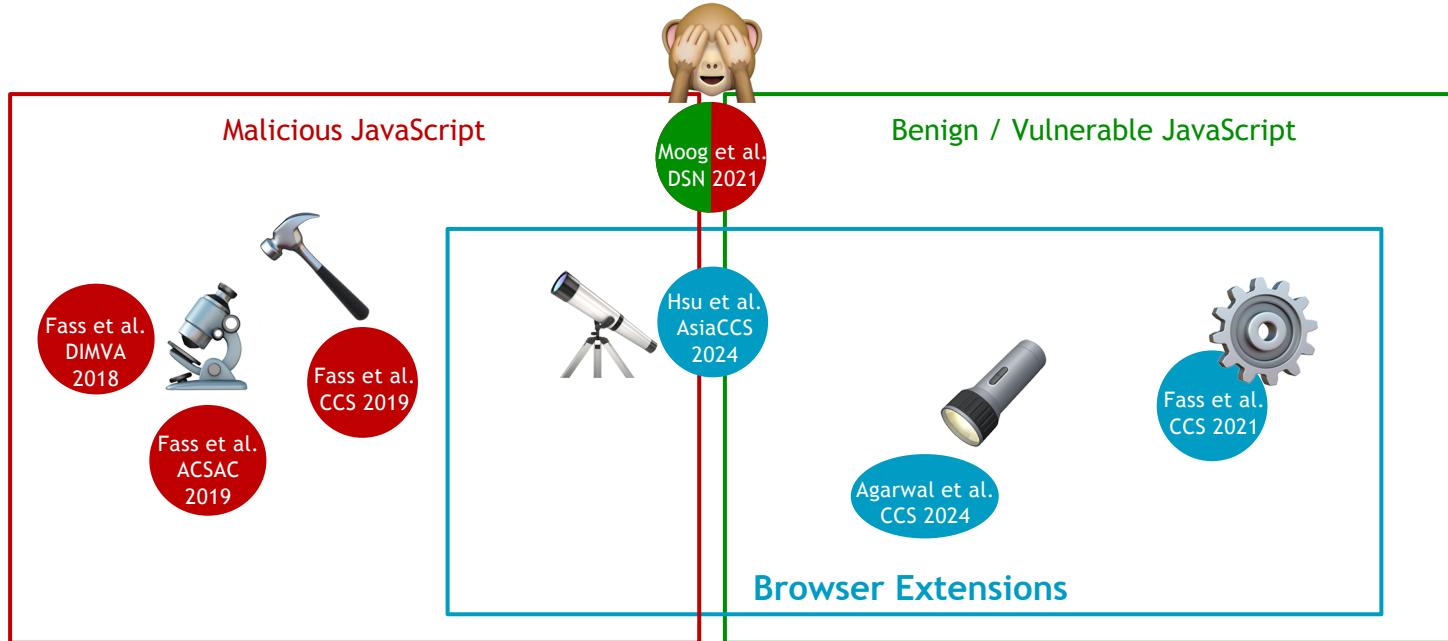


# Browser Extension (In)Security

Aurore Fass

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

# Research Work: Web Security & Privacy



Apruzzese et al.  
AISeC 2024

Machine Learning



Ruth et al.  
IMC 2022

Internet Measurements

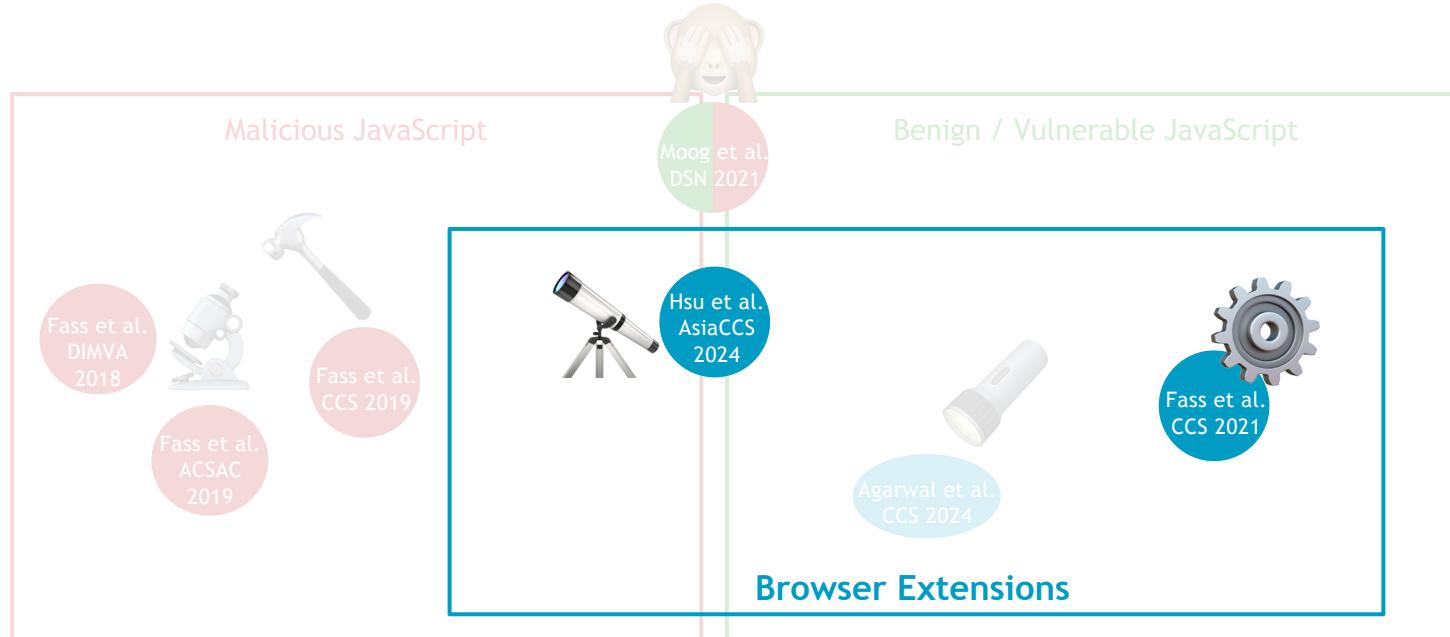
Izhikevich et al.  
IMC 2023



Software Engineering

Troppmann et al.  
ASE 2024

# Research Work: Web Security & Privacy



Apruzzese et al.  
AISeC 2024

Machine Learning



Ruth et al.  
IMC 2022

Internet Measurements

Izhikevich et al.  
IMC 2023



Software Engineering

Troppmann et al.  
ASE 2024

# What are Browser Extensions?

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



AdBlock — best ad blocker

Offered by: [getadblock.com](http://getadblock.com)



Adblock Plus - free ad blocker

Offered by: [adblockplus.org](http://adblockplus.org)



Adobe Acrobat

Offered by: Adobe Inc.



Avast Online Security

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



Cisco Webex Extension

Offered by: [webex.com](http://webex.com)



Google Translate

Offered by: [translate.google.com](http://translate.google.com)



Grammarly for Chrome

Offered by: [grammarly.com](http://grammarly.com)



Honey

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



Pinterest Save Button

Offered by: [pinterest.com](http://pinterest.com)



Skype

Offered by: [www.skype.com](http://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)

→ 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?

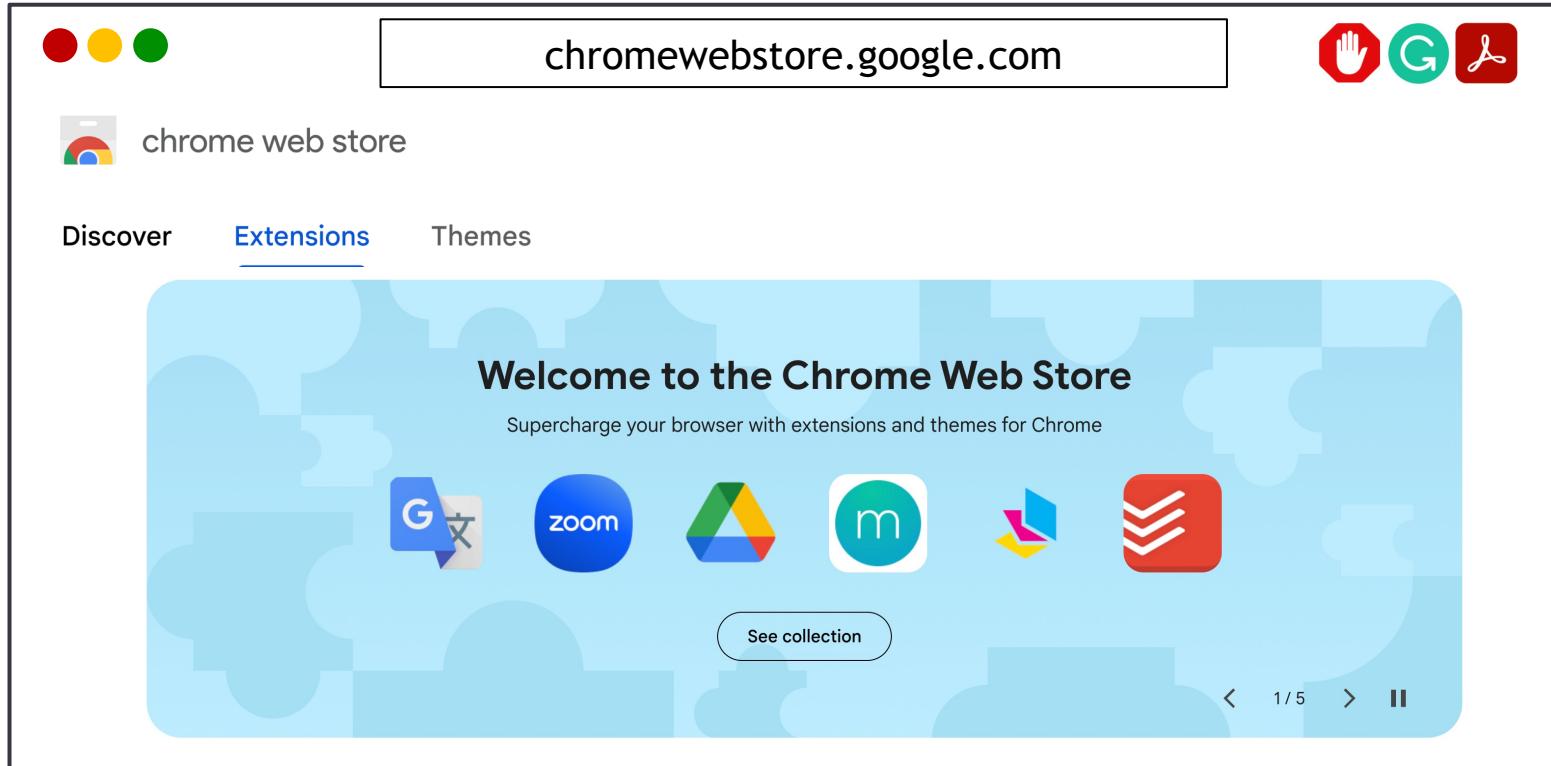


> What is in the Chrome Web Store?

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



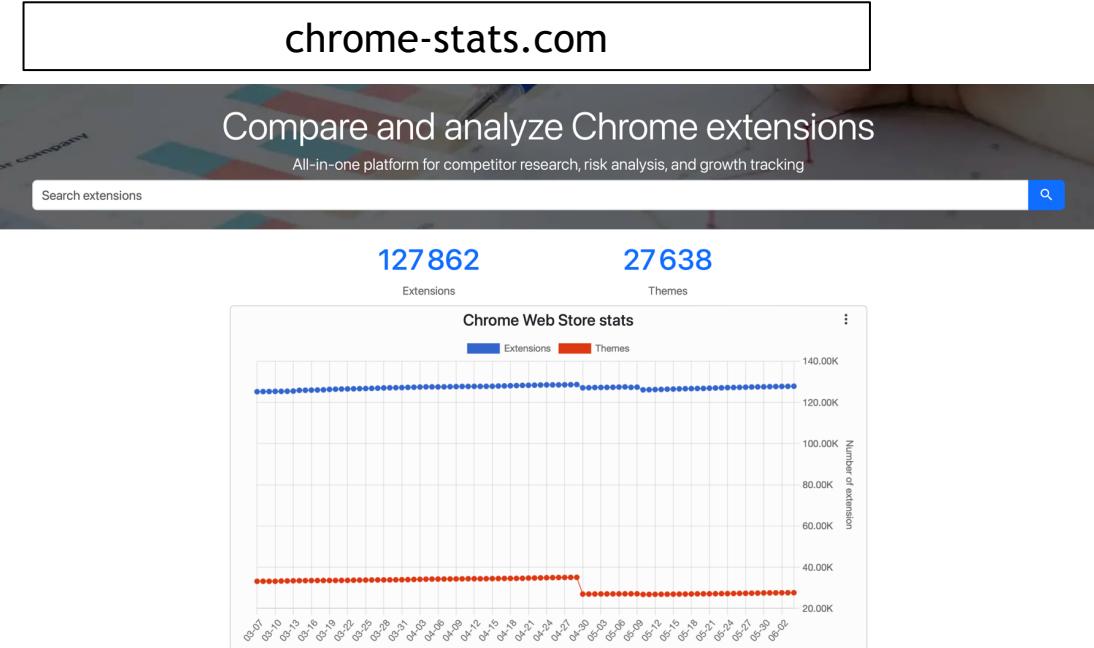
# How to Install Extensions or SNE?



# How to Install Extensions or SNE?



# Browser Extension Collection: Chrome-Stats



The screenshot shows the Chrome-Stats.com homepage. At the top, there's a search bar with the text "chrome-stats.com". Below it is a banner with the heading "Compare and analyze Chrome extensions" and the subtext "All-in-one platform for competitor research, risk analysis, and growth tracking". On the left, there's a sidebar with a navigation menu. The main content area features two large numbers: "127862" under "Extensions" and "27638" under "Themes". Below these are two line charts. The top chart, titled "Chrome Web Store stats", tracks the number of extensions and themes from March 2021 to August 2021. The bottom chart tracks the number of extensions and themes from April 2021 to August 2021. A link "Explore more Chrome extension statistics" is at the bottom of the chart area.

Recently viewed

- Spotify™ & Deezer™ Music Downloader
- GS Auto Clicker:Free Download 2021
- Fraud Risk Scoring
- Autoskip for Youtube
- Maxi Refresher

Stats & analysis tools

- Chrome extension statistics
- Extension explorer
- Keyword explorer
- Publisher explorer
- Advanced search
- Raw data download
- Chrome-Stats extension

chrome-stats.com

Compare and analyze Chrome extensions

All-in-one platform for competitor research, risk analysis, and growth tracking

Search extensions

127862

Extensions

27638

Themes

Chrome Web Store stats

Explore more Chrome extension statistics

Chrome-Stats makes Chrome extension metrics more accessible to everyone, enable competitive analysis, identify bad actors, and help support the growth of good Chrome extensions.

# Browser Extension Collection: Chrome-Stats

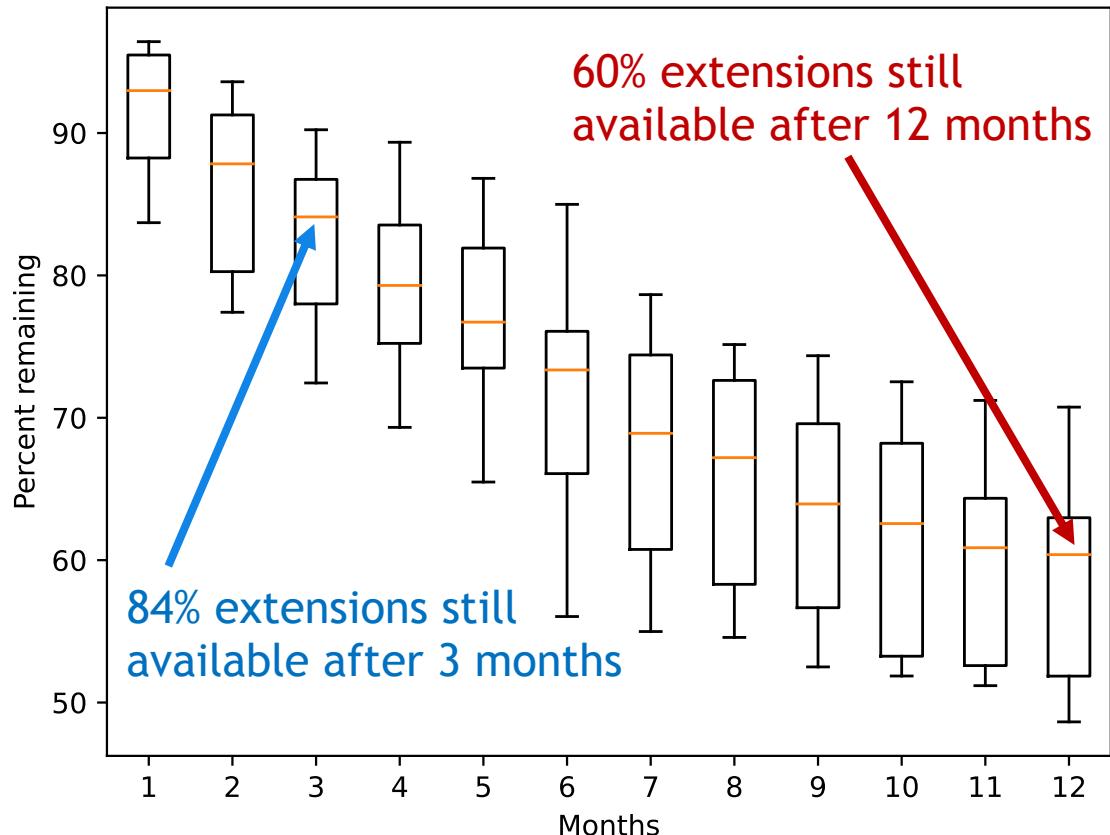
Category	#Extensions Metadata collected	#Extensions Code collected	When collected
SNE	26,014	16,377	Before May 1, 2023
- Malware-containing	10,426	6,587	Before May 1, 2023
- Policy-violating	15,404	9,638	Before May 1, 2023
- Vulnerable [1]	184	152	March 16, 2021
Benign extensions	226,762	92,482	Before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

# Life Cycle of Extensions

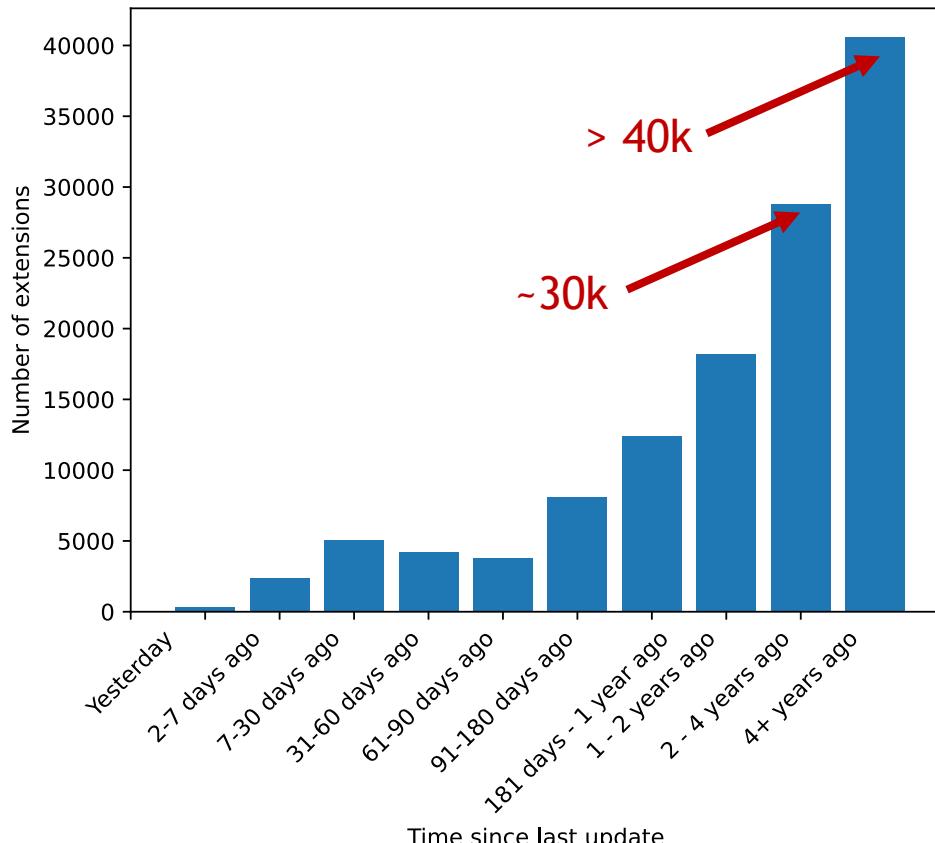
## Methodology:

- 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

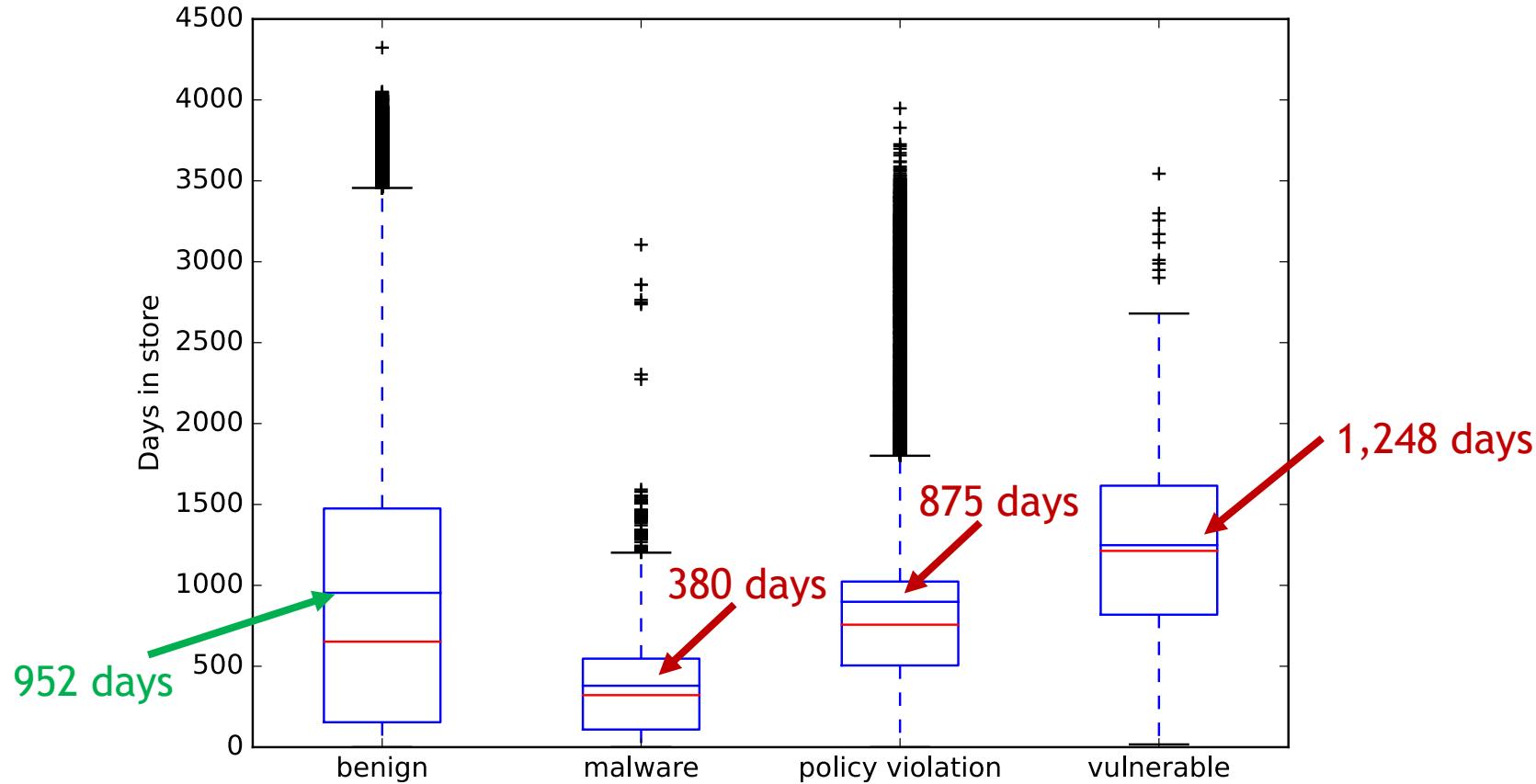


# Extension Maintenance and Security

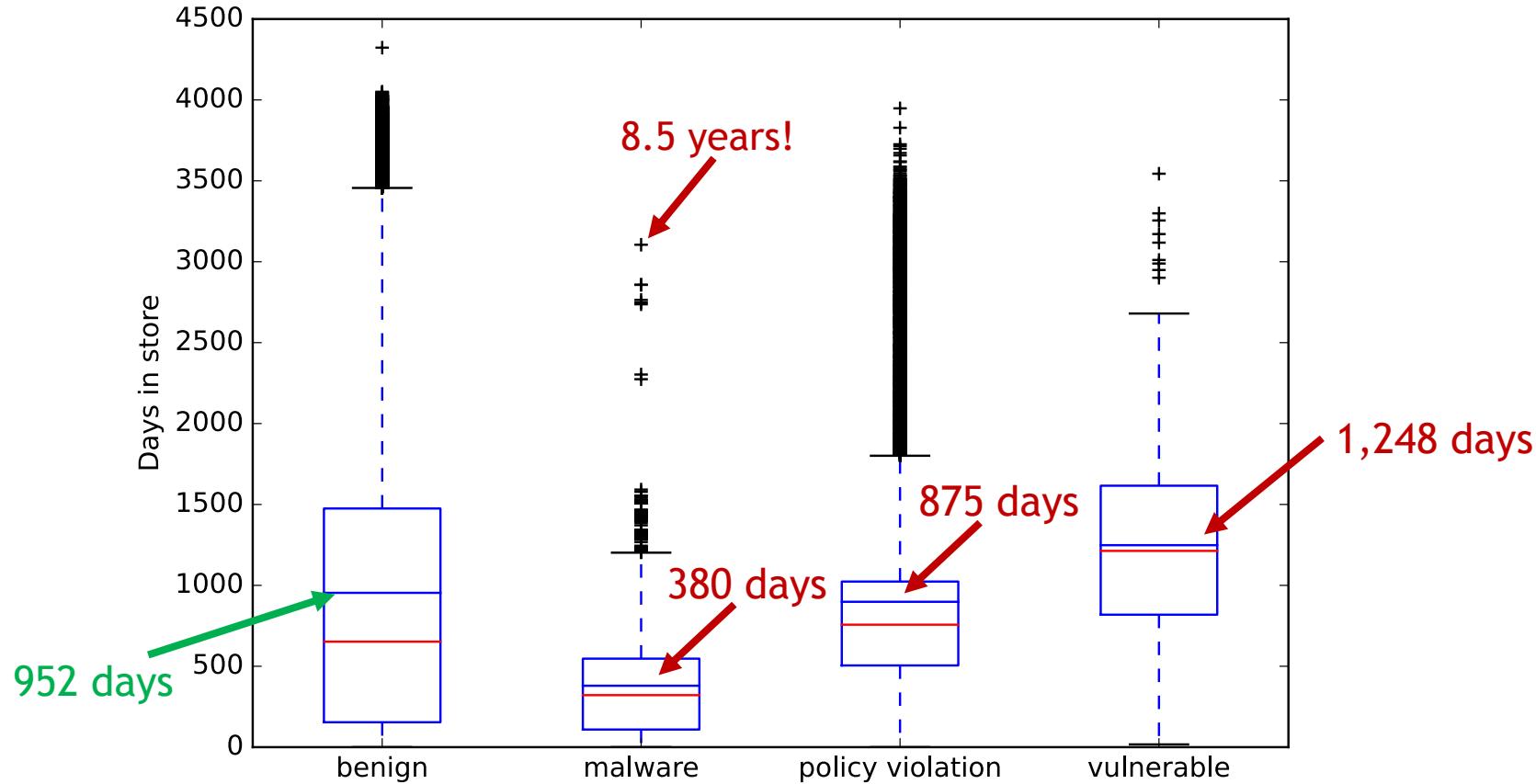


- Critical lack of maintenance in the CWS
- 60% of the extensions have never been updated
- Security & privacy implications

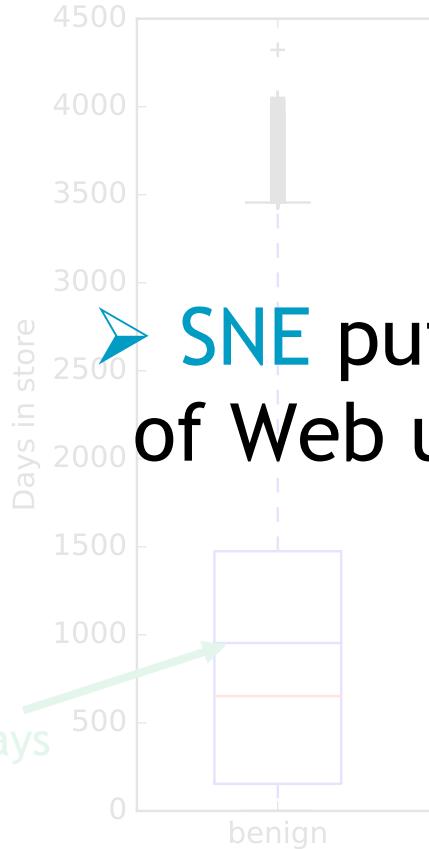
# Number of Days in the CWS



# Number of Days in the CWS



# Number of Days in the CWS

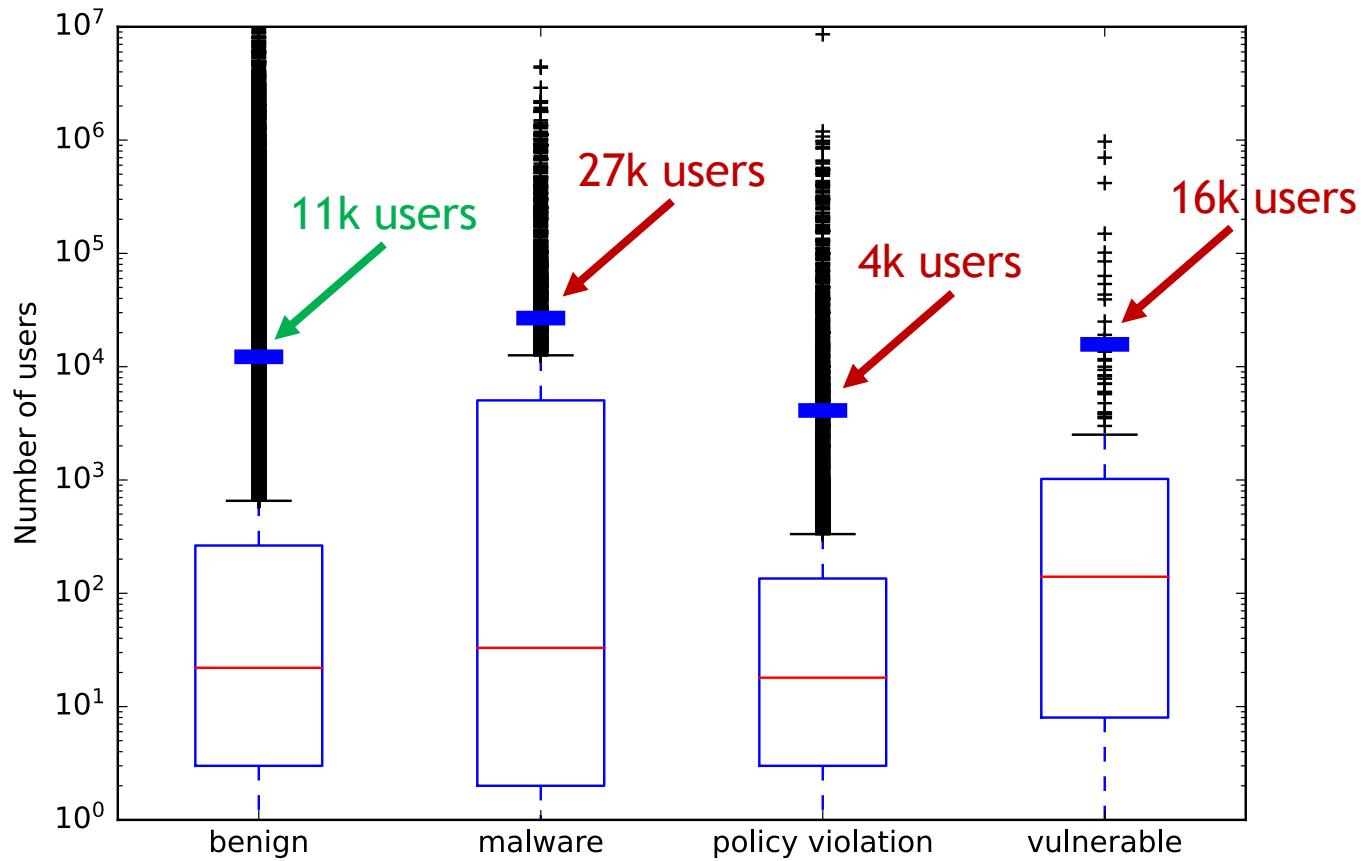


➤ SNE put the security & privacy  
of Web users **at risk *for years***

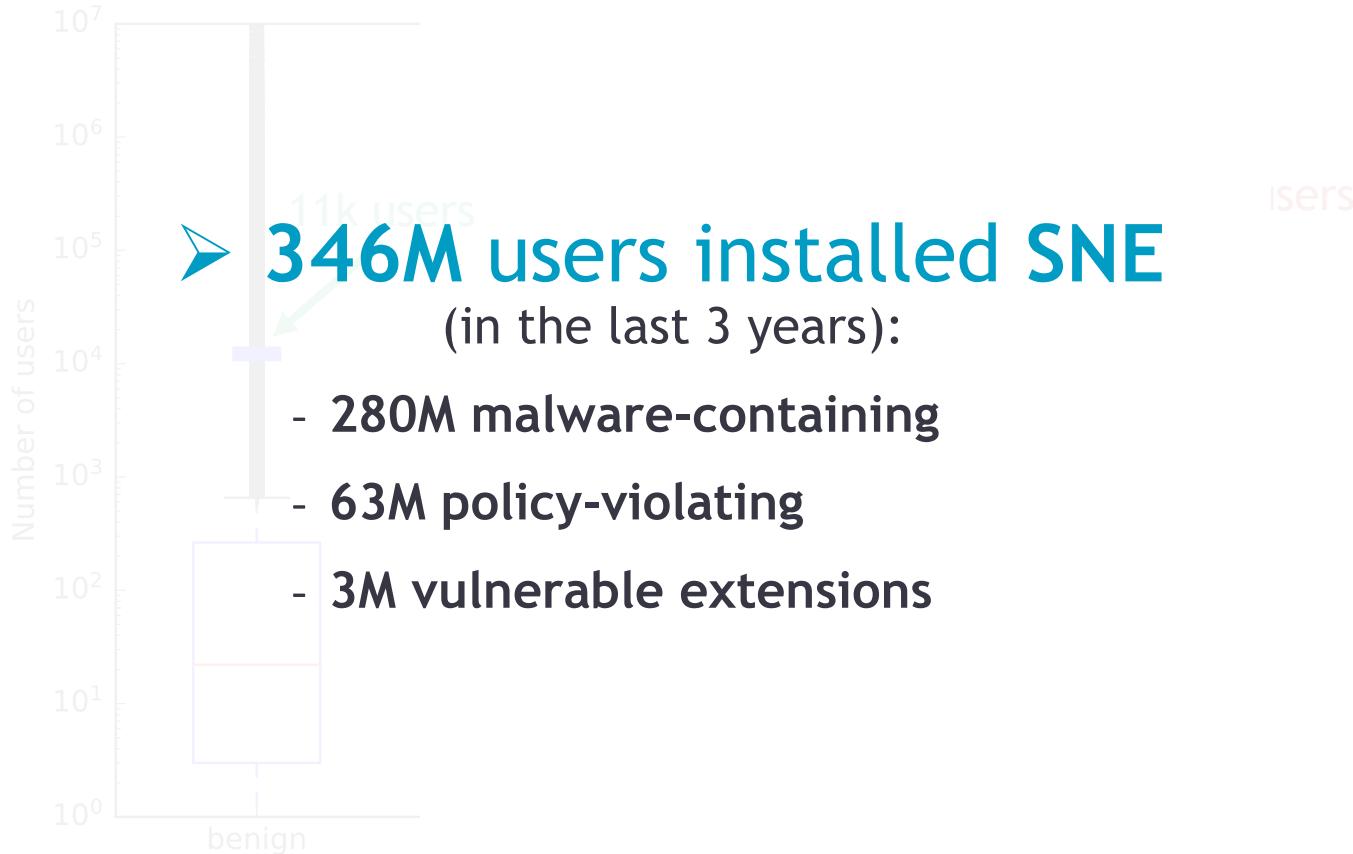
,248 days

952 days

# Number of Users



# Number of Users



# Media Coverage

**Forbes**

FORBES > INNOVATION > CYBERSECURITY

## 280 Million Google Chrome Users Installed Dangerous Extensions, Study Says

Davey Winder Senior Contributor 

Davey Winder is a veteran cybersecurity writer, hacker and analyst.

Jun 24, 2024, 06:57am EDT



How safe are Google Chrome extensions? SOPA IMAGES/LIGHTROCKET VIA GETTY IMAGES

**The Register®**

## Risk of installing dodgy extensions from Chrome store way worse than Google's letting on, study suggests

All depends on how you count it – Chocolate Factory claims 1% fail rate

Thomas Claburn

Sun 23 Jun 2024 // 10:36 UTC

 ADGUARD

Subscribe to news  Search blog 

AdGuard > Blog > Google is failing miserably at weeding out bad extensions, new research indicates

### Google is failing miserably at weeding out bad extensions, new research indicates

July 5, 2024 · 7 min read

**TECHSPOT**

TRENDING FEATURES REVIEWS THE BEST DOWNLOADS PRODUCT FINDER FORUMS

SECURITY THE WEB MALWARE CHROME

## Researchers say 280 million people have installed malware-infected Chrome extensions in the last 3 years

Google claims less than 1% of all installs include malware

By Rob Thubron June 24, 2024 at 11:39 AM



# 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

– Exploit the web browser to download and execute malicious code

– E.g., can lead to user-sensitive data exfiltration or destruction

## ▪ Violate the Chrome Web Store policies

– Exploit the web browser to download and execute malicious code

## ▪ 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*)



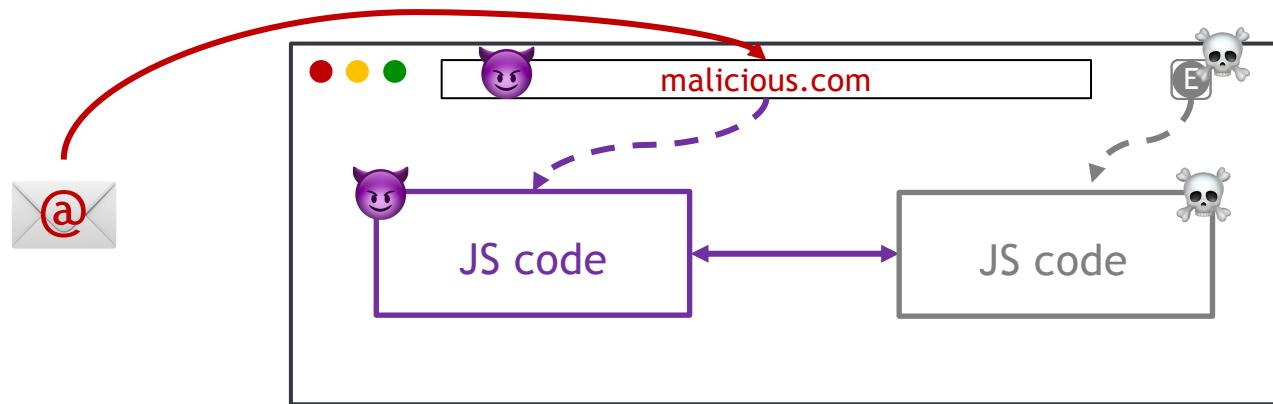
# Analysis of Vulnerable Extensions

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



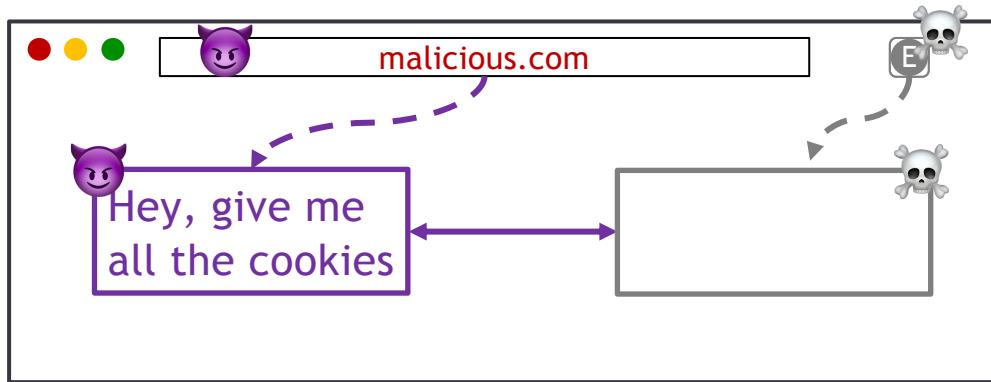
# Analysis of Vulnerable Extensions

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



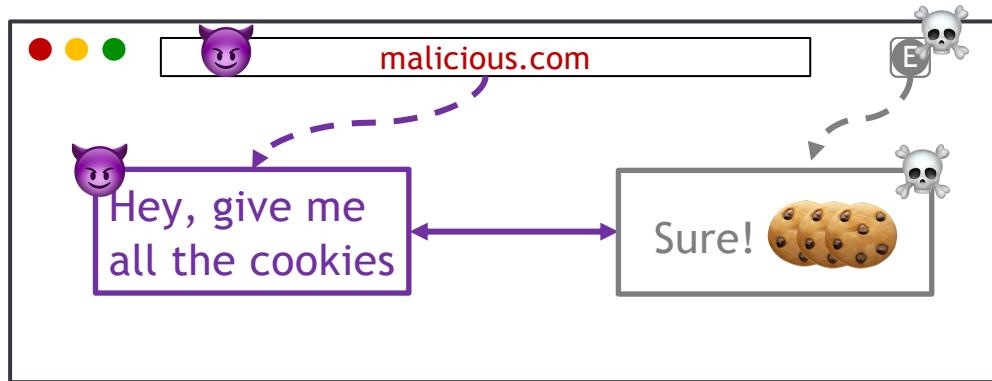
# Analysis of Vulnerable Extensions

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



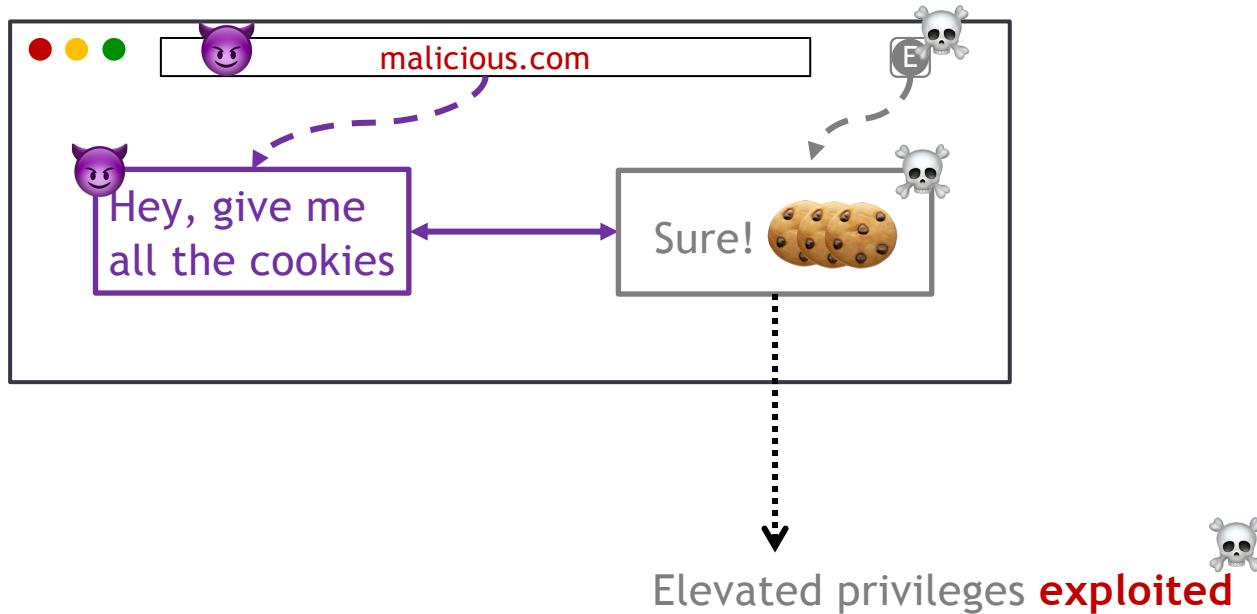
# Analysis of Vulnerable Extensions

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



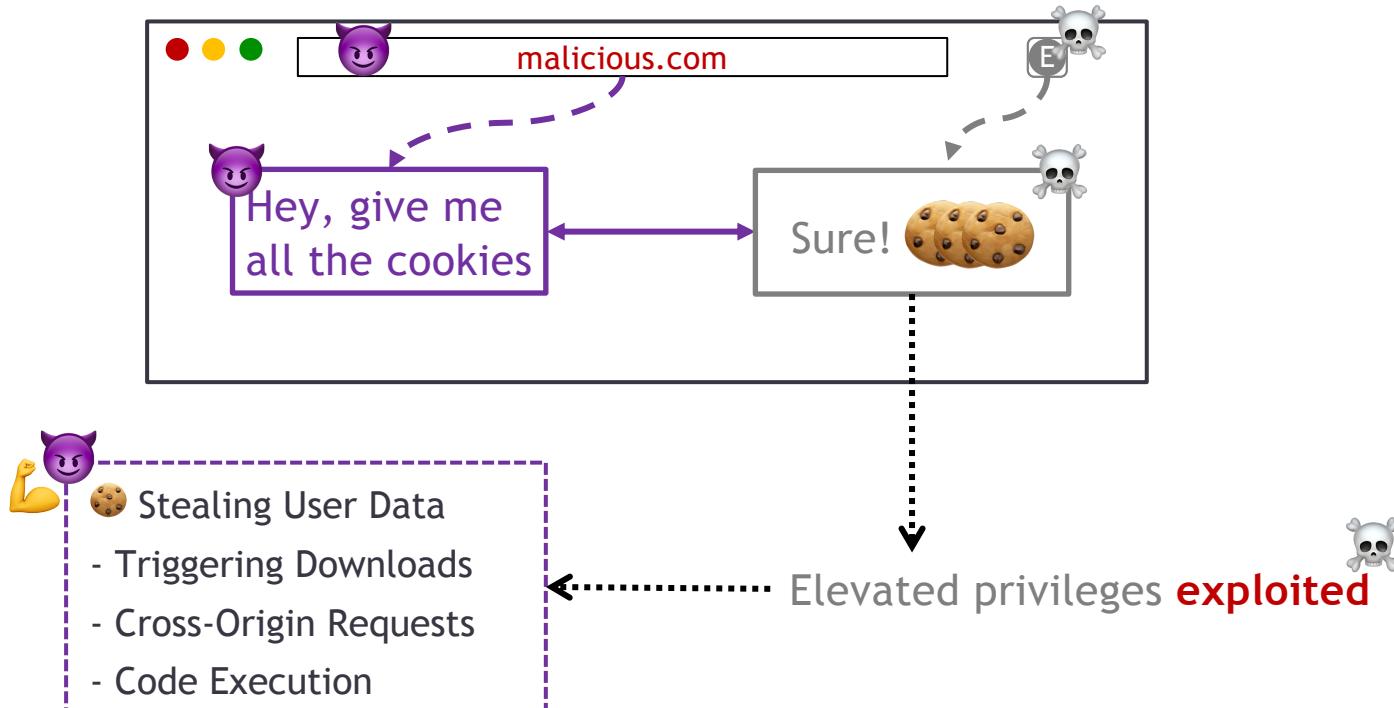
# Analysis of Vulnerable Extensions

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



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



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



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



Malicious web page



# Detecting Vulnerable Extensions



CISPA  
HELMHOLTZ CENTER FOR  
INFORMATION SECURITY

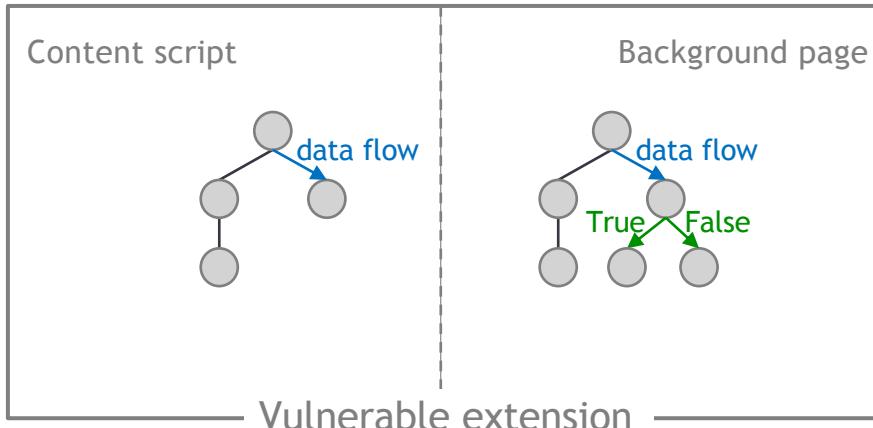


## > DOUBLEX: Statically Detecting Vulnerable Data Flows in Browser Extensions

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



Malicious web page



### Per-component JS code abstraction

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

# Detecting Vulnerable Extensions

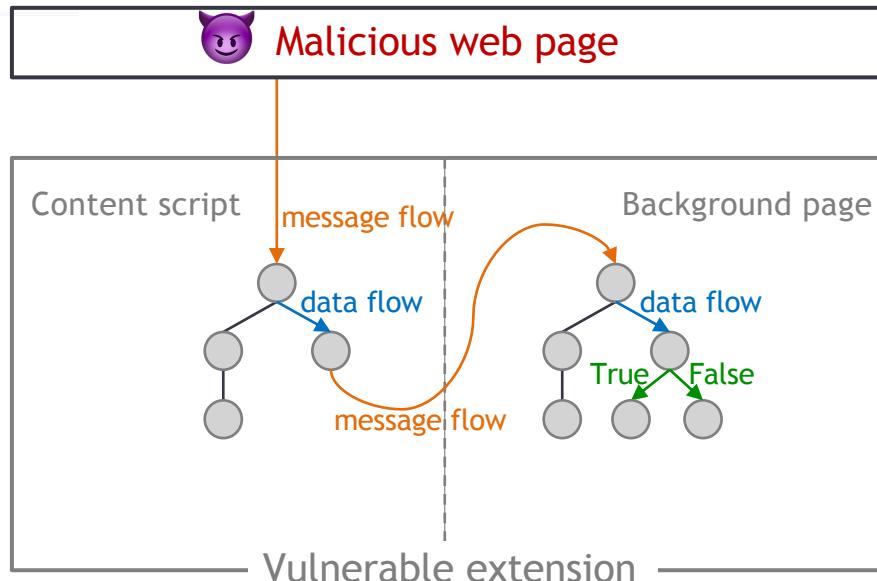


CISPA  
HELMHOLTZ CENTER FOR  
INFORMATION SECURITY



## > 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

# Detecting Vulnerable Extensions

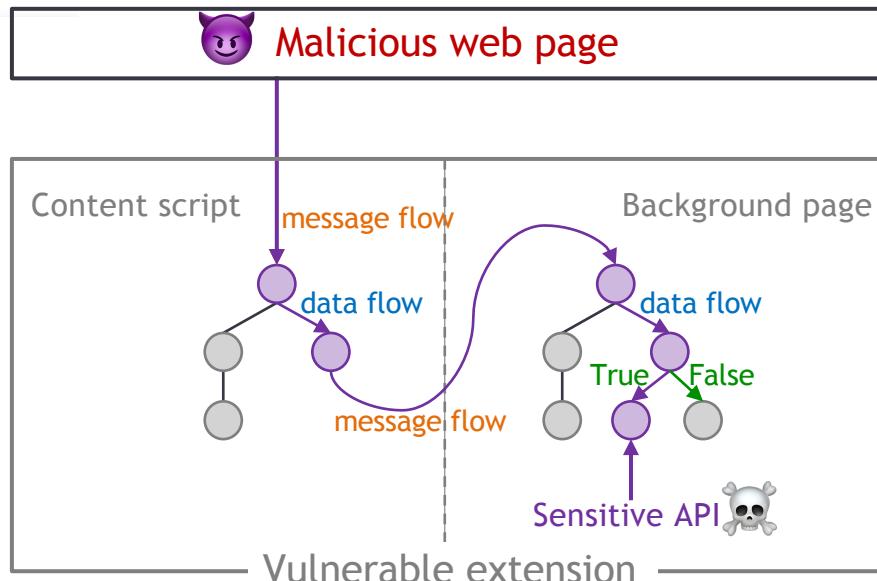


CISPA  
HELMHOLTZ CENTER FOR  
INFORMATION SECURITY



## > 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)

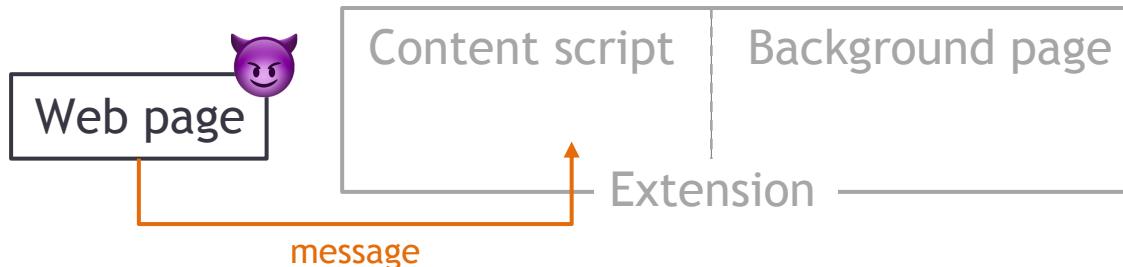
- Message interactions

### Suspicious data flow tracking

- Detects any path between an attacker & sensitive APIs

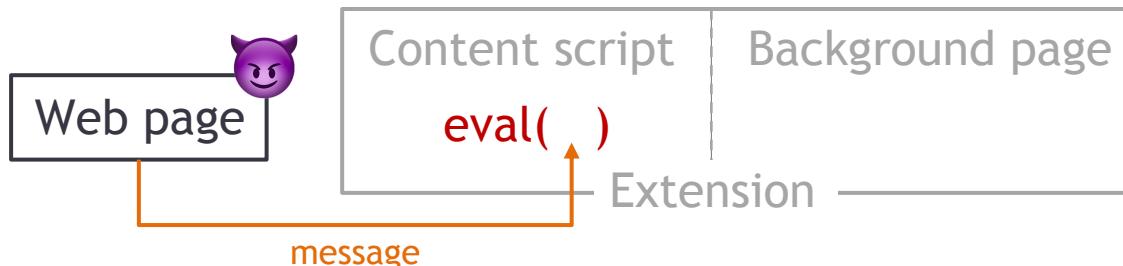
# Simplified Example of a Vulnerability

```
// 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

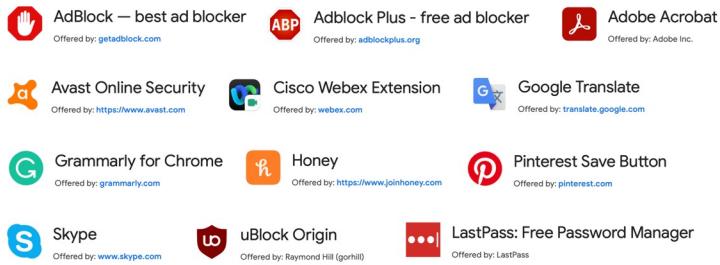
- **184 vulnerable Chrome extensions**
- Impacting **3M users**
- **Precision:** 89% of the flagged extensions are vulnerable
- **Recall:** 93% of known vulnerabilities [2] are detected
- **Integration** in the **vetting process** conducted by Google
- **Available online**, for developers
  - (even in other fields!)



 Aurore54F/DoubleX

# Takeaways – Browser Extension (In)Security

## Browser Extensions are Popular



- 125k Chrome extensions totaling over 1.6B active users

## What is in the Chrome Web Store?

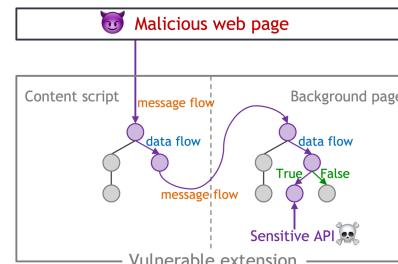


- 350M users installed SNE in the last 3 years
- These SNE stay in the Chrome Web Store *for years*
- Extensions have a **short life cycle** in the CWS (60% stay 1 year)
- Critical **lack of maintenance** in the CWS (60% received no update)

## Security-Noteworthy Extensions (SNE)

- **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

## Detecting Vulnerable Extensions with 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