

# Browser Extension (In)Security

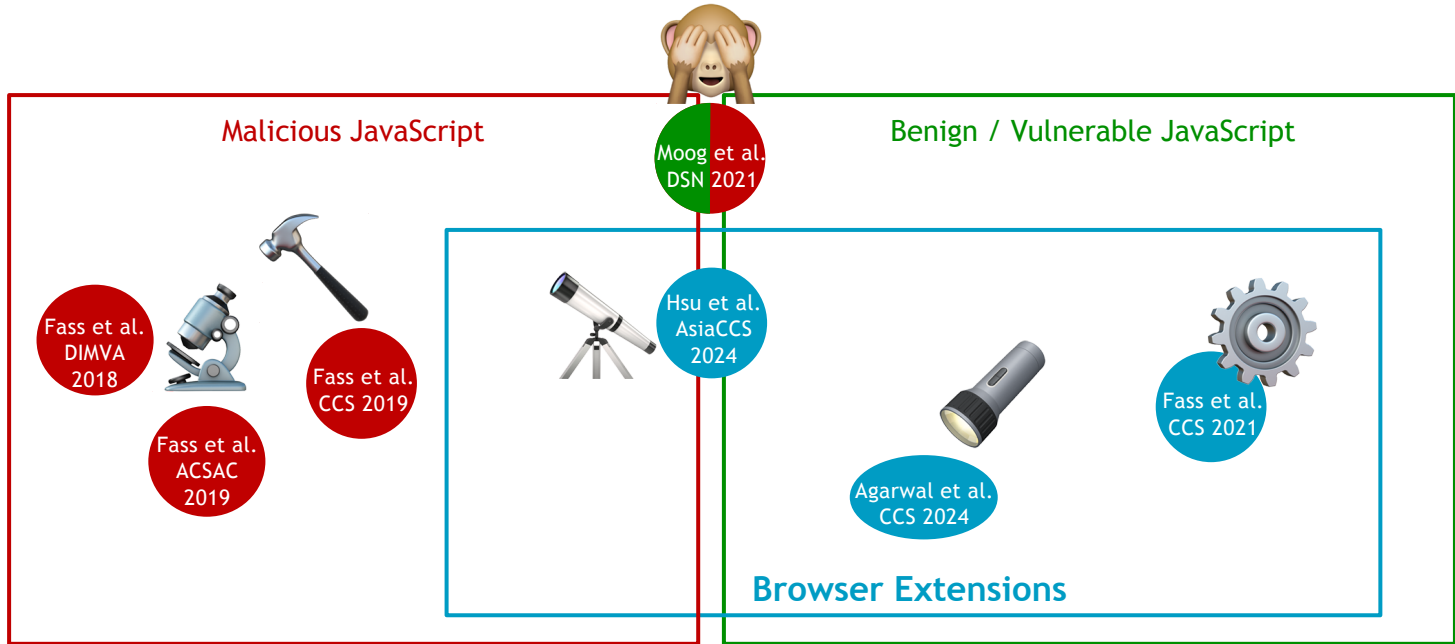
Aurore Fass

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

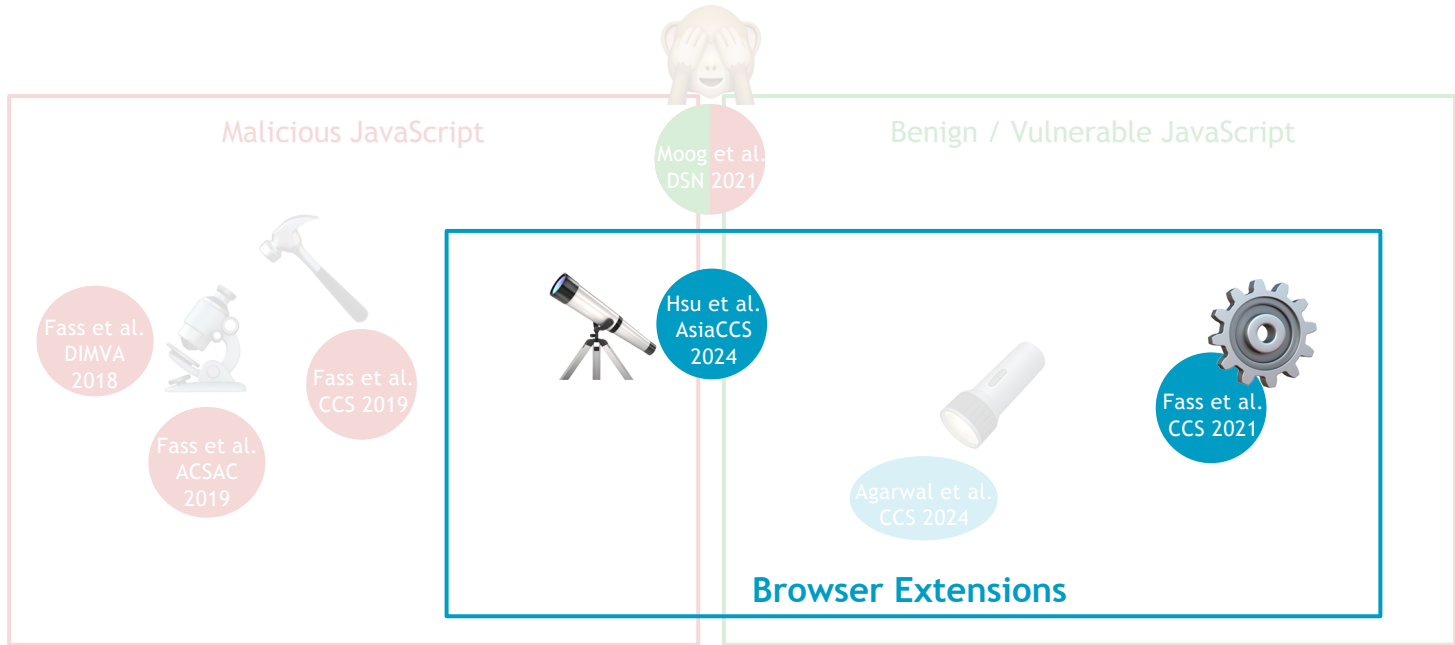
Spirals Seminar, Lille, December 5<sup>th</sup>, 2024



# Research Work: Web Security & Privacy



# Research Work: Web Security & Privacy



# What are Browser Extensions?

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



**Adblock** — best ad blocker

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



**Adblock Plus** - free ad blocker

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



**Adobe Acrobat**

Offered by: Adobe Inc.



**Avast Online Security**

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



**Cisco Webex Extension**

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



**Google Translate**

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



**Grammarly for Chrome**

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



**Honey**

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



**Pinterest Save Button**

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



**Skype**

Offered by: [www.skype.com](https://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** 

→ 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**?

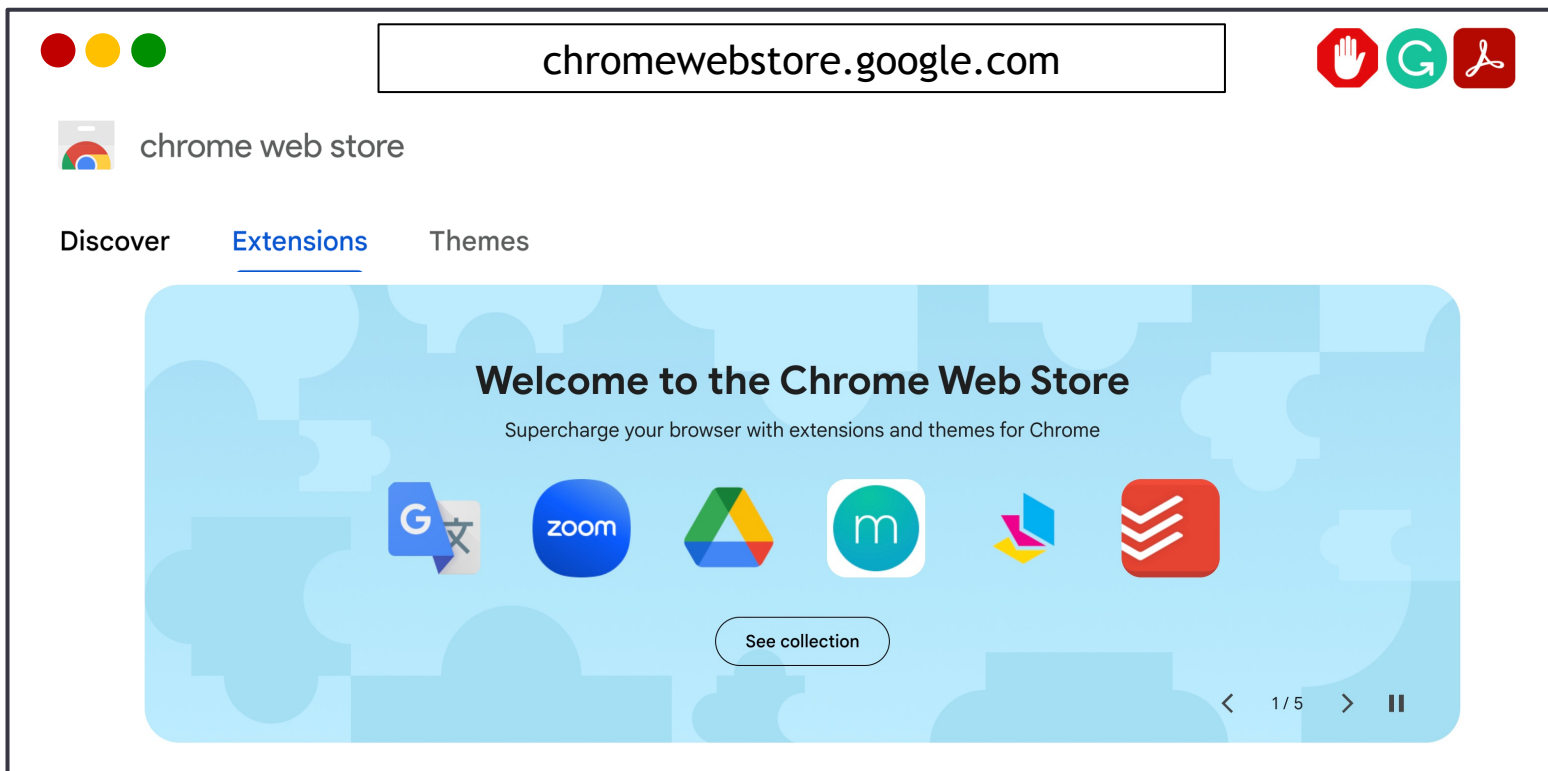


> What is in the Chrome Web Store?



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

# How to Install Extensions or SNE?





# How to Install Extensions or SNE?



The screenshot shows a browser window with the address bar containing `chromewebstore.google.com`. The page title is "chrome web store". The navigation menu includes "Discover", "Extensions", and "Themes". A large blue banner features the text **>26k SNE** (in the last 3 years) in red. Below the text is a "See collection" button. The banner also includes a "Welcome to the Chrome Web Store" message and a "Subscribe to our newsletter" link. The background of the banner shows various extension icons like Google Assistant, Zoom, and a list icon. Navigation controls at the bottom right of the banner include a left arrow, "1/5", a right arrow, and a pause icon.

# Browser Extension Collection: Chrome-Stats

chrome-stats.com

Compare and analyze Chrome extensions  
All-in-one platform for competitor research, risk analysis, and growth tracking

127 862 Extensions      27 638 Themes

Chrome Web Store stats

Number of extension

Extensions Themes

03-07 04-10 05-16 06-20 07-28 08-31 09-05 04-09 04-10 04-16 04-21 04-24 04-27 04-30 05-05 05-08 05-12 05-15 05-18 05-21 05-24 05-27 05-30 06-02

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.

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

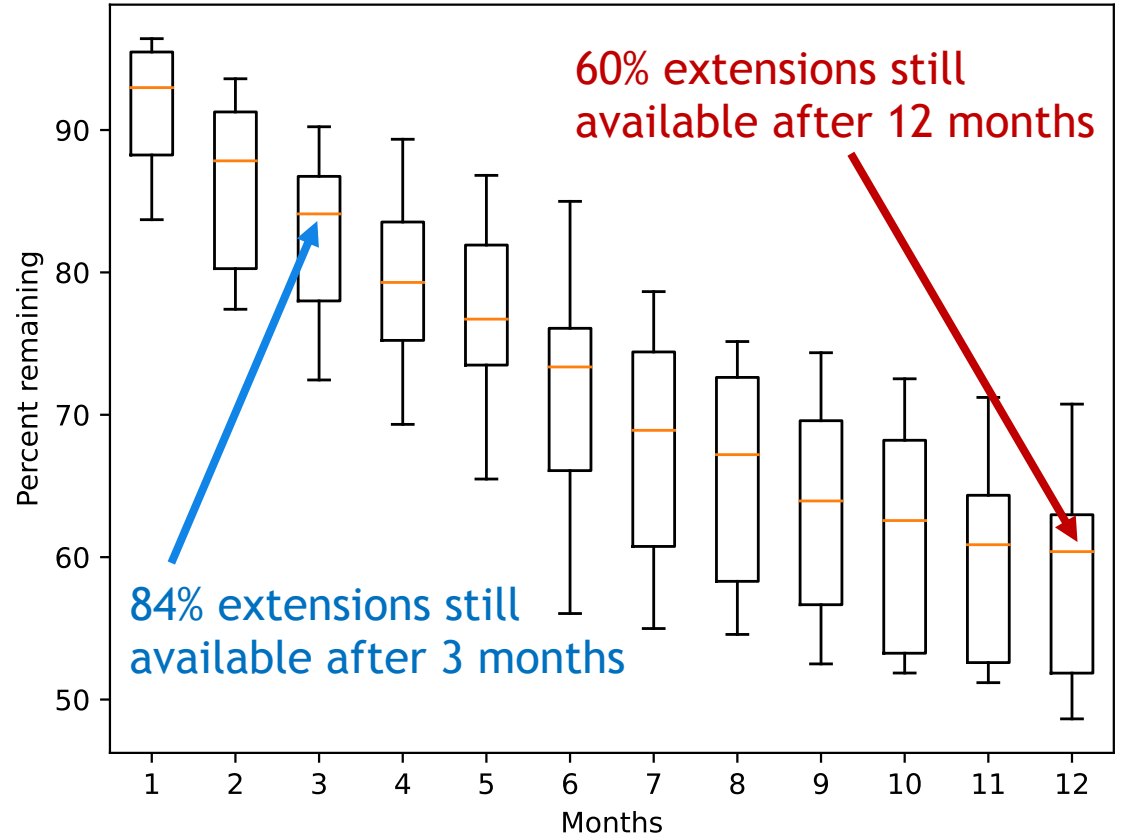
# Life Cycle of Extensions

## Methodology:

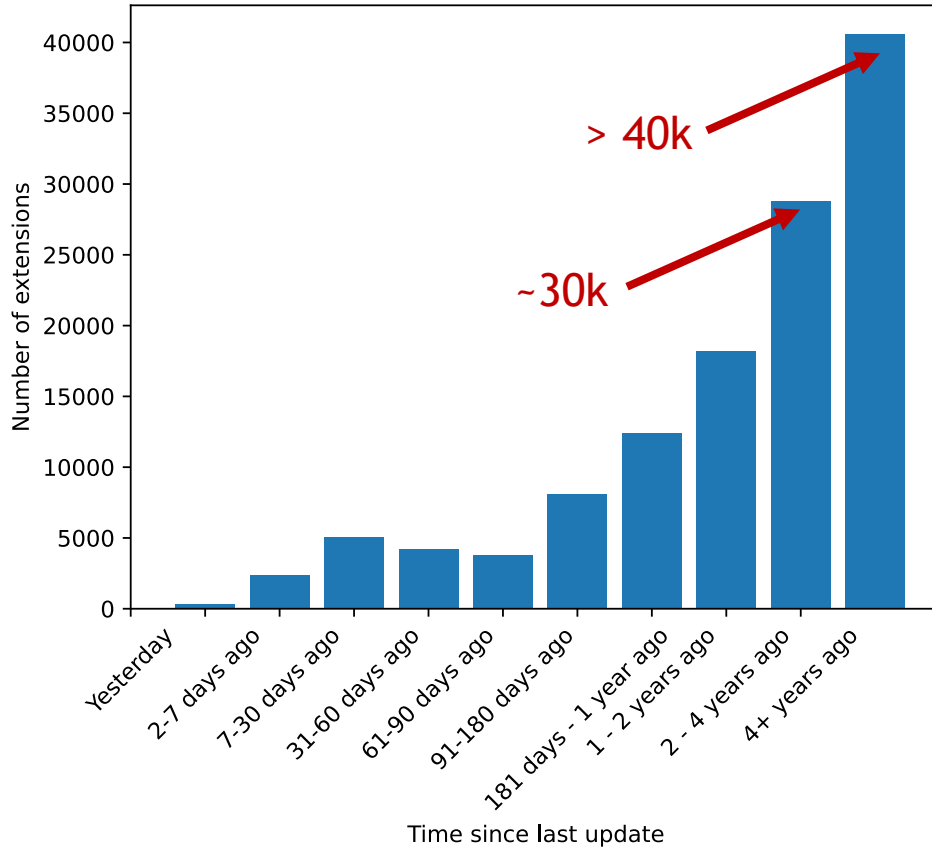
- Collected extensions added to the CWS in Jan–Dec 2021
- Computed the percentage of those extensions still in the CWS 1, 2, ..., 12 months later

➤ Extensions have a very short life cycle

➤ Analyses on the CWS should be run regularly

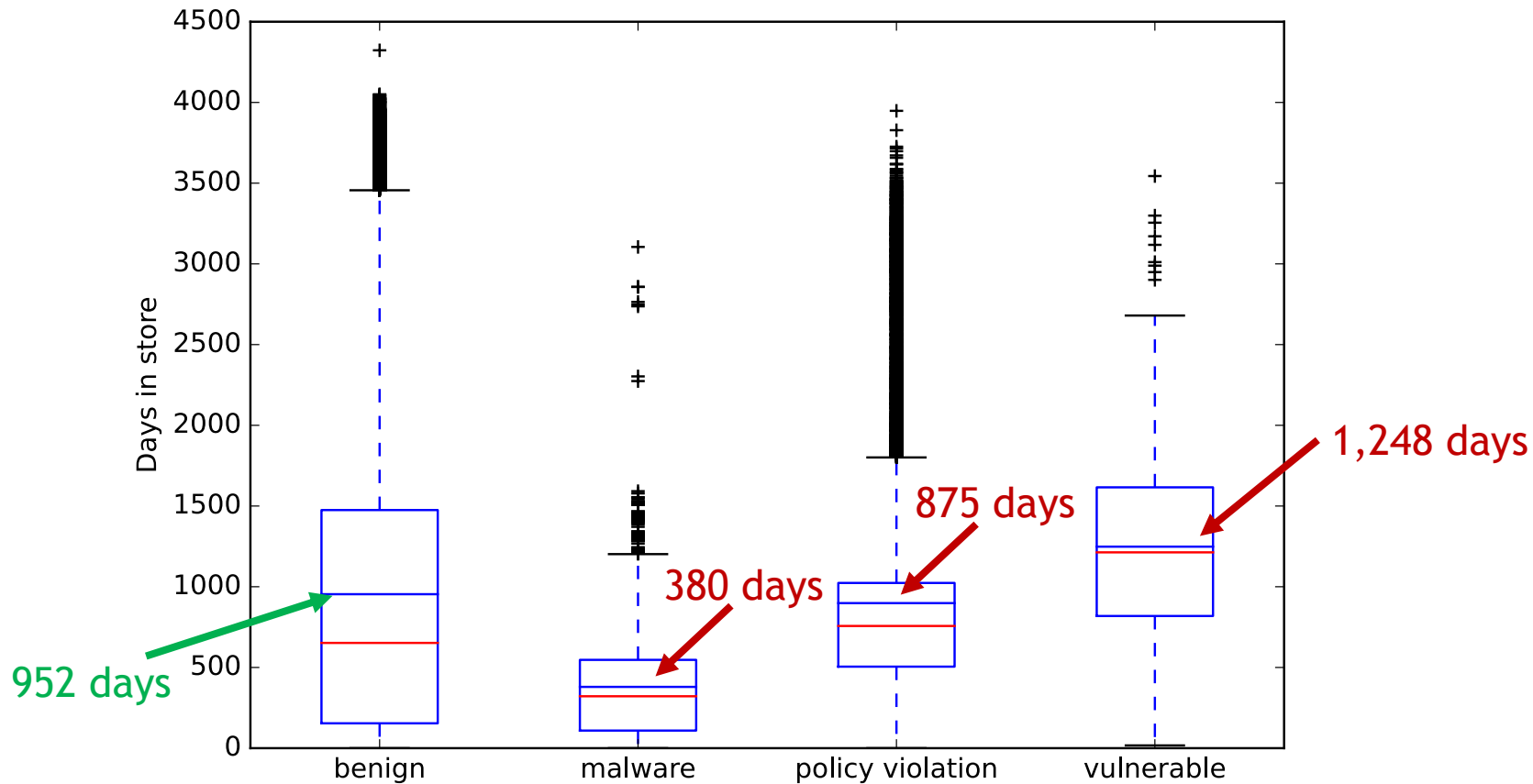


# Extension Maintenance and Security

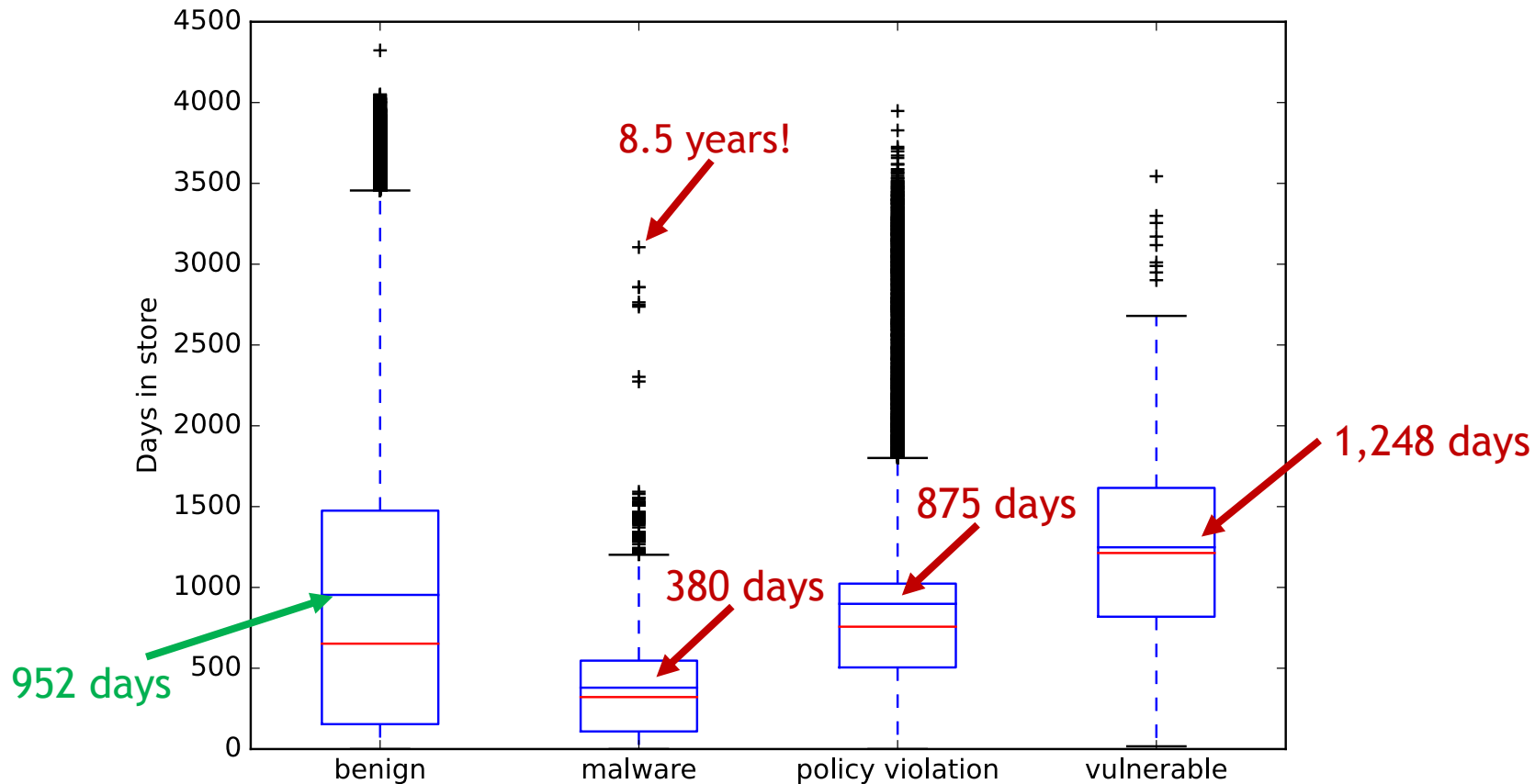


- Critical **lack of maintenance** in the CWS
- **60%** of the extensions have **never been updated**
- **Security & privacy implications**

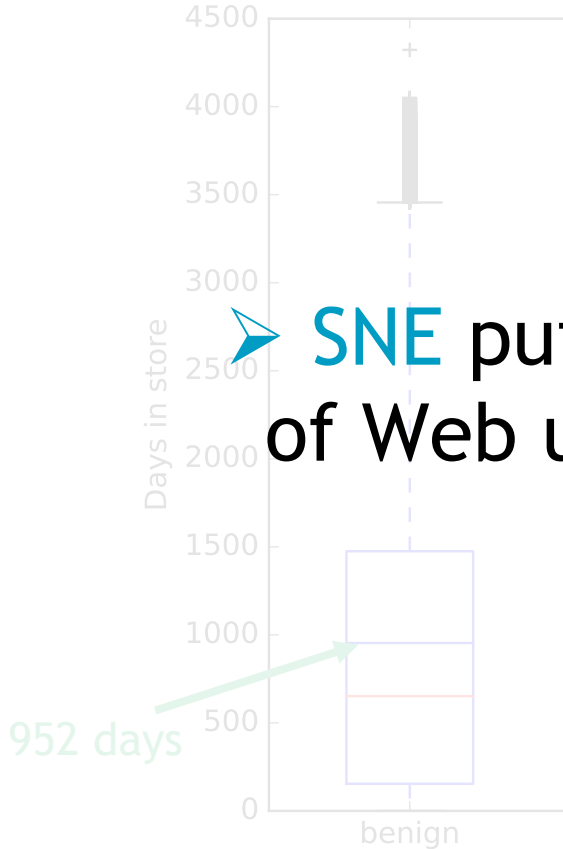
# Number of Days in the CWS



# Number of Days in the CWS



# Number of Days in the CWS

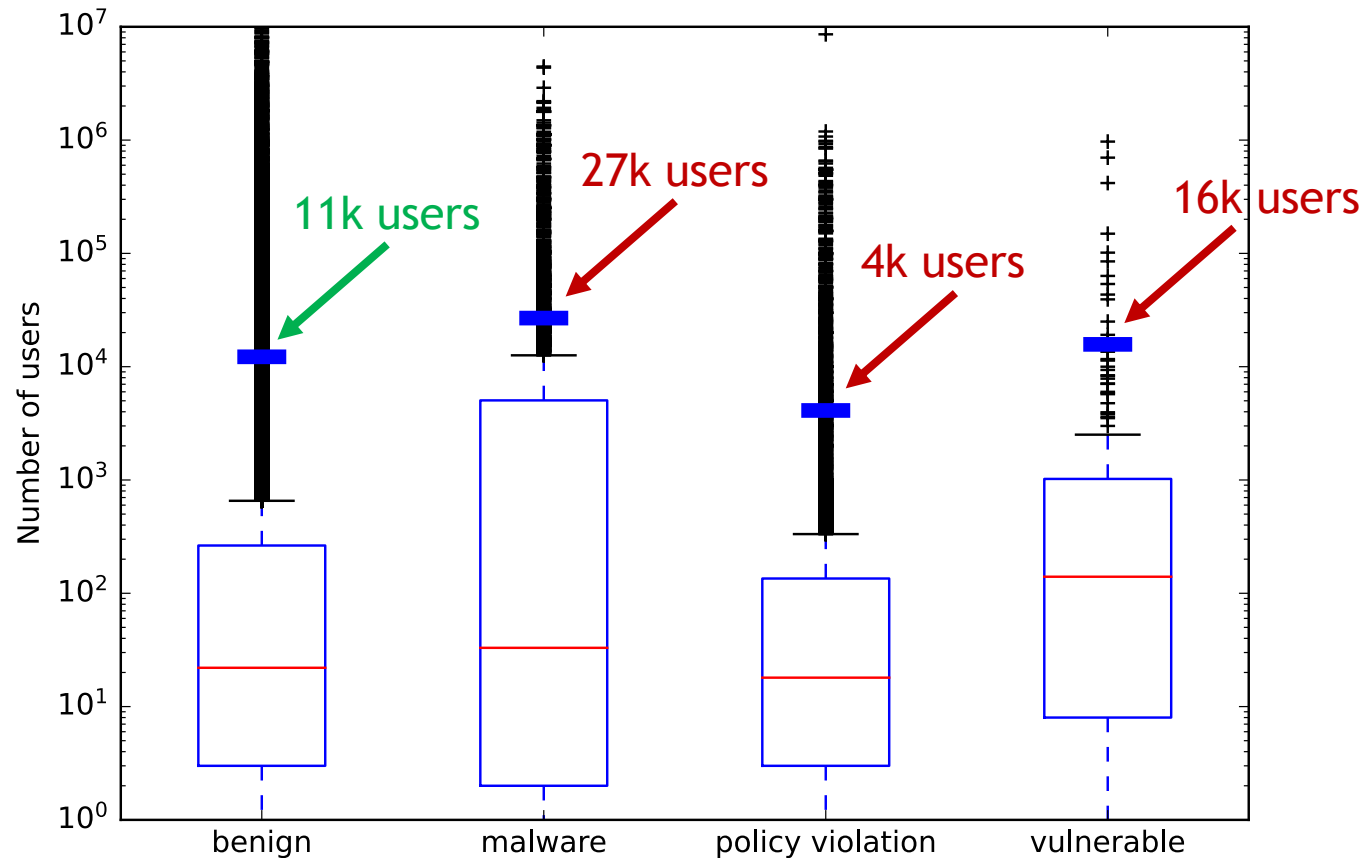


➤ SNE put the security & privacy of Web users *at risk for years*

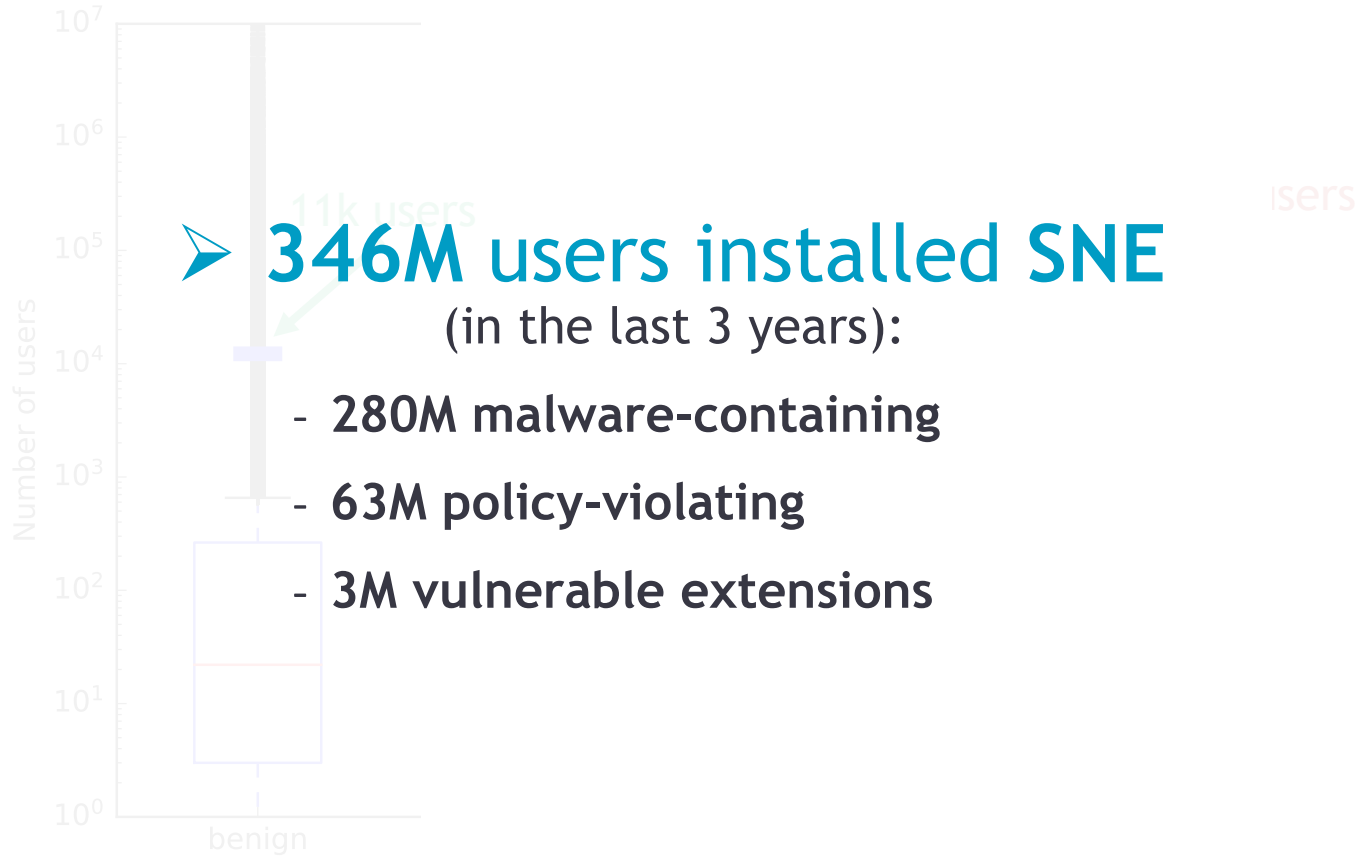
,248 days



# 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.*

Follow

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

A<sup>5</sup>

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**



Fass et al.  
CCS 2021

- Designed by well-intentioned developers... but contain some vulnerabilities
- E.g., can lead to user-sensitive data exfiltration

- 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**



Fass et al.  
CCS 2021

- Designed by well-intentioned developers... but contain some vulnerabilities

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

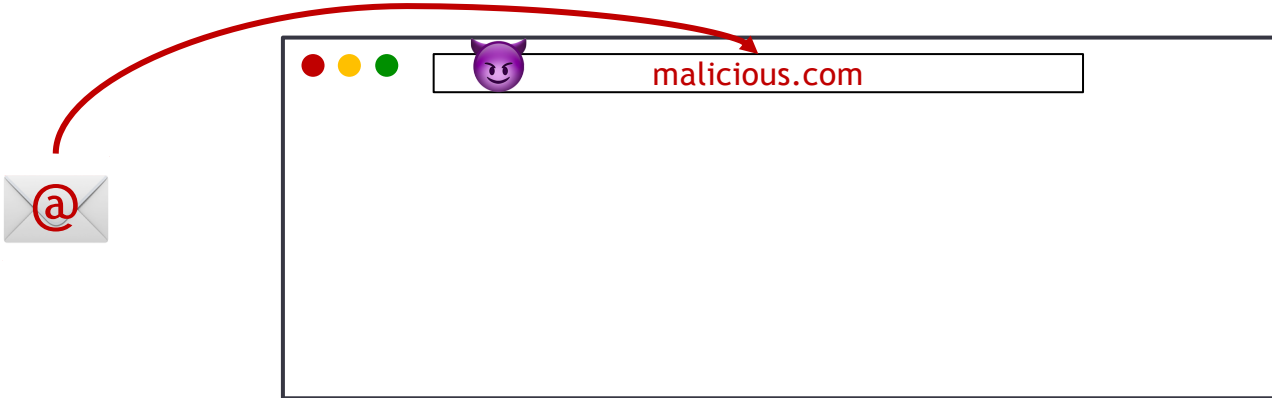
# Analysis of Vulnerable Extensions

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



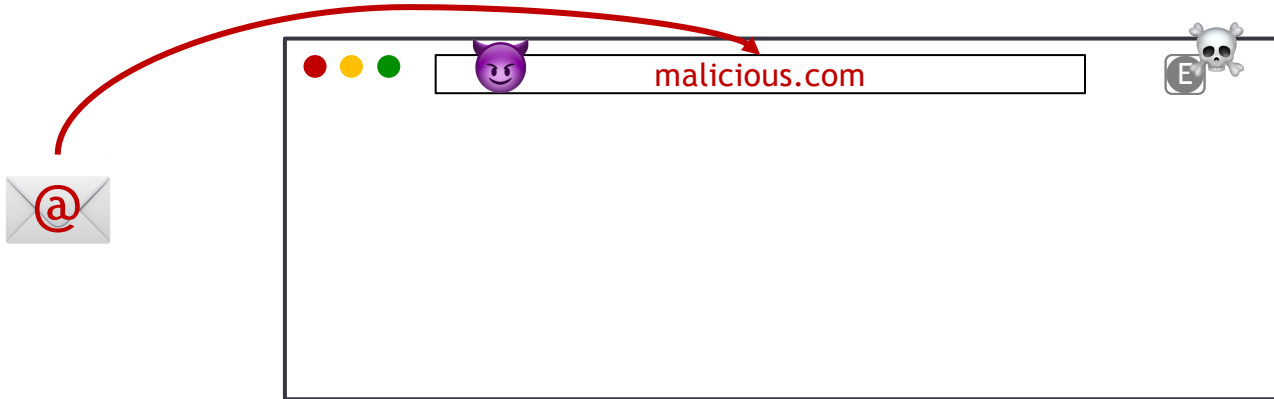
# Analysis of Vulnerable Extensions

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



# Analysis of Vulnerable Extensions

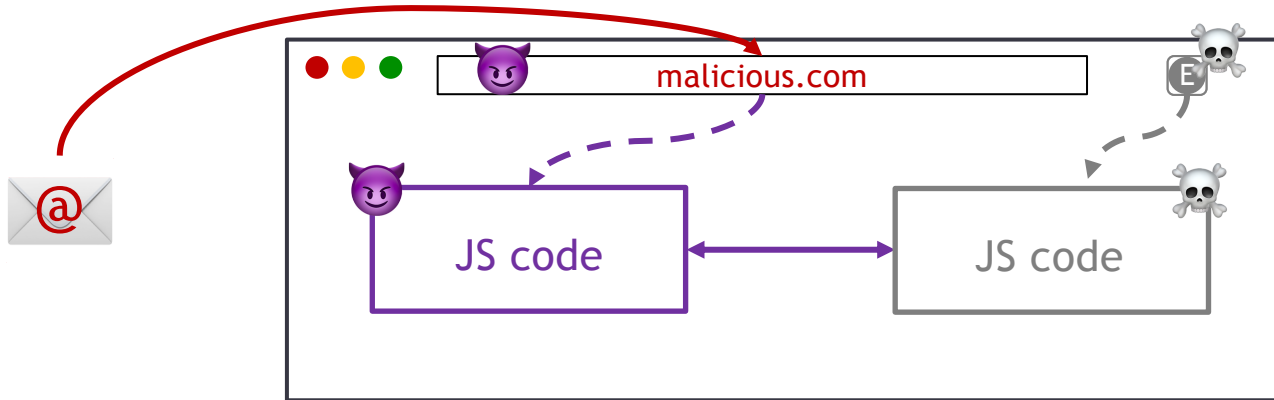
Challenging to detect due to their inherently benign intent (*benign-but-buggy*)





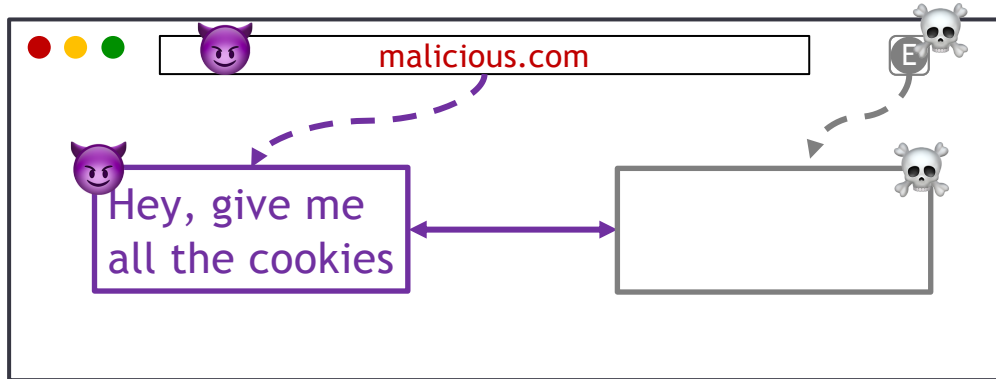
# Analysis of Vulnerable Extensions

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



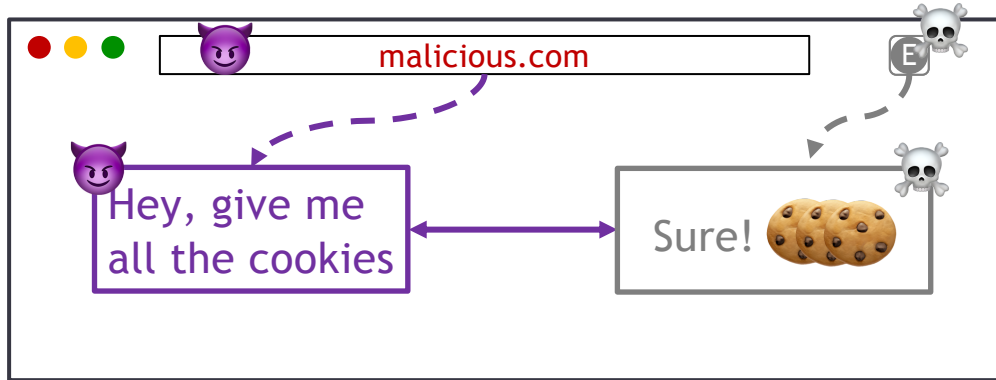
# Analysis of Vulnerable Extensions

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



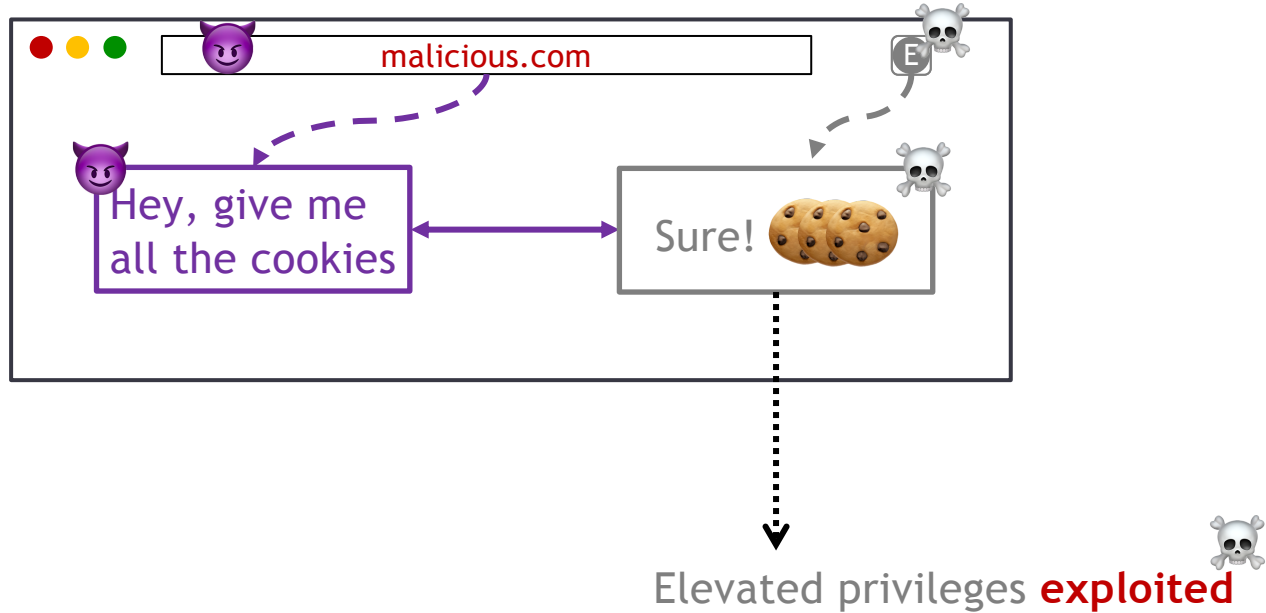
# Analysis of Vulnerable Extensions

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



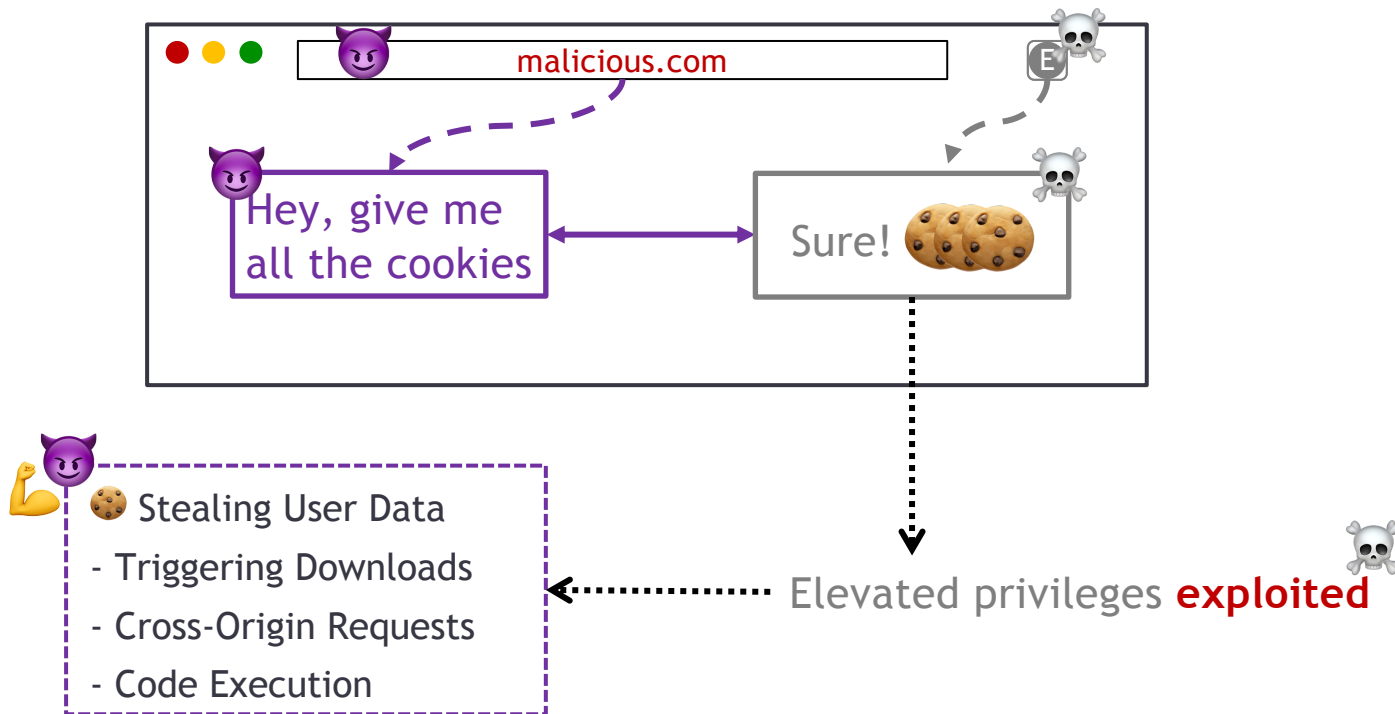
# Analysis of Vulnerable Extensions

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

**DOUBLEX: Statically Detecting Vulnerable Data Flows in Browser Extensions at Scale**  
Aurore Fass, Dolière Francis Somé, Michael Backes, and Ben Stock  
2021 ACM Conference on Computer and Communications Security (CCS '21)

**Abstract**  
Browser extensions are a popular way to customize and extend the functionality of web browsers. However, they are also a common source of security vulnerabilities. In this paper, we present DOUBLEX, a static analysis tool for detecting vulnerable data flows in browser extensions. DOUBLEX is designed to be efficient and scalable, and is able to analyze millions of extensions. We evaluate DOUBLEX on a large dataset of browser extensions and show that it is able to detect a wide range of vulnerabilities, including data leaks, data tampering, and unauthorized access to sensitive information. We also show that DOUBLEX is able to detect vulnerabilities in extensions that have not been previously identified by other tools.

**1 Introduction**  
Browser extensions are a popular way to customize and extend the functionality of web browsers. However, they are also a common source of security vulnerabilities. In this paper, we present DOUBLEX, a static analysis tool for detecting vulnerable data flows in browser extensions. DOUBLEX is designed to be efficient and scalable, and is able to analyze millions of extensions. We evaluate DOUBLEX on a large dataset of browser extensions and show that it is able to detect a wide range of vulnerabilities, including data leaks, data tampering, and unauthorized access to sensitive information. We also show that DOUBLEX is able to detect vulnerabilities in extensions that have not been previously identified by other tools.

**CCS Highlights**  
DOUBLEX is a static analysis tool for detecting vulnerable data flows in browser extensions. DOUBLEX is designed to be efficient and scalable, and is able to analyze millions of extensions. We evaluate DOUBLEX on a large dataset of browser extensions and show that it is able to detect a wide range of vulnerabilities, including data leaks, data tampering, and unauthorized access to sensitive information. We also show that DOUBLEX is able to detect vulnerabilities in extensions that have not been previously identified by other tools.

**Keywords**  
Browser extensions, static analysis, data flows, security vulnerabilities.

> **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



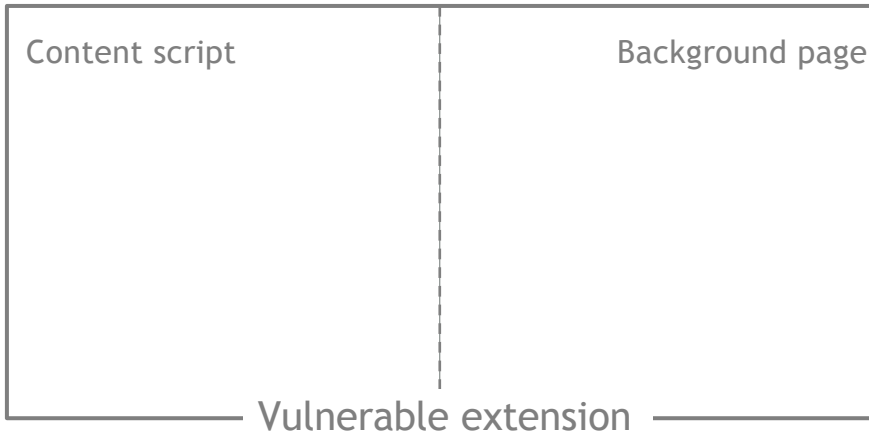
Fass et al.  
CCS 2021

**DOUBLEX: Statically Detecting Vulnerable Data Flows in Browser Extensions at Scale**  
Aurore Fass, Dolière Francis Somé, Michael Backes, and Ben Stock  
1 Introduction

**Abstract**  
Browser extensions are a popular way to extend the functionality of web browsers. However, they are often developed by third parties and can be vulnerable to attacks. This paper presents DOUBLEX, a static analysis tool that detects vulnerable data flows in browser extensions. DOUBLEX is designed to be scalable and accurate, and is able to detect a wide range of vulnerabilities. We evaluate DOUBLEX on a large dataset of browser extensions and show that it is able to detect a high number of vulnerabilities. We also show that DOUBLEX is able to detect vulnerabilities that other tools are unable to detect.

**CCS keywords**  
Software security, Web browsers, Browser extensions, Static analysis, Vulnerability detection, Data flows, Security, Information security, Software security, Web browsers, Browser extensions, Static analysis, Vulnerability detection, Data flows, Security, 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





**DOUBLEX: Statically Detecting Vulnerable Data Flows in Browser Extensions at Scale**  
Aurore Fass, Dolie Francis Somé, Michael Backes, and Ben Stock  
1 Introduction

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

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



Malicious web page

Content script

Background page

Vulnerable extension



# 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  
CCS 2021

**Abstract**  
Browser extensions are a popular way to customize web browsing. However, they are also a common source of security vulnerabilities. In this paper, we present DOUBLEX, a static analysis tool that detects vulnerable data flows in browser extensions. DOUBLEX is based on a novel abstraction of JavaScript code that allows for the detection of data flows that are vulnerable to information leakage. We evaluate DOUBLEX on a large dataset of browser extensions and show that it can detect a significant number of vulnerabilities that were previously undetected.

**1 Introduction**  
Browser extensions are a popular way to customize web browsing. However, they are also a common source of security vulnerabilities. In this paper, we present DOUBLEX, a static analysis tool that detects vulnerable data flows in browser extensions. DOUBLEX is based on a novel abstraction of JavaScript code that allows for the detection of data flows that are vulnerable to information leakage. We evaluate DOUBLEX on a large dataset of browser extensions and show that it can detect a significant number of vulnerabilities that were previously undetected.

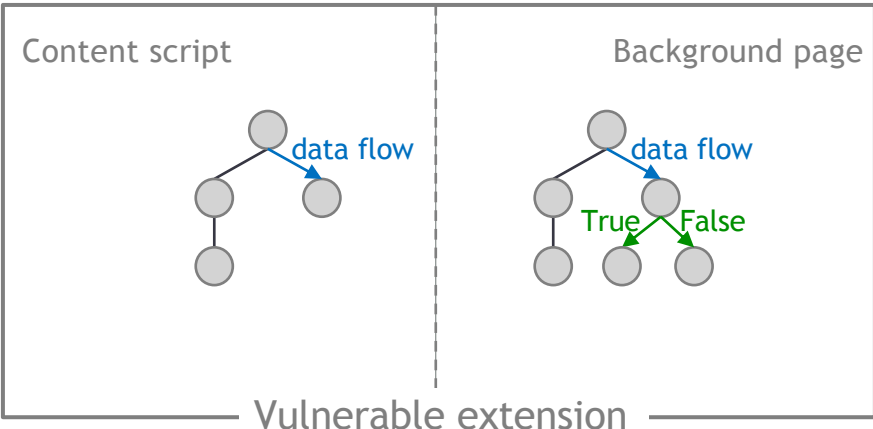
**CCS keywords**  
Security and privacy, Web applications, Browser extensions

**Keywords**  
Static analysis, JavaScript, Browser extensions, Information leakage, Vulnerability detection

## > 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



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

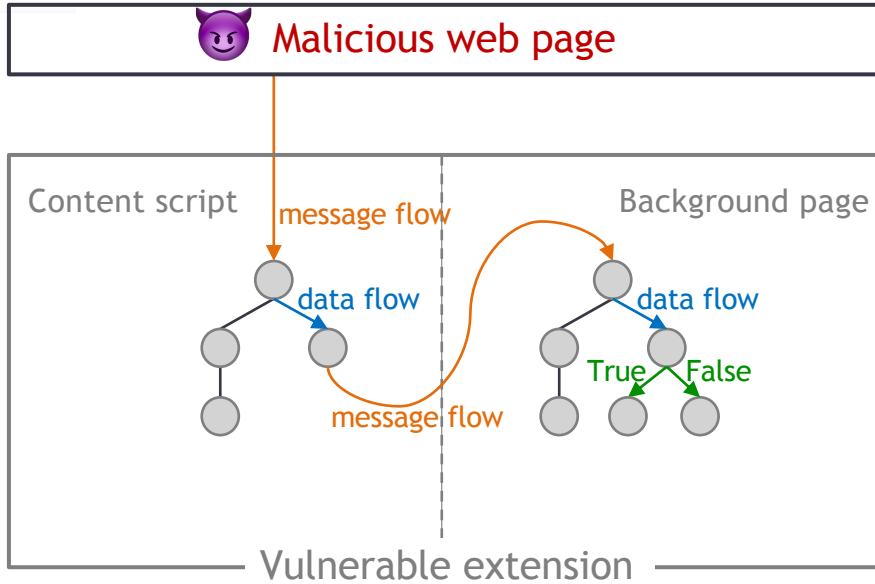
**DOUBLEX: Statically Detecting Vulnerable Data Flows in Browser Extensions at Scale**  
Aurore Fass, Dolière Francis Somé, Michael Backes, and Ben Stock  
CCS 2021

**Abstract**  
Browser extensions are a popular way to customize web browsing. However, they are often vulnerable to attacks. We present DOUBLEX, a static analysis tool that detects vulnerable data flows in browser extensions. DOUBLEX is the first tool to detect vulnerable data flows in browser extensions at scale. It is based on a novel abstraction of browser extensions and a new data flow analysis. DOUBLEX has been evaluated on a large dataset of browser extensions and has detected several vulnerabilities that were not known to the developers. DOUBLEX is available as an open-source tool.

**1 Introduction**  
Browser extensions are a popular way to customize web browsing. However, they are often vulnerable to attacks. We present DOUBLEX, a static analysis tool that detects vulnerable data flows in browser extensions. DOUBLEX is the first tool to detect vulnerable data flows in browser extensions at scale. It is based on a novel abstraction of browser extensions and a new data flow analysis. DOUBLEX has been evaluated on a large dataset of browser extensions and has detected several vulnerabilities that were not known to the developers. DOUBLEX is available as an open-source tool.

**CCS keywords**  
Static analysis, Browser extensions, Data flow analysis, Vulnerability detection

**Keywords**  
Browser extensions, Data flow analysis, Vulnerability detection



**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  
ACM CCS 2021

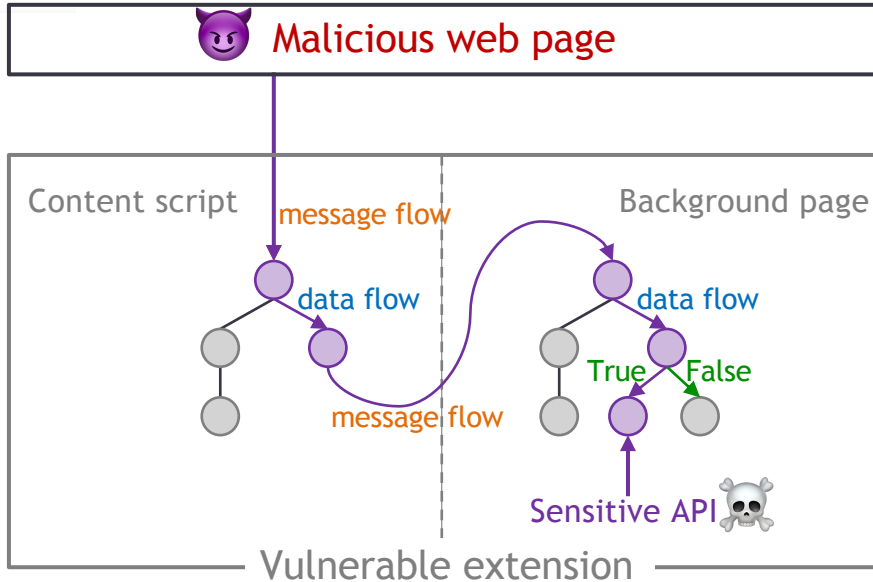
**Abstract**  
Browser extensions are a popular way to customize web browsing. However, they are also a common source of security vulnerabilities. In this paper, we present DOUBLEX, a static analysis tool that detects vulnerable data flows in browser extensions. DOUBLEX is designed to be scalable and accurate, and it is able to detect a wide range of vulnerabilities, including data leaks, data tampering, and data manipulation. We evaluate DOUBLEX on a large dataset of browser extensions and show that it is able to detect a significant number of vulnerabilities that were previously undetected.

**1 Introduction**  
Browser extensions are a popular way to customize web browsing. However, they are also a common source of security vulnerabilities. In this paper, we present DOUBLEX, a static analysis tool that detects vulnerable data flows in browser extensions. DOUBLEX is designed to be scalable and accurate, and it is able to detect a wide range of vulnerabilities, including data leaks, data tampering, and data manipulation. We evaluate DOUBLEX on a large dataset of browser extensions and show that it is able to detect a significant number of vulnerabilities that were previously undetected.

**CCS keywords**  
Security and privacy, Web applications, Browser extensions, Static analysis, Vulnerability detection

## > 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)

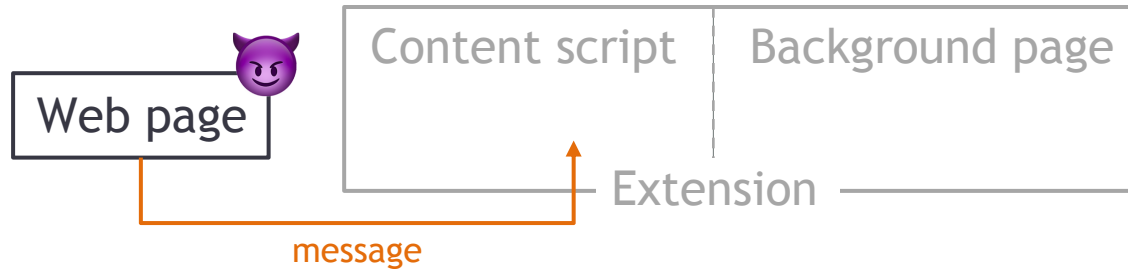
- Message interactions

### 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) {  
  
  
  
  
  
  
  
  
  
})
```

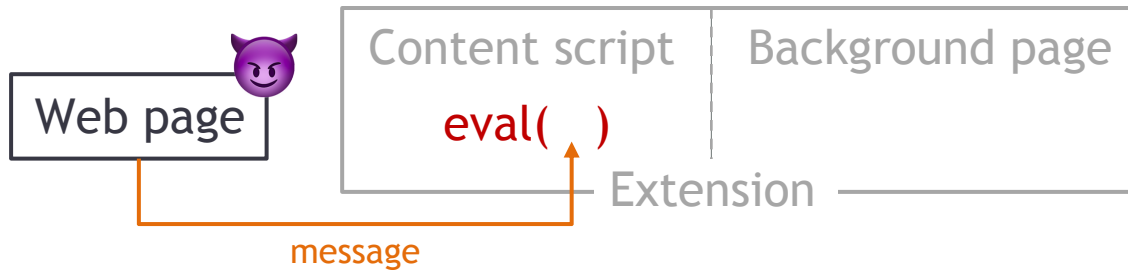


# Simplified Example of a Vulnerability

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

    eval(event.data);

})
```



# Detecting Vulnerable Extensions with DOUBLEX

Analyzed 155k Chrome extensions from 2021 with DOUBLEX

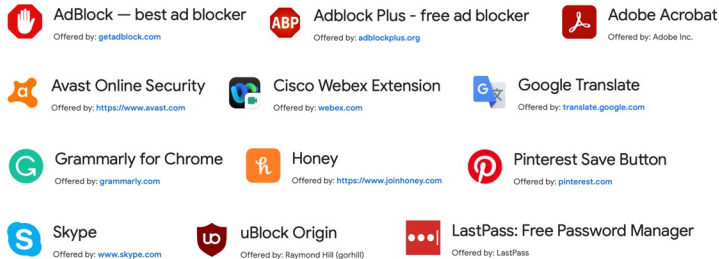
- **184 vulnerable Chrome extensions**
- **Impacting 3M users**
  
- **Precision: 89%** of the flagged extensions are vulnerable
- **Recall: 93%** of known vulnerabilities [2] are detected
  
- **Integration** in the **vetting process** conducted by Google
- **Available online**, for developers  
(even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



 Aurore54F/DoubleX

# Takeaways — Browser Extension (In)Security

## Browser Extensions are Popular



- 125k Chrome extensions totaling over 1.6B active users

## 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

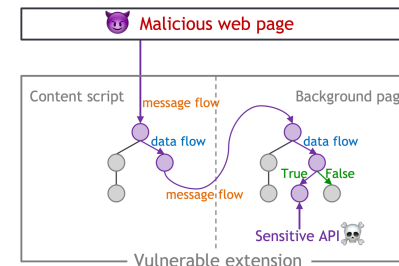
## What is in the Chrome Web Store?

- 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)



Hsu et al.  
AsiaCCS  
2024

## 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%

- [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*