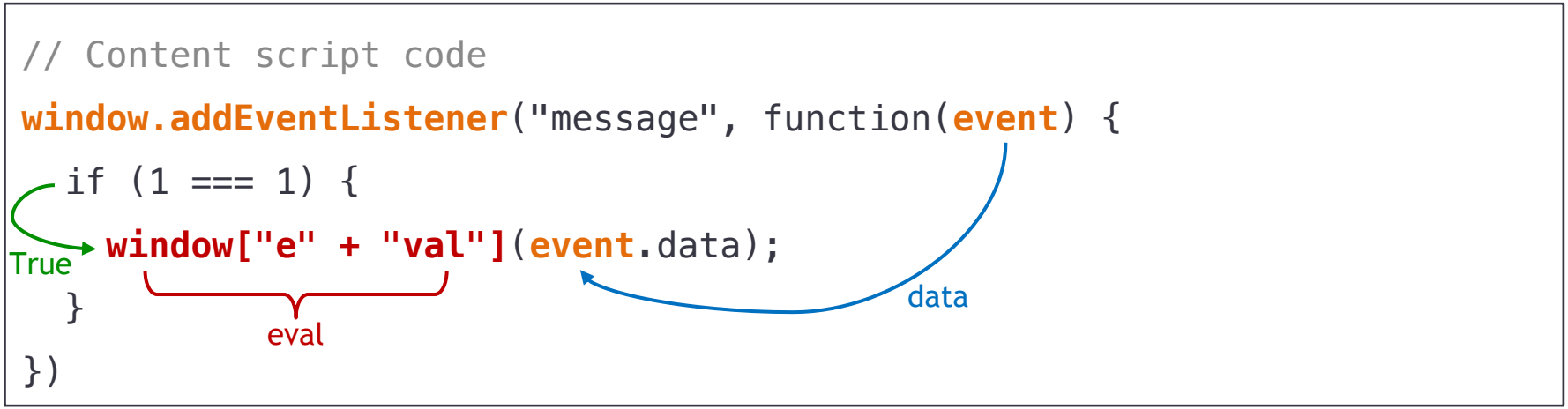
```
// Content script code
window.addEventListener("message", function(event) {
  if (1 === 1) {
    window["e" + "val"](event.data);
  }
})
```



Abstract code representation → ✅ AST

- conditions → ✅ control flow
- variable dependencies → ✅ data flow
- variable values → ✅ pointer analysis

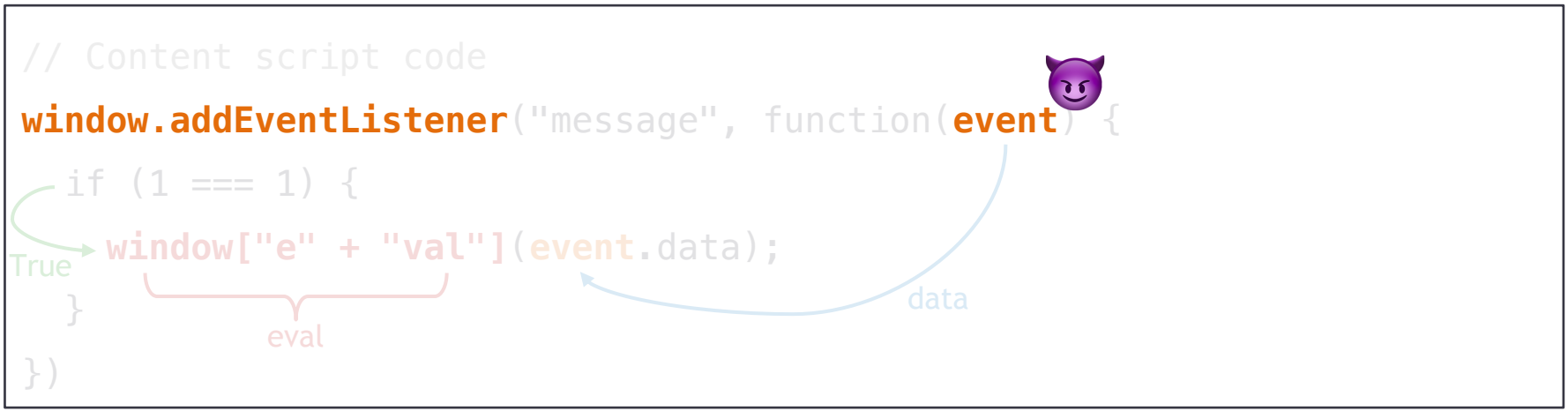
Extension Dependence Graph



– external messages

– internal messages

Extension Dependence Graph



- external messages ✅
- internal messages

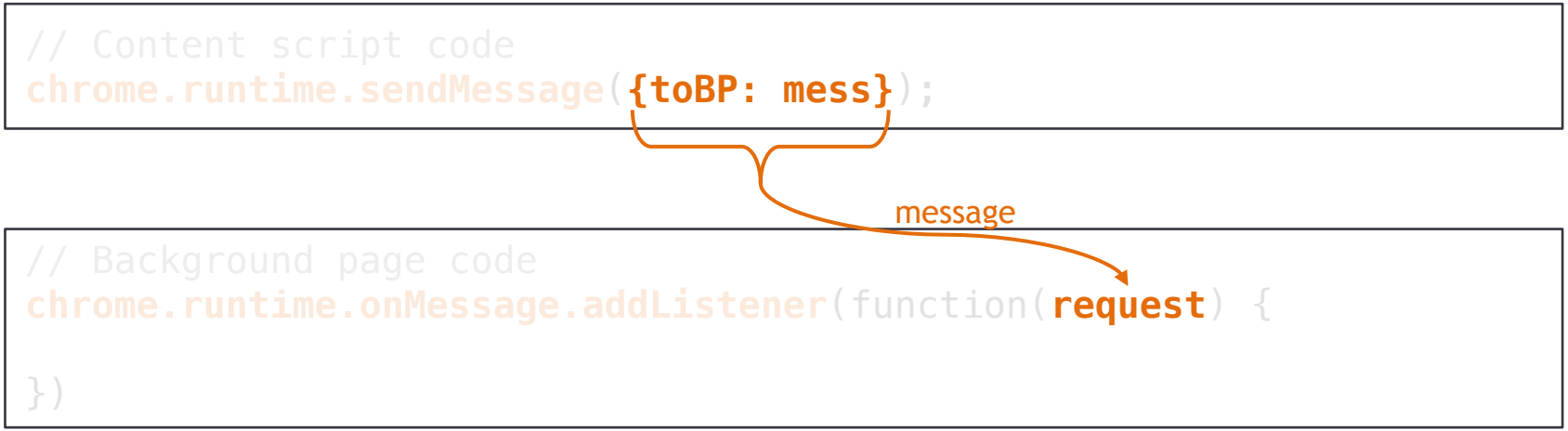
Extension Dependence Graph

```
// Content script code
chrome.runtime.sendMessage({toBP: mess});
```

```
// Background page code
chrome.runtime.onMessage.addListener(function(request) {

})
```

- external messages ✅
- internal messages

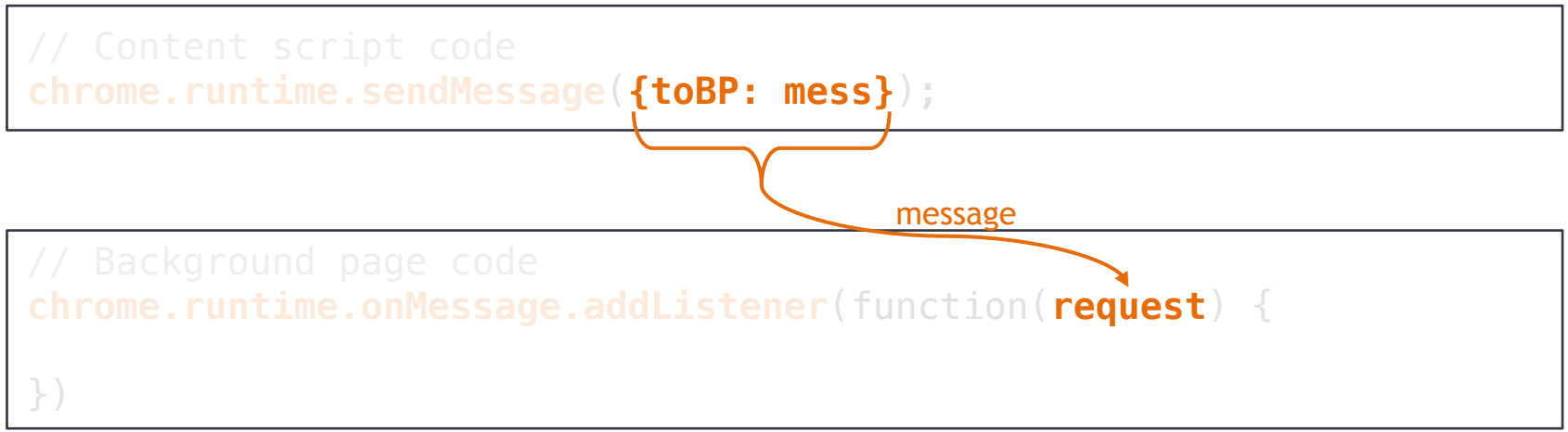
Extension Dependence Graph



– external messages ✅

– internal messages ✅

Extension Dependence Graph



– external messages ✅

– internal messages ✅

➢ Models message interaction within and outside of an extension

Suspicious Data Flow Tracking

```
1  // Content script code
2  window.addEventListener("message", function(event) {
3    if (1 === 1) {
4      window["e" + "val"](event.data);
5    }
6  })
```

True

eval

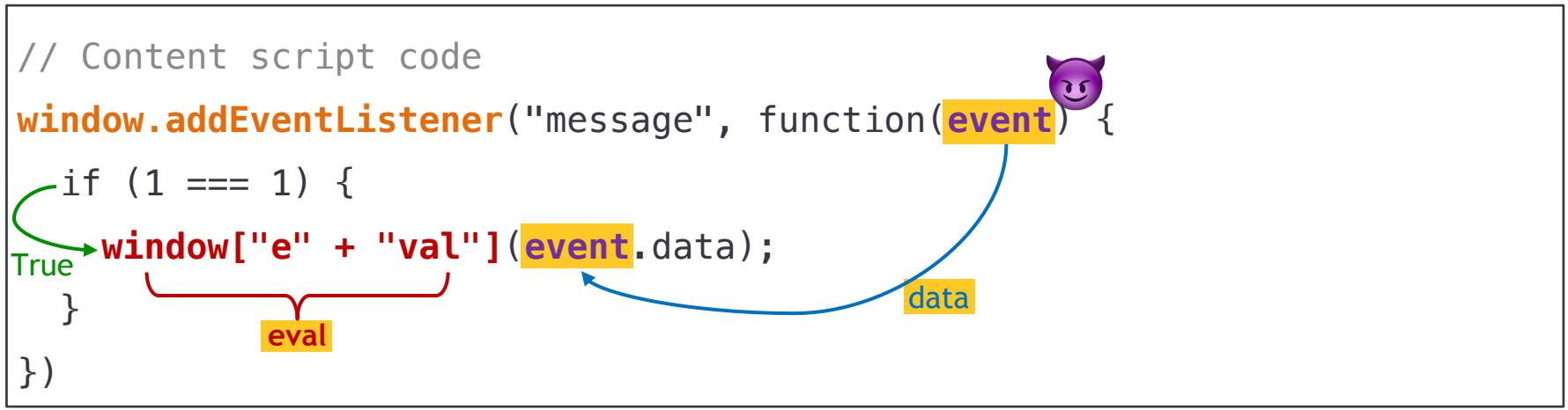
Suspicious Data Flow Tracking

```
1  // Content script code
2  window.addEventListener("message", function(event) {
3    if (1 === 1) {
4      window["e" + "val"](event.data);
5    }
6  })
```

True

eval

Suspicious Data Flow Tracking



Suspicious Data Flow Tracking

```
1  // Content script code
2  window.addEventListener("message", function(event) {
3    if (1 === 1) {
4      window["e" + "val"](event.data);
5    }
6  })
```

True

eval

data

Suspicious Data Flow Tracking

```
1  // Content script code
2  window.addEventListener("message", function(event) {
3    if (1 === 1) {
4      window["e" + "val"](event.data);
5    }
6  })
```

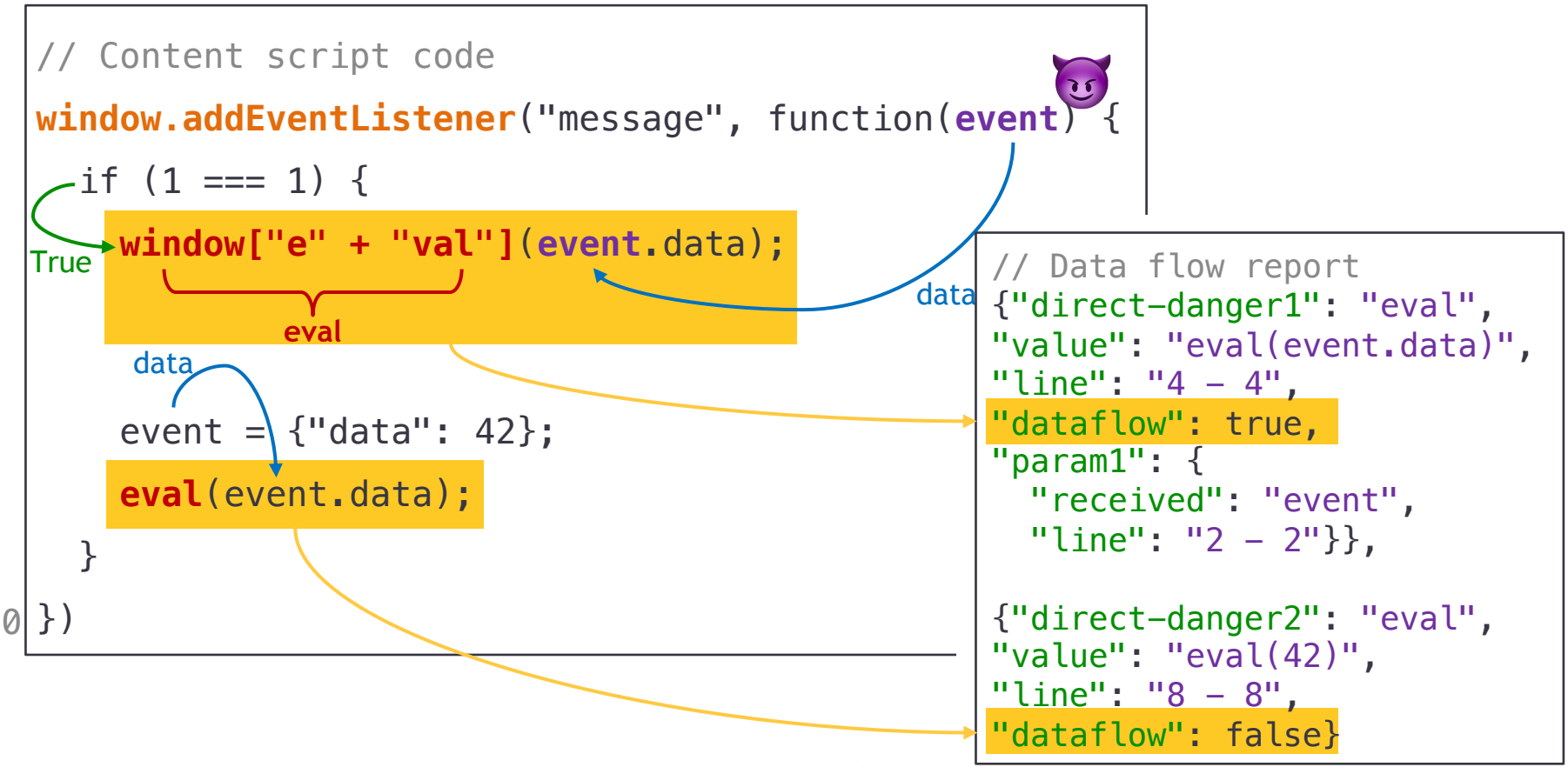
True

eval

data


```
// Data flow report
{"direct-danger1": "eval",
"value": "eval(event.data)",
"line": "4 - 4",
"dataflow": true,
"param1": {
  "received": "event",
  "line": "2 - 2"}}
```

Suspicious Data Flow Tracking



Sensitive APIs Considered

Flaw category	All components	High-privilege components
Code Execution	`eval`, `setInterval`, `setTimeout`	`tabs.executeScript`
Triggering Downloads		`downloads.download`
Cross-Origin Requests	`$.ajax`, `jQuery.ajax`, `fetch`, `$.get`, `jQuery.get`, `$http.get`, `$.post`, `$http.post`, `XMLHttpRequest().open`, `jQuery.post`, `XMLHttpRequest.open`	
Data Exfiltration		`bookmarks.getTree`, `cookies.getAll`, `history.search`, `topSites.get`

Large-Scale Analysis of Chrome Extensions

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Attacker capabilities	#Exploitable
Code Execution	63
Triggering Downloads	21
Cross-Origin Requests	49
Data Exfiltration	76
Sum	209