Detecting Dangerous Browser Extensions

Dr.-Ing. Aurore Fass

Tenured Researcher — Inria Centre at Université Côte d'Azur (since Dec 1, 2025)

Dagstuhl Seminar 26291 — Web Application Security, July 14th 2026

What are Browser Extensions?

- Third-party programs to **improve user browsing experience**…
- … so browser extensions need additional & elevated privileges compared to web pages

Adblock Plus - free ad blocker
Offered by: adblockplus.org

Grammarly for Chrome
Offered by: grammarly.com

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

  - e.g., ad-blockers need to modify web page content or intercept network requests

➢ Browser extensions are an attractive target for attackers 😈

- **~270k** Chrome extensions totaling **~3B** active users

Dangerous Browser Extensions

→ 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 [1, 3]
- **Contain vulnerabilities**: designed by well-intentioned developers… but buggy
  - E.g., can lead to user-sensitive data exfiltration [1, 2]
- **Violate the Chrome Web Store policies**
  - E.g., deceive users, promote unlawful activities, lack a privacy policy [1]

[1] Hsu, Tran, and Fass; *AsiaCCS* 2024 | [2] Fass, Somé, Backes, and Stock; *CCS* 2021 | [3] Rosenzweig, Dalla Valle, Apruzzese, and Fass; *TWEB* 2026

Main Findings on the Chrome Web Store

> What is in the Chrome Web Store?

In *ACM AsiaCCS* 2024. Sheryl Hsu, Manda Tran, and <u>Aurore Fass</u>

Hsu et al.
AsiaCCS
2024

[1] Hsu, Tran, and <u>Fass</u>; *AsiaCCS* 2024

Main Findings on the Chrome Web Store

- The Chrome Web Store hosted **>26k dangerous extensions** in 2020—23
- **350M users** installed **dangerous extensions** in 2020—2023
- These **dangerous extensions** stay in the Chrome Web Store ***for years***


What is in the Chrome Web Store?

Hsu et al. AsiaCCS 2024

> What is in the Chrome Web Store?

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

[1] Hsu, Tran, and Fass; *AsiaCCS* 2024

Main Findings on the C

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

[1] Hsu, Tran, and Fass; *AsiaCCS* 2024

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

Dangerous Browser Extensions

→ 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 [1, 3]
- **Contain vulnerabilities**: designed by well-intentioned developers… but buggy
  - E.g., can lead to user-sensitive data exfiltration [1, 2]
- **Violate the Chrome Web Store policies**
  - E.g., deceive users, promote unlawful activities, lack a privacy policy [1]
- **Be fingerprintable**: can be recognized and uniquely identified
  - E.g., can lead to user tracking or inferring of user personal information [4]

[1] Hsu, Tran, and Fass; *AsiaCCS* 2024 | [2] Fass, Somé, Backes, and Stock; *CCS* 2021 | [3] Rosenzweig, Dalla Valle, Apruzzese, and Fass; *TWEB* 2026 | [4] Agarwal, Fass, and Stock; *CCS* 2024

Detecting vulnerable extensions

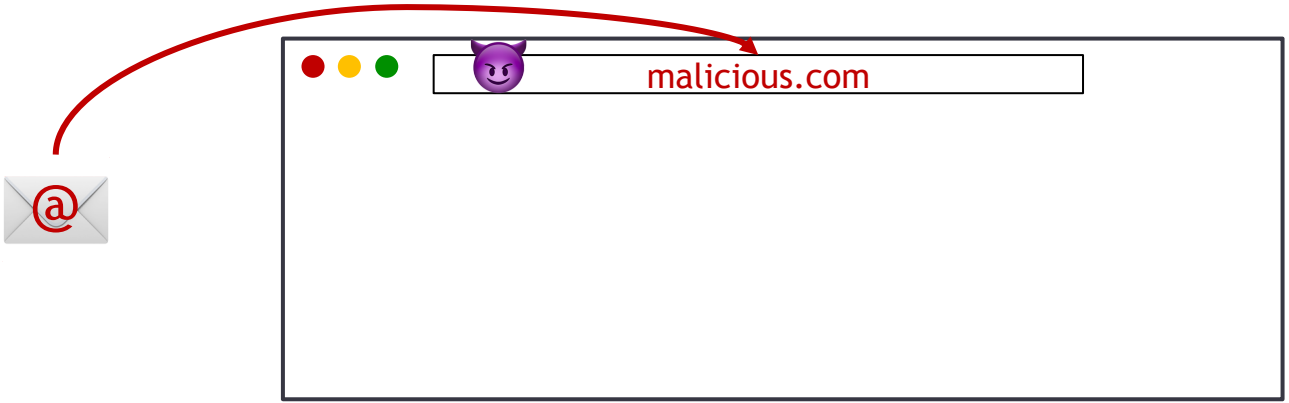
Analysis of Vulnerable Extensions: Threat Model

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

[2] Fass et al.; *CCS* 2021

Analysis of Vulnerable Extensions: Threat Model

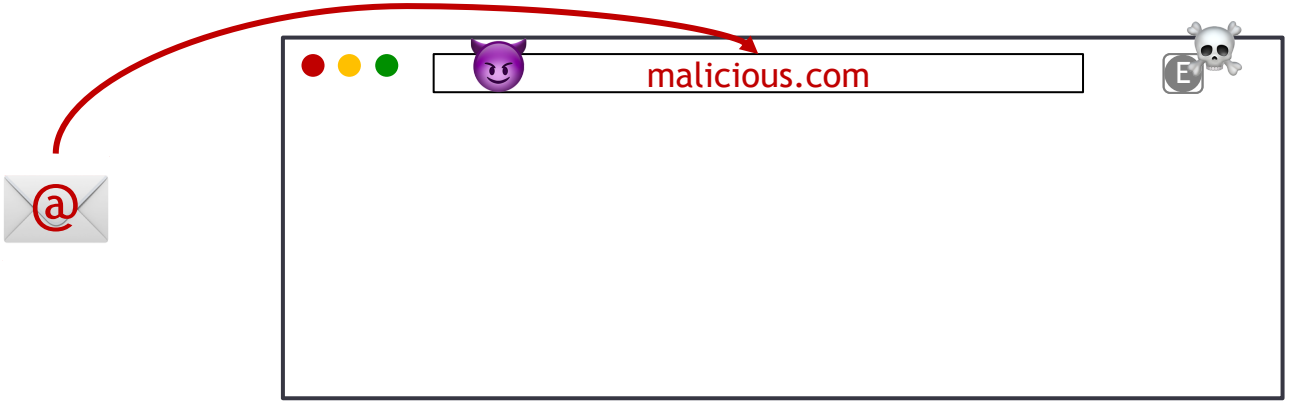
Challenging to detect due to their inherently benign intent (*benign-but-buggy*)



[2] Fass et al.; *CCS* 2021

Analysis of Vulnerable Extensions: Threat Model

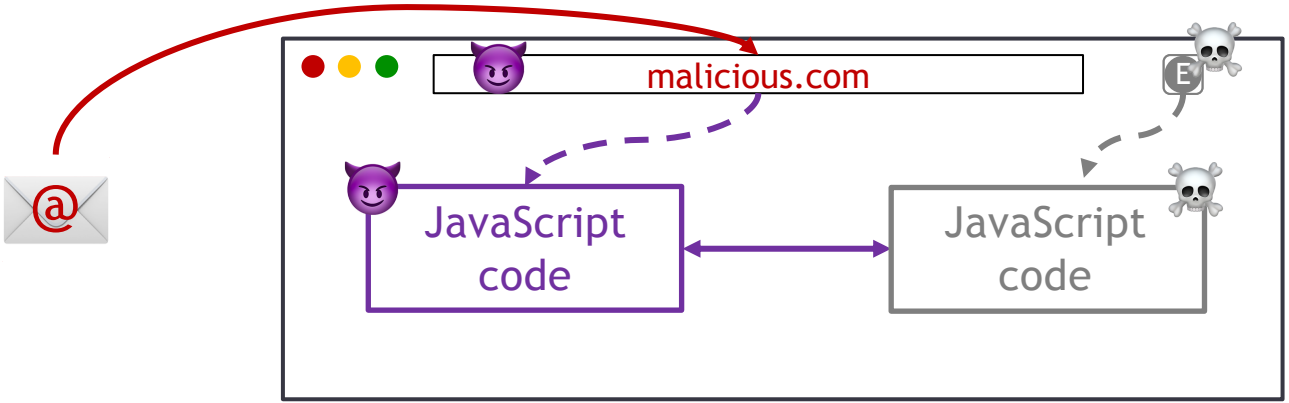
Challenging to detect due to their inherently benign intent (*benign-but-buggy*)



[2] Fass et al.; *CCS* 2021

Analysis of Vulnerable Extensions: Threat Model

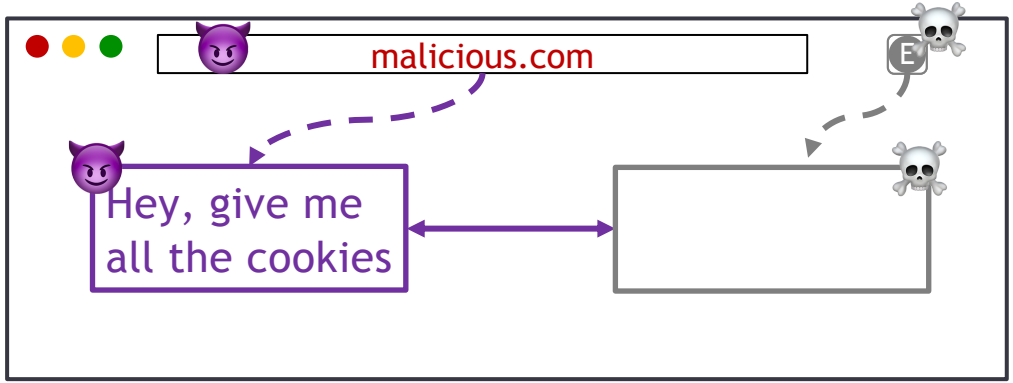
Challenging to detect due to their inherently benign intent (*benign-but-buggy*)



[2] Fass et al.; *CCS* 2021

Analysis of Vulnerable Extensions: Threat Model

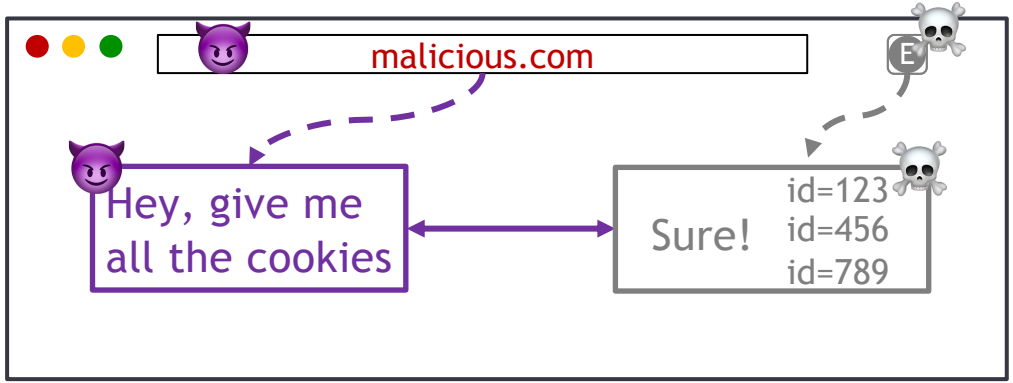
Challenging to detect due to their inherently benign intent (*benign-but-buggy*)



[2] Fass et al.; *CCS* 2021

Analysis of Vulnerable Extensions: Threat Model

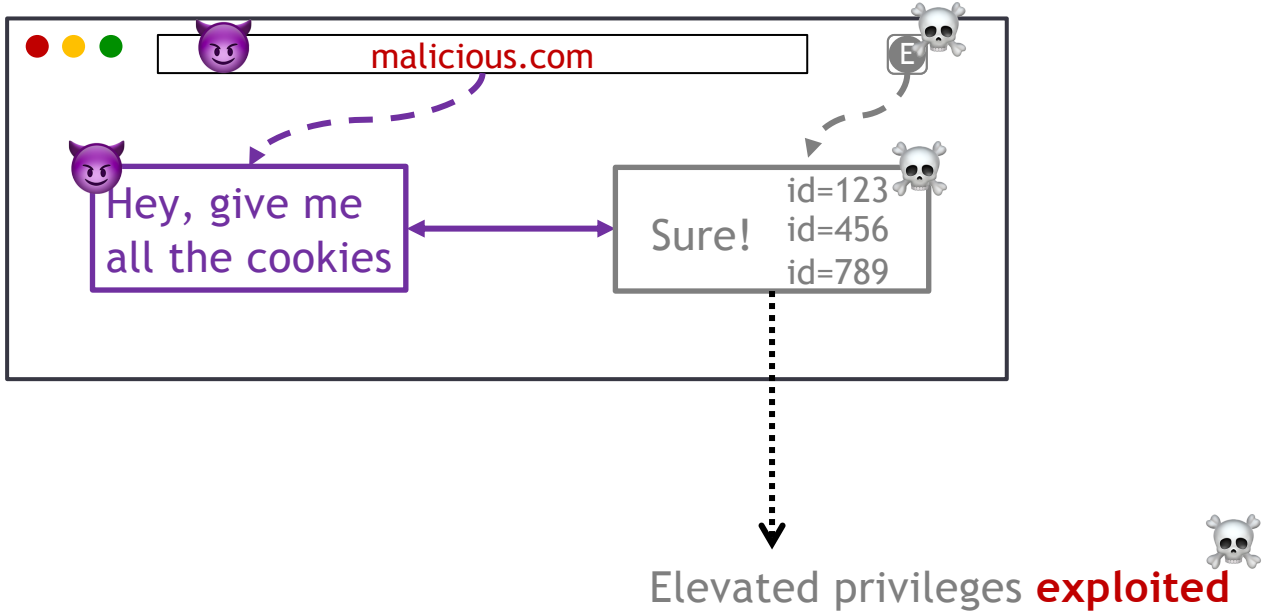
Challenging to detect due to their inherently benign intent (*benign-but-buggy*)



[2] Fass et al.; *CCS* 2021

Analysis of Vulnerable Extensions: Threat Model

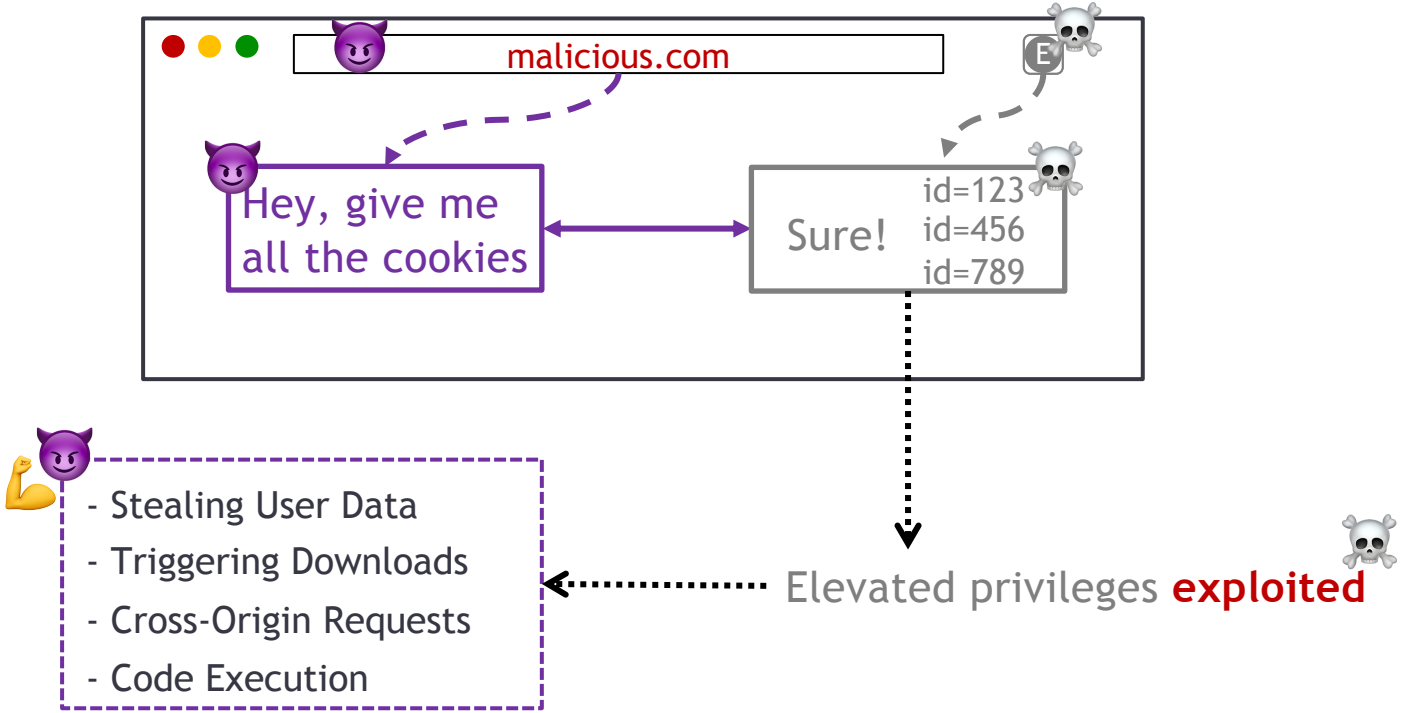
Challenging to detect due to their inherently benign intent (*benign-but-buggy*)



[2] Fass et al.; *CCS* 2021

Analysis of Vulnerable Extensions: Threat Model

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



[2] Fass et al.; *CCS* 2021

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

Abstract

Introduction

CCS Concepts

Keywords

ACM Reference Format

> DOUBLEX: Statically Detecting Vulnerable Data Flows in Browser Extensions

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

[2] Fass et al.; *CCS* 2021

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

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

Malicious web page

Content script

Background page
Service worker

Vulnerable extension

[2] Fass et al.; *CCS* 2021

Detecting Vulnerable Extensions


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

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

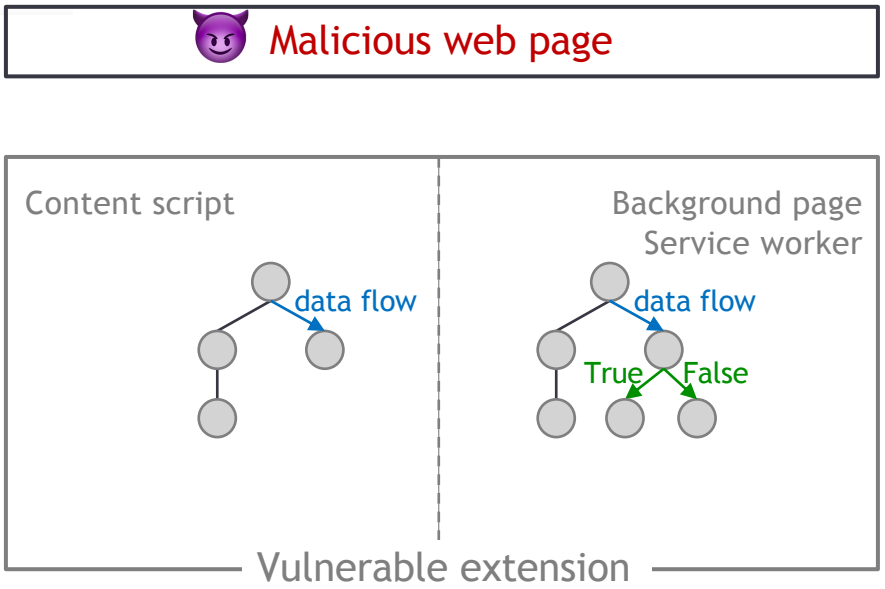
CISPA Helmholtz Center for Information Security

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 JavaScript code abstraction

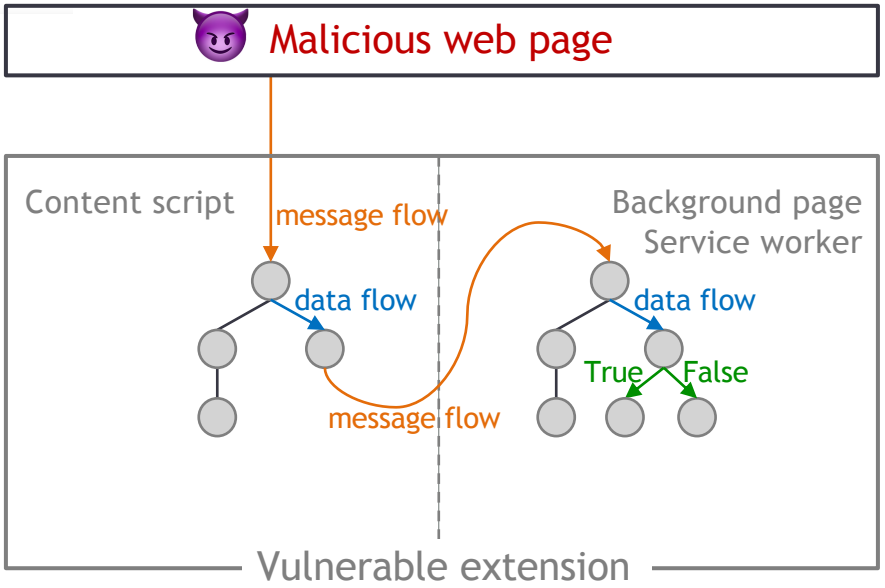
- AST (Abstract Syntax Tree)
- Control flow
- Data flow
- Pointer analysis

[2] Fass et al.; *CCS* 2021

Detecting Vulnerable Extensions

> 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 JavaScript code abstraction

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

Extension Dependence Graph (EDG)

➢ Message interactions

[2] Fass et al.; *CCS* 2021

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

Abstract

1 Introduction

2 Background

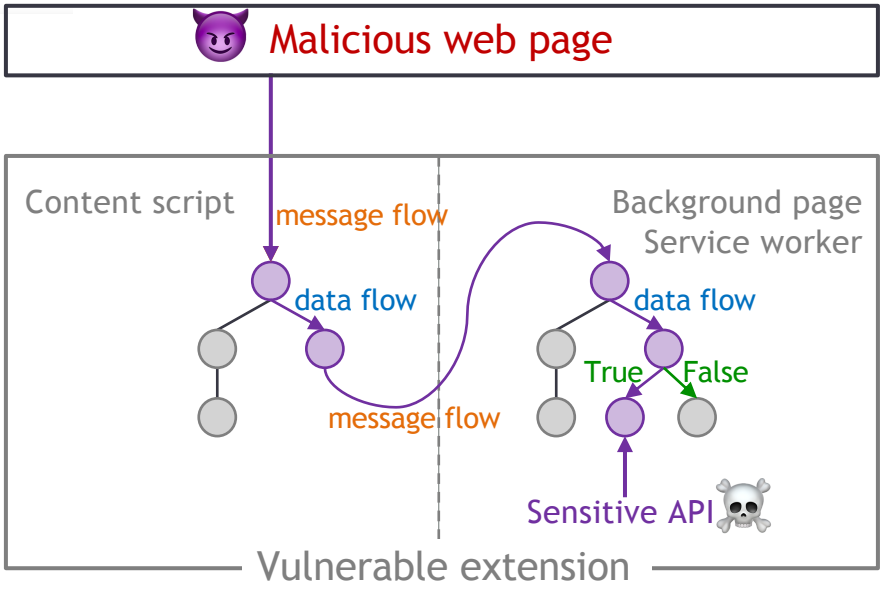
CCS Concepts

Keywords

ACM Reference Format

> 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 JavaScript 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

[2] Fass et al.; *CCS* 2021

Simplified Example of a Vulnerability

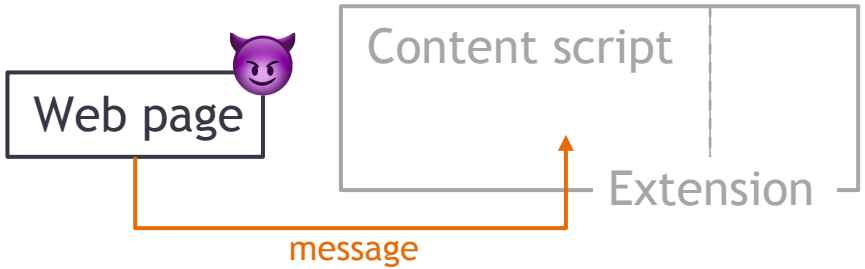
```
1  // Content script code = from the extension
2  window.addEventListener("message", function(event) {
3
4
5
6  })
```

[2] Fass et al.; *CCS* 2021

Simplified Example of a Vulnerability

message received

```
1  // Content script code = from the extension
2  window.addEventListener("message", function(event) {
3
4
5
6  })
```

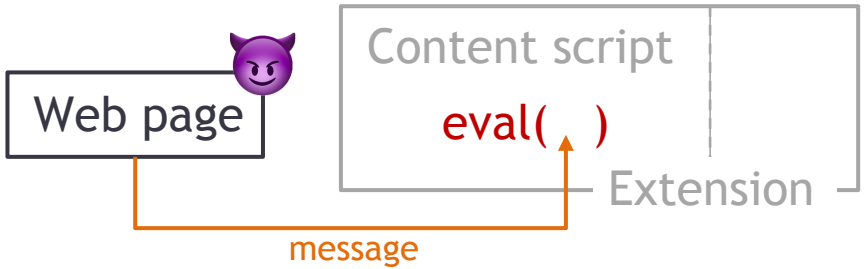


[2] Fass et al.; *CCS* 2021

Simplified Example of a Vulnerability

message received

```
1  // Content script code = from the extension
2  window.addEventListener("message", function(event) {
3
4      eval(event.data);
5
6  })
```



[2] Fass et al.; *CCS* 2021

Simplified Example of a Vulnerability

message received

```
1  // Content script code = from the extension
2  window.addEventListener("message", function(event) {
3
4      eval(event.data);
5
6  })
```


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

[2] Fass et al.; *CCS* 2021

Detecting Vulnerable Extensions with DOUBLEX

Analyzed 155k Chrome extensions from 2021 with DOUBLEX (takes 2—3s per extension)

- **184 vulnerable Chrome extensions**
- Impacting **3M users*** (* based on Google's definition)

- **Precision: 89%** of the flagged extensions are vulnerable
- **Recall: 93%** of known vulnerabilities [Somé, S&P 2019] are detected

- **Open source**, for developers and Web users

  (even in other fields, e.g., mini apps [Wang et al., ICSE 2023])

Aurore54F/DoubleX

[2] Fass et al.; *CCS* 2021

Detecting fingerprintable extensions

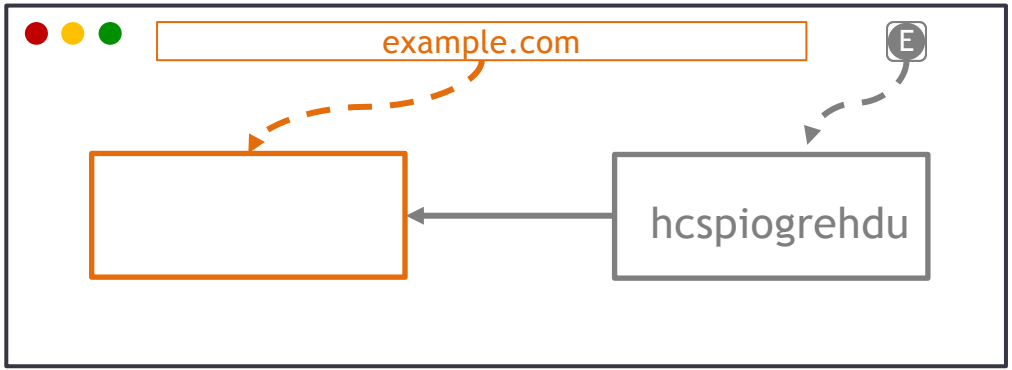
Browser Extension Fingerprinting

Browser extensions can **interact with web pages…**

Browser Extension Fingerprinting

Browser extensions can **interact with web pages…**

- 1) Extensions send **PostMessage** to web pages



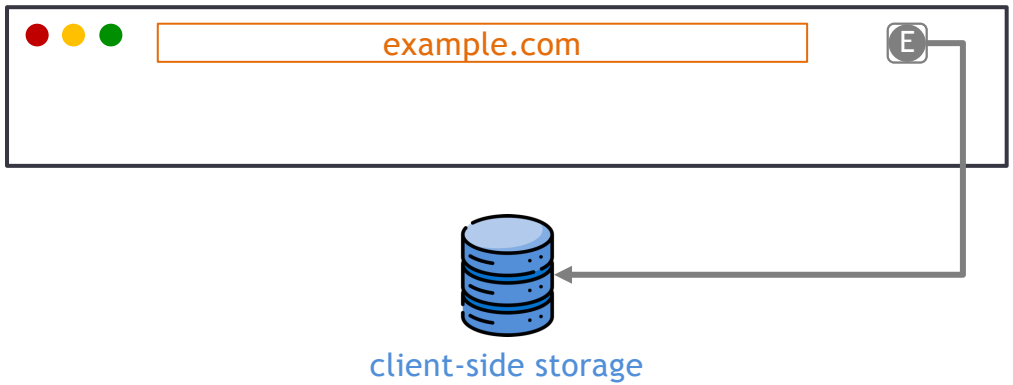
[4] Agarwal, Fass, and Stock; *CCS* 2024

Browser Extension Fingerprinting

Browser extensions can **interact with web pages…**

- 1) Extensions send **PostMessage** to web pages
- 2) Extensions store data on the client side through **storage APIs**

  (e.g., cookies, local/session storage, IndexedDB)

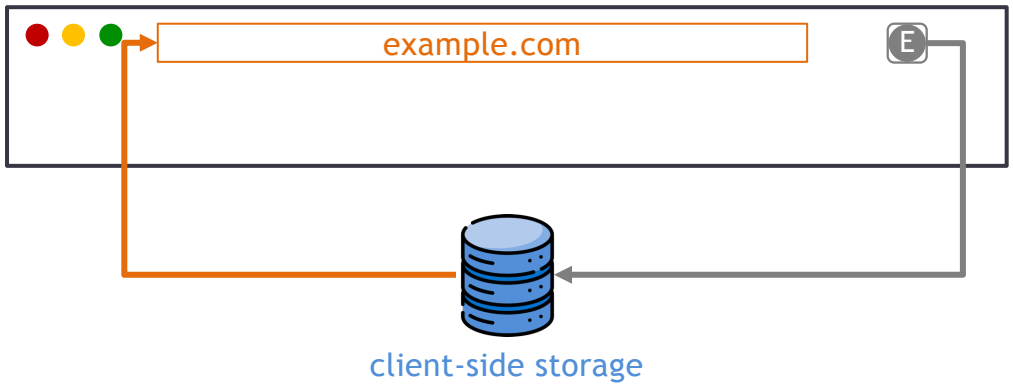


Browser Extension Fingerprinting

Browser extensions can **interact with web pages…**

- 1) Extensions send **PostMessage** to web pages
- 2) Extensions store data on the client side through **storage APIs**

  (e.g., cookies, local/session storage, IndexedDB)

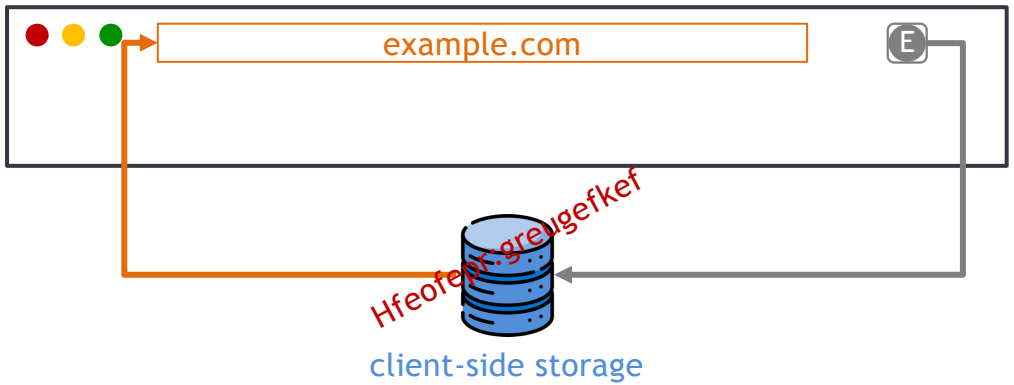


Browser Extension Fingerprinting

Browser extensions can **interact with web pages…**

- 1) Extensions send **PostMessage** to web pages
- 2) Extensions store data on the client side through **storage APIs**

  (e.g., cookies, local/session storage, IndexedDB)



Browser Extension Fingerprinting

Browser extensions can **interact with web pages…**

- 1) Extensions send **PostMessage** to web pages
- 2) Extensions store data on the client side through **storage APIs**

  (e.g., cookies, local/session storage, IndexedDB)
- 3) Extensions **inject JavaScript** code directly into web pages

  → registering global variables

  → invocation of global APIs and properties

[4] Agarwal, Fass, and Stock; *CCS* 2024

Browser Extension Fingerprinting

Browser extensions can **interact with web pages…**

- 1) Extensions send **PostMessage** to web pages
- 2) Extensions store data on the client side through **storage APIs**

  (e.g., cookies, local/session storage, IndexedDB)
- 3) Extensions **inject JavaScript** code directly into web pages

  → registering global variables

  → invocation of global APIs and properties

… which leaves traces → **observable side effects**, can be seen by a “malicious” site

[4] Agarwal, Fass, and Stock; *CCS* 2024

Detecting Fingerprintable Extensions

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

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

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

Detecting Fingerprintable Extensions


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

Shubham Agarwal
CISPA Helmholtz Center for Information Security
shubham.agarwal@cispa.de

Aurore Fass
CISPA Helmholtz Center for Information Security
fass@cispa.de

Ben Stock
CISPA Helmholtz Center for Information Security
stock@cispa.de

ABSTRACT

KEYWORDS

CCS CONCEPTS

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

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

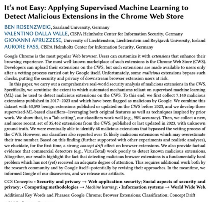
Analyzed 38k Chrome extensions from 2024 with Raider

- **>2,747 fingerprintable Chrome extensions** | impacting >**169M users**
- **Notified 1,967 developers** about their fingerprintable extension(s)
  - Only 30 (!) replied
  - Of those, only 16 positively acknowledged the issues
- Raider PoC is **available online** https://github.com/raider-ext/raider

Detecting malicious extensions

Detecting Malicious Extensions — Lab Setting

Rosenzweig et al. TWEB 2026


It’s not Easy: Applying Supervised Machine Learning to Detect Malicious Extensions in the Chrome Web Store

BEN ROSENZWEIG, Saarland University, Germany
VALENTINO DALLA VALLE, CISPA Helmholtz Center for Information Security, Germany
GIOVANNI APRUZZESE, University of Liechtenstein, Liechtenstein and Reykjavik University, Iceland
AURORE FASS, CISPA Helmholtz Center for Information Security, Germany

Google Chrome is the most popular Web browser. Users can customize it with *extensions* that enhance their browsing experience. The most well-known marketplace of such extensions is the Chrome Web Store (CWS). Developers can upload their extensions on the CWS, but such extensions are made available to users only after a vetting process carried out by Google itself. Unfortunately, some *malicious* extensions bypass such checks, putting the security and privacy of downstream browser extension users at risk.

In this paper, we carry out a comprehensive real-world security analysis of malicious extensions in the CWS. Specifically, we scrutinize the extent to which automated mechanisms reliant on supervised machine learning (ML) can be used to detect malicious extensions on the CWS. To this end, we first collect 7,140 malicious extensions published in 2017–2023 and which have been flagged as malicious by Google. We combine this dataset with 63,598 benign extensions published or updated on the CWS before 2023, and we develop three supervised-ML-based classifiers—leveraging both original features as well as techniques inspired by prior work. We show that, in a "lab setting", our classifiers work well (e.g., 98% accuracy). Then, we collect a new, and more recent, set of 35,462 extensions from the CWS, published or last updated in 2023, with unknown ground truth. We were eventually able to identify 68 malicious extensions that bypassed the vetting process of the CWS. However, our classifiers also reported over 1k likely malicious extensions which may overestimate their true number. Based on this finding (further supported with other experiments and realistic analyses), we elucidate, for the first time, a strong *concept drift* effect on browser extensions. We also provide factual evidence that commercial detectors (e.g., VirusTotal) work poorly to detect known malicious extensions. Altogether, our results highlight the fact that detecting malicious browser extensions is a fundamentally hard problem which has not (yet) received an adequate degree of attention. This requires additional work both by the research community and by Google itself—potentially by revising their approaches. In the meantime, we informed Google of our discoveries, and we release our artifacts.

CCS Concepts: • **Security and privacy → Web application security**; **Social aspects of security and privacy**; • **Computing methodologies →** *Machine learning*; • **Information systems → World Wide Web**.

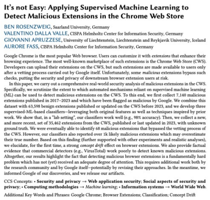
Additional Key Words and Phrases: Google Chrome; Browser Extensions; Classification; Concept Drift

> It’s not Easy: Applying Supervised ML to Detect Malicious Extensions in the CWS

In *ACM TWEB* 2026. Ben Rosenzweig, Valentino Dalla Valle, Giovanni Apruzzese, and Aurore Fass

Detecting Malicious Extensions — Lab Setting

Rosenzweig et al. TWEB 2026


It's not Easy: Applying Supervised Machine Learning to Detect Malicious Extensions in the Chrome Web Store

BEN ROSENZWEIG, Saarland University, Germany
VALENTINO DALLA VALLE, CISPA Helmholtz Center for Information Security, Germany
GIOVANNI APRUZZESE, University of Liechtenstein, Liechtenstein and Reykjavik University, Iceland
AURORE FASS, CISPA Helmholtz Center for Information Security, Germany

Google Chrome is the most popular Web browser. Users can customize it with *extensions* that enhance their browsing experience. The most well-known marketplace of such extensions is the Chrome Web Store (CWS). Developers can upload their extensions on the CWS, but such extensions are made available to users only after a vetting process carried out by Google itself. Unfortunately, some *malicious* extensions bypass such checks, putting the security and privacy of downstream browser extension users at risk.

In this paper, we carry out a comprehensive real-world security analysis of malicious extensions in the CWS. Specifically, we scrutinize the extent to which automated mechanisms reliant on supervised machine learning (ML) can be used to detect malicious extensions on the CWS. To this end, we first collect 7,140 malicious extensions published in 2017–2023 and which have been flagged as malicious by Google. We combine this dataset with 63,598 benign extensions published or updated on the CWS before 2023, and we develop three supervised-ML-based classifiers—leveraging both original features as well as techniques inspired by prior work. We show that, in a "lab setting", our classifiers work well (e.g., 98% accuracy). Then, we collect a new, and more recent, set of 35,462 extensions from the CWS, published or last updated in 2023, with unknown ground truth. We were eventually able to identify 68 malicious extensions that bypassed the vetting process of the CWS. However, our classifiers also reported over 1k likely malicious extensions which may overestimate their true number. Based on this finding (further supported with other experiments and realistic analyses), we elucidate, for the first time, a strong *concept drift* effect on browser extensions. We also provide factual evidence that commercial detectors (e.g., VirusTotal) work poorly to detect known malicious extensions. Altogether, our results highlight the fact that detecting malicious browser extensions is a fundamentally hard problem which has not (yet) received an adequate degree of attention. This requires additional work both by the research community and by Google itself—potentially by revising their approaches. In the meantime, we informed Google of our discoveries, and we release our artifacts.

CCS Concepts: • **Security and privacy → Web application security**; **Social aspects of security and privacy**; • **Computing methodologies →** *Machine learning*; • **Information systems → World Wide Web**.

Additional Key Words and Phrases: Google Chrome; Browser Extensions; Classification; Concept Drift

> It's not Easy: Applying Supervised ML to Detect Malicious Extensions in the CWS

In *ACM TWEB* 2026. Ben Rosenzweig, Valentino Dalla Valle, Giovanni Apruzzese, and Aurore Fass

DATASET

7,140 malicious extensions

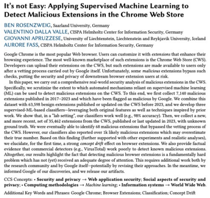
Last update 2017—23

63,598 "benign" extensions

Last update 2012—22

Detecting Malicious Extensions — Lab Setting

Rosenzweig et al. TWEB 2026


It's not Easy: Applying Supervised Machine Learning to Detect Malicious Extensions in the Chrome Web Store

BEN ROSENZWEIG, Saarland University, Germany
VALENTINO DALLA VALLE, CISPA Helmholtz Center for Information Security, Germany
GIOVANNI APRUZZESE, University of Liechtenstein, Liechtenstein and Reykjavik University, Iceland
AURORE FASS, CISPA Helmholtz Center for Information Security, Germany

Google Chrome is the most popular Web browser. Users can customize it with *extensions* that enhance their browsing experience. The most well-known marketplace of such extensions is the Chrome Web Store (CWS). Developers can upload their extensions on the CWS, but such extensions are made available to users only after a vetting process carried out by Google itself. Unfortunately, some *malicious* extensions bypass such checks, putting the security and privacy of downstream browser extension users at risk.

In this paper, we carry out a comprehensive real-world security analysis of malicious extensions in the CWS. Specifically, we scrutinize the extent to which automated mechanisms reliant on supervised machine learning (ML) can be used to detect malicious extensions on the CWS. To this end, we first collect 7,140 malicious extensions published in 2017–2023 and which have been flagged as malicious by Google. We combine this dataset with 63,598 benign extensions published or updated on the CWS before 2023, and we develop three supervised-ML-based classifiers—leveraging both original features as well as techniques inspired by prior work. We show that, in a "lab setting", our classifiers work well (e.g., 98% accuracy). Then, we collect a new, and more recent, set of 35,462 extensions from the CWS, published or last updated in 2023, with unknown ground truth. We were eventually able to identify 68 malicious extensions that bypassed the vetting process of the CWS. However, our classifiers also reported over 1k likely malicious extensions which may overestimate their true number. Based on this finding (further supported with other experiments and realistic analyses), we elucidate, for the first time, a strong *concept drift* effect on browser extensions. We also provide factual evidence that commercial detectors (e.g., VirusTotal) work poorly to detect known malicious extensions. Altogether, our results highlight the fact that detecting malicious browser extensions is a fundamentally hard problem which has not (yet) received an adequate degree of attention. This requires additional work both by the research community and by Google itself—potentially by revising their approaches. In the meantime, we informed Google of our discoveries, and we release our artifacts.

CCS Concepts: • **Security and privacy → Web application security**; **Social aspects of security and privacy**; • **Computing methodologies →** *Machine learning*; • **Information systems → World Wide Web**.

Additional Key Words and Phrases: Google Chrome; Browser Extensions; Classification; Concept Drift

> It's not Easy: Applying Supervised ML to Detect Malicious Extensions in the CWS

In *ACM TWEB* 2026. Ben Rosenzweig, Valentino Dalla Valle, Giovanni Apruzzese, and Aurore Fass

DATASET

7,140 malicious extensions

Last update 2017—23

63,598 "benign" extensions

Last update 2012—22

FEATURES

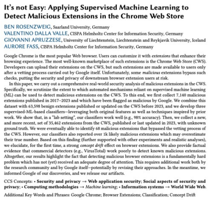
Source code [A]

Metadata

[A] Fass et al.; *ACSAC* 2018

Detecting Malicious Extensions — Lab Setting

Rosenzweig et al. TWEB 2026


It's not Easy: Applying Supervised Machine Learning to Detect Malicious Extensions in the Chrome Web Store

BEN ROSENZWEIG, Saarland University, Germany
VALENTINO DALLA VALLE, CISPA Helmholtz Center for Information Security, Germany
GIOVANNI APRUZZESE, University of Liechtenstein, Liechtenstein and Reykjavik University, Iceland
AURORE FASS, CISPA Helmholtz Center for Information Security, Germany

Google Chrome is the most popular Web browser. Users can customize it with *extensions* that enhance their browsing experience. The most well-known marketplace of such extensions is the Chrome Web Store (CWS). Developers can upload their extensions on the CWS, but such extensions are made available to users only after a vetting process carried out by Google itself. Unfortunately, some *malicious* extensions bypass such checks, putting the security and privacy of downstream browser extension users at risk.

In this paper, we carry out a comprehensive real-world security analysis of malicious extensions in the CWS. Specifically, we scrutinize the extent to which automated mechanisms reliant on supervised machine learning (ML) can be used to detect malicious extensions on the CWS. To this end, we first collect 7,140 malicious extensions published in 2017–2023 and which have been flagged as malicious by Google. We combine this dataset with 63,598 benign extensions published or updated on the CWS before 2023, and we develop three supervised-ML-based classifiers—leveraging both original features as well as techniques inspired by prior work. We show that, in a "lab setting", our classifiers work well (e.g., 98% accuracy). Then, we collect a new, and more recent, set of 35,462 extensions from the CWS, published or last updated in 2023, with unknown ground truth. We were eventually able to identify 68 malicious extensions that bypassed the vetting process of the CWS. However, our classifiers also reported over 1k likely malicious extensions which may overestimate their true number. Based on this finding (further supported with other experiments and realistic analyses), we elucidate, for the first time, a strong *concept drift* effect on browser extensions. We also provide factual evidence that commercial detectors (e.g., VirusTotal) work poorly to detect known malicious extensions. Altogether, our results highlight the fact that detecting malicious browser extensions is a fundamentally hard problem which has not (yet) received an adequate degree of attention. This requires additional work both by the research community and by Google itself—potentially by revising their approaches. In the meantime, we informed Google of our discoveries, and we release our artifacts.

CCS Concepts: • **Security and privacy → Web application security**; **Social aspects of security and privacy**; • **Computing methodologies →** *Machine learning*; • **Information systems → World Wide Web**.

Additional Key Words and Phrases: Google Chrome; Browser Extensions; Classification; Concept Drift

> It's not Easy: Applying Supervised ML to Detect Malicious Extensions in the CWS

In *ACM TWEB* 2026. Ben Rosenzweig, Valentino Dalla Valle, Giovanni Apruzzese, and Aurore Fass

DATASET

7,140 malicious extensions

Last update 2017—23

63,598 "benign" extensions

Last update 2012—22

FEATURES

Source code [A]

Metadata

[A] Fass et al.; *ACSAC* 2018

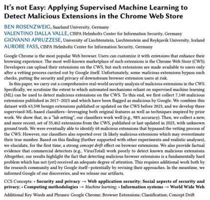
ML DETECTORS

80% train | 20% test

→ *Predictions*

Detecting Malicious Extensions — Lab Setting

Rosenzweig et al. TWEB 2026



It's not Easy: Applying Supervised Machine Learning to Detect Malicious Extensions in the Chrome Web Store

BEN ROSENZWEIG, Saarland University, Germany
VALENTINO DALLA VALLE, CISPA Helmholtz Center for Information Security, Germany
GIOVANNI APRUZZESE, University of Liechtenstein, Liechtenstein and Reykjavik University, Iceland
AURORE FASS, CISPA Helmholtz Center for Information Security, Germany

Google Chrome is the most popular Web browser. Users can customize it with *extensions* that enhance their browsing experience. The most well-known marketplace of such extensions is the Chrome Web Store (CWS). Developers can upload their extensions on the CWS, but such extensions are made available to users only after a vetting process carried out by Google itself. Unfortunately, some *malicious* extensions bypass such checks, putting the security and privacy of downstream browser extension users at risk.

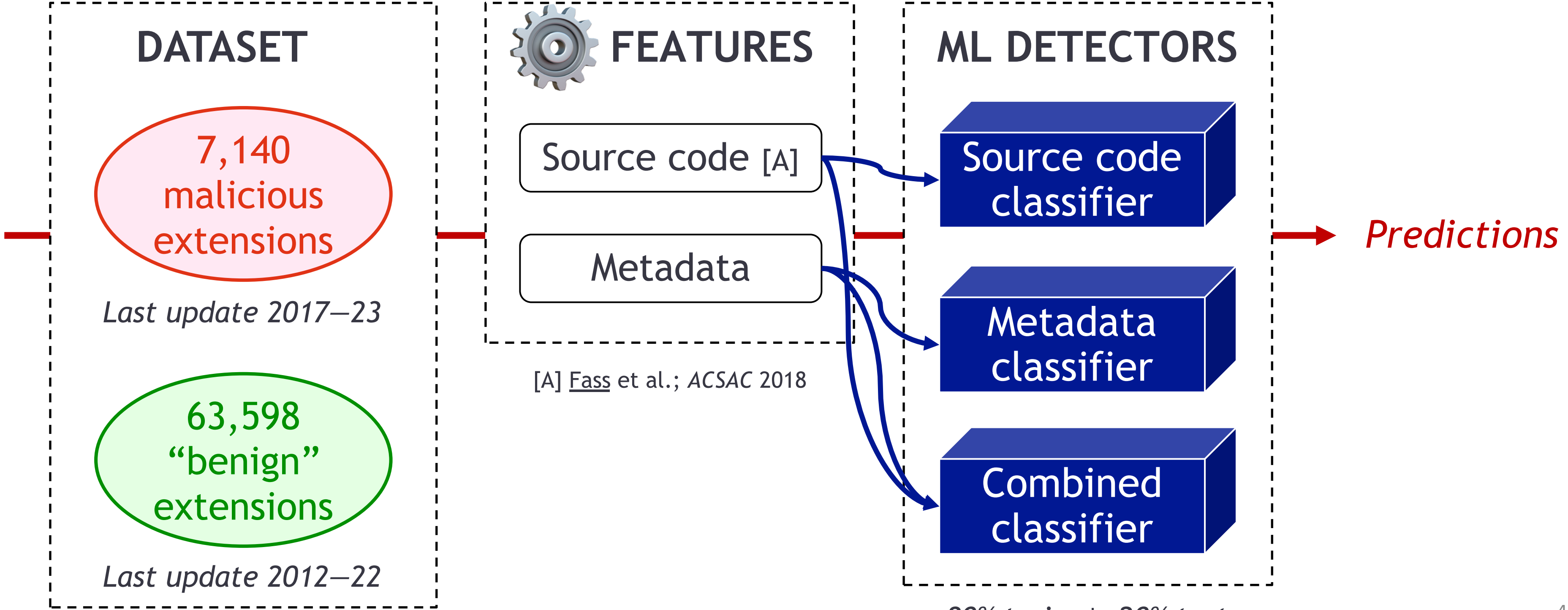
In this paper, we carry out a comprehensive real-world security analysis of malicious extensions in the CWS. Specifically, we scrutinize the extent to which automated mechanisms reliant on supervised machine learning (ML) can be used to detect malicious extensions on the CWS. To this end, we first collect 7,140 malicious extensions published in 2017–2023 and which have been flagged as malicious by Google. We combine this dataset with 63,598 benign extensions published or updated on the CWS before 2023, and we develop three supervised-ML-based classifiers—leveraging both original features as well as techniques inspired by prior work. We show that, in a "lab setting", our classifiers work well (e.g., 98% accuracy). Then, we collect a new, and more recent, set of 35,462 extensions from the CWS, published or last updated in 2023, with unknown ground truth. We were eventually able to identify 68 malicious extensions that bypassed the vetting process of the CWS. However, our classifiers also reported over 1k likely malicious extensions which may overestimate their true number. Based on this finding (further supported with other experiments and realistic analyses), we elucidate, for the first time, a strong *concept drift* effect on browser extensions. We also provide factual evidence that commercial detectors (e.g., VirusTotal) work poorly to detect known malicious extensions. Altogether, our results highlight the fact that detecting malicious browser extensions is a fundamentally hard problem which has not (yet) received an adequate degree of attention. This requires additional work both by the research community and by Google itself—potentially by revising their approaches. In the meantime, we informed Google of our discoveries, and we release our artifacts.

CCS Concepts: • **Security and privacy → Web application security**; **Social aspects of security and privacy**; • **Computing methodologies →** *Machine learning*; • **Information systems → World Wide Web**.

Additional Key Words and Phrases: Google Chrome; Browser Extensions; Classification; Concept Drift

> It's not Easy: Applying Supervised ML to Detect Malicious Extensions in the CWS

In *ACM TWEB* 2026. Ben Rosenzweig, Valentino Dalla Valle, Giovanni Apruzzese, and Aurore Fass

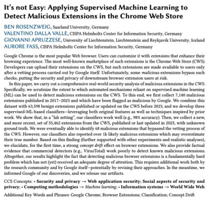


[A] Fass et al.; *ACSAC* 2018

80% train | 20% test

Detecting Malicious Extensions — Lab Setting

Rosenzweig et al. TWEB 2026



It's not Easy: Applying Supervised Machine Learning to Detect Malicious Extensions in the Chrome Web Store

BEN ROSENZWEIG, Saarland University, Germany
VALENTINO DALLA VALLE, CISPA Helmholtz Center for Information Security, Germany
GIOVANNI APRUZZESE, University of Liechtenstein, Liechtenstein and Reykjavik University, Iceland
AURORE FASS, CISPA Helmholtz Center for Information Security, Germany

Google Chrome is the most popular Web browser. Users can customize it with *extensions* that enhance their browsing experience. The most well-known marketplace of such extensions is the Chrome Web Store (CWS). Developers can upload their extensions on the CWS, but such extensions are made available to users only after a vetting process carried out by Google itself. Unfortunately, some *malicious* extensions bypass such checks, putting the security and privacy of downstream browser extension users at risk.

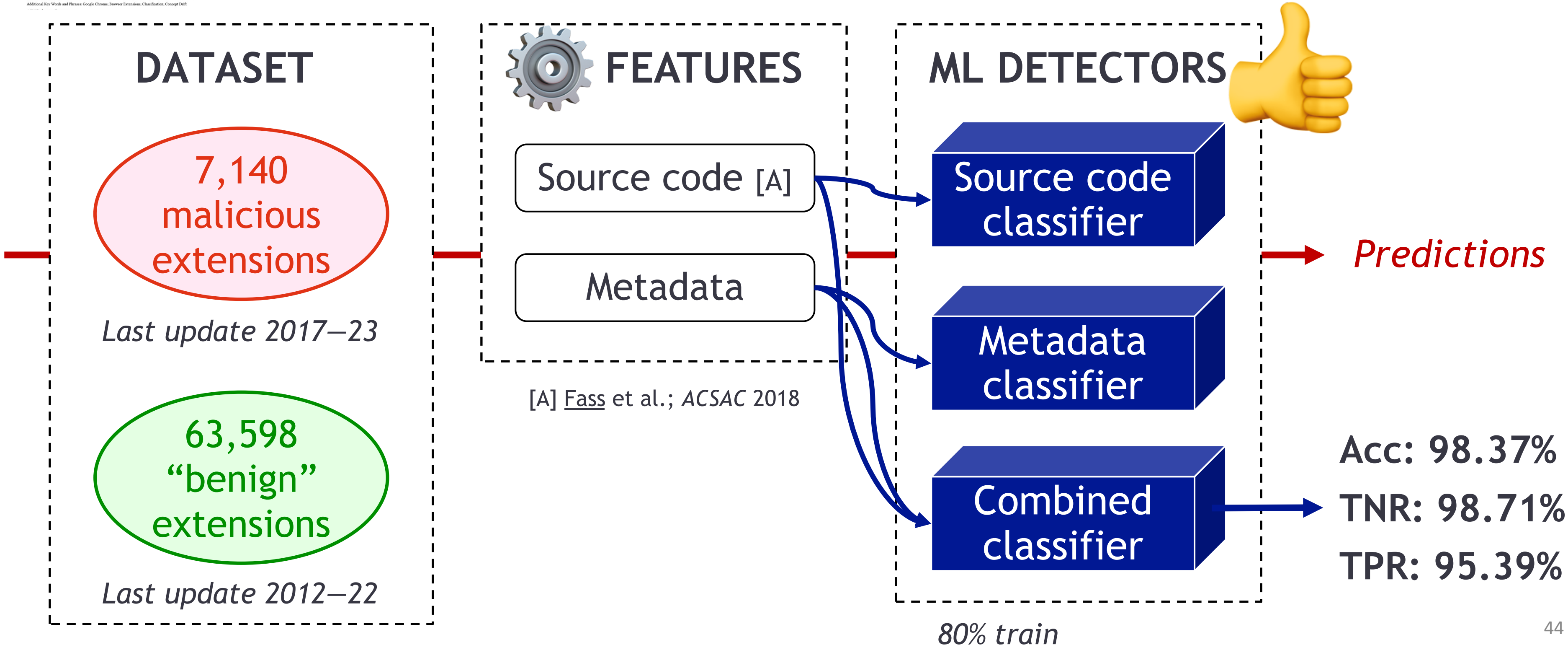
In this paper, we carry out a comprehensive real-world security analysis of malicious extensions in the CWS. Specifically, we scrutinize the extent to which automated mechanisms reliant on supervised machine learning (ML) can be used to detect malicious extensions on the CWS. To this end, we first collect 7,140 malicious extensions published in 2017–2023 and which have been flagged as malicious by Google. We combine this dataset with 63,598 benign extensions published or updated on the CWS before 2023, and we develop three supervised-ML-based classifiers—leveraging both original features as well as techniques inspired by prior work. We show that, in a "lab setting", our classifiers work well (e.g., 98% accuracy). Then, we collect a new, and more recent, set of 35,462 extensions from the CWS, published or last updated in 2023, with unknown ground truth. We were eventually able to identify 68 malicious extensions that bypassed the vetting process of the CWS. However, our classifiers also reported over 1k likely malicious extensions which may overestimate their true number. Based on this finding (further supported with other experiments and realistic analyses), we elucidate, for the first time, a strong *concept drift* effect on browser extensions. We also provide factual evidence that commercial detectors (e.g., VirusTotal) work poorly to detect known malicious extensions. Altogether, our results highlight the fact that detecting malicious browser extensions is a fundamentally hard problem which has not (yet) received an adequate degree of attention. This requires additional work both by the research community and by Google itself—potentially by revising their approaches. In the meantime, we informed Google of our discoveries, and we release our artifacts.

CCS Concepts: • **Security and privacy → Web application security**; **Social aspects of security and privacy**; • **Computing methodologies →** *Machine learning*; • **Information systems → World Wide Web**.

Additional Key Words and Phrases: Google Chrome; Browser Extensions; Classification; Concept Drift

> It's not Easy: Applying Supervised ML to Detect Malicious Extensions in the CWS

In *ACM TWEB* 2026. Ben Rosenzweig, Valentino Dalla Valle, Giovanni Apruzzese, and Aurore Fass



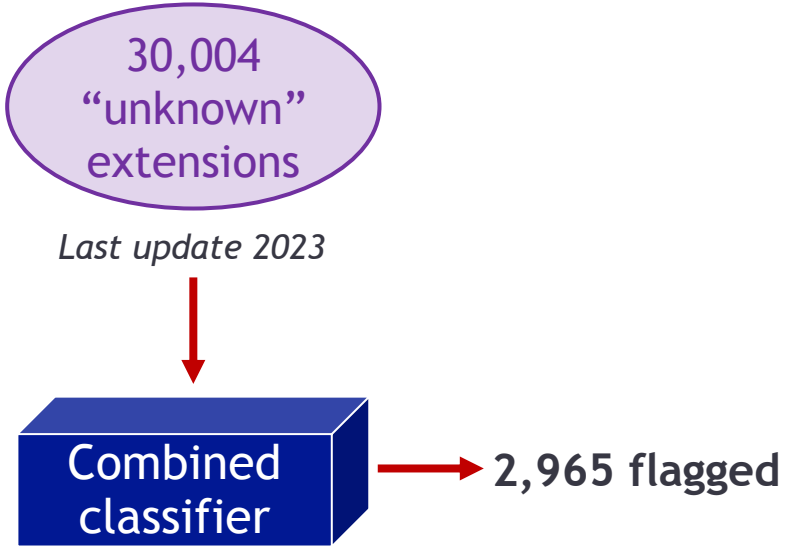
Detecting Malicious Extensions — Real World

30,004 “unknown” extensions

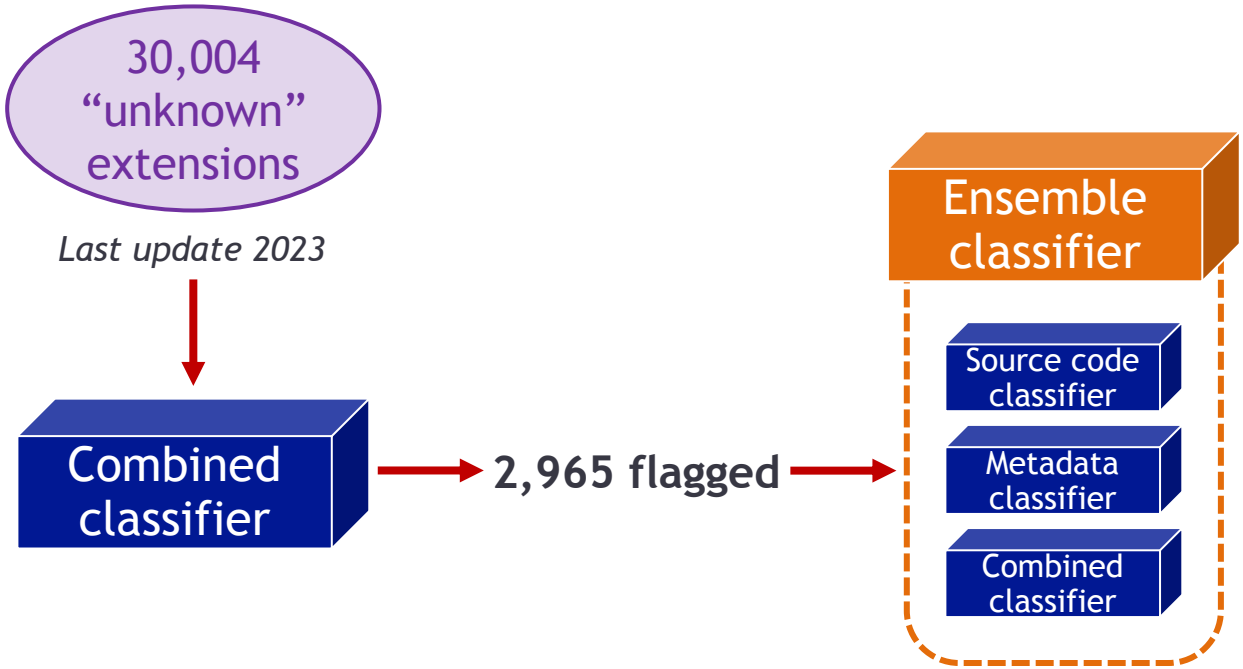
Last update 2023

[3] Rosenzweig, Dalla Valle, Apruzzese, and Fass; *TWEB* 2026

Detecting Malicious Extensions — Real World

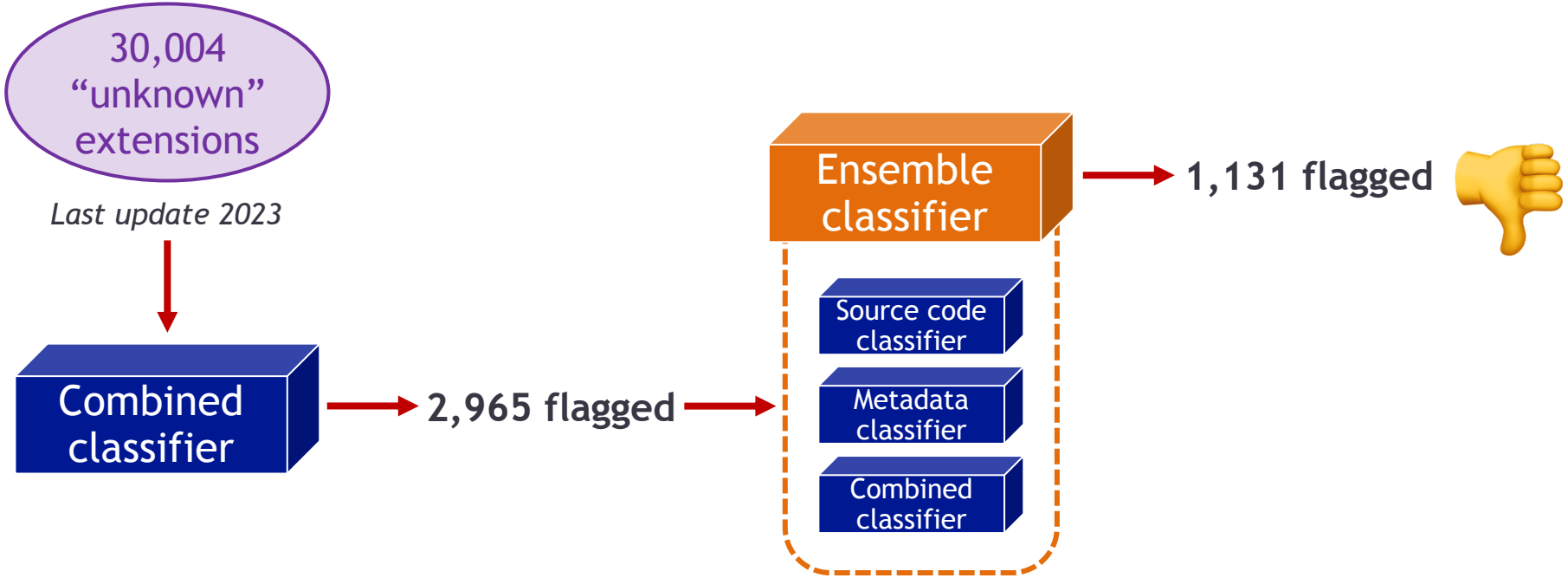


Detecting Malicious Extensions — Real World



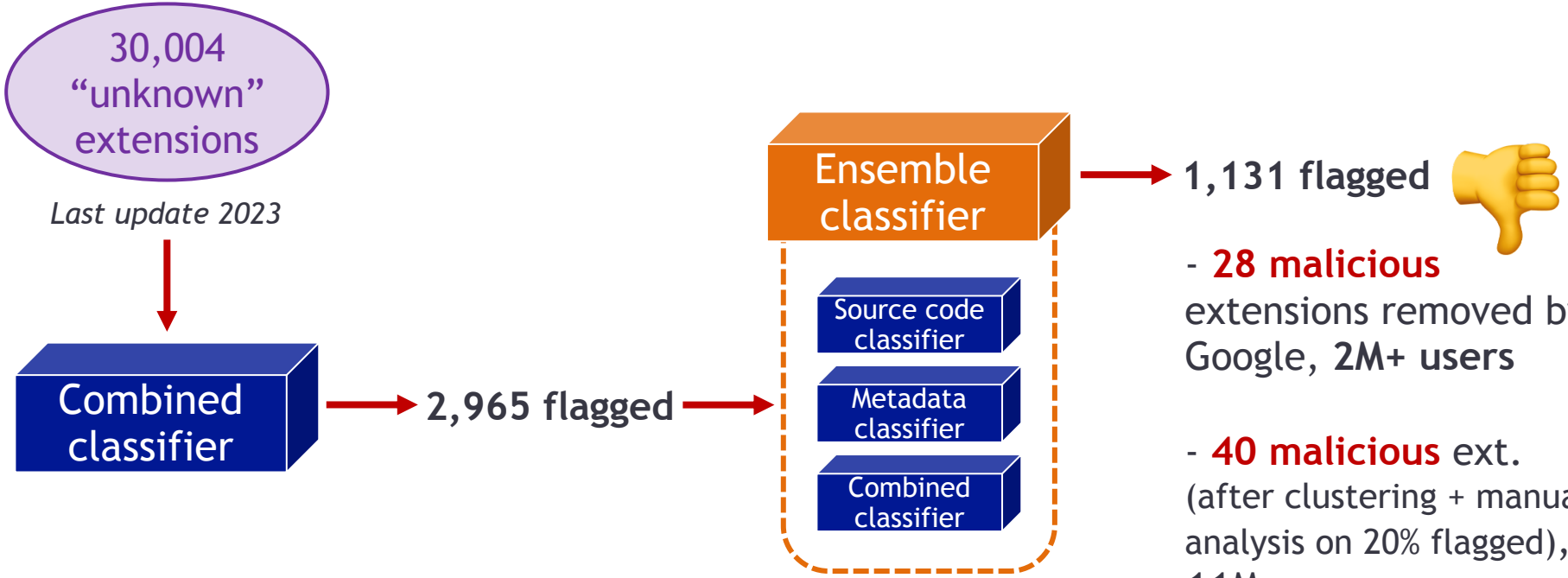
[3] Rosenzweig, Dalla Valle, Apruzzese, and Fass; *TWEB* 2026

Detecting Malicious Extensions — Real World



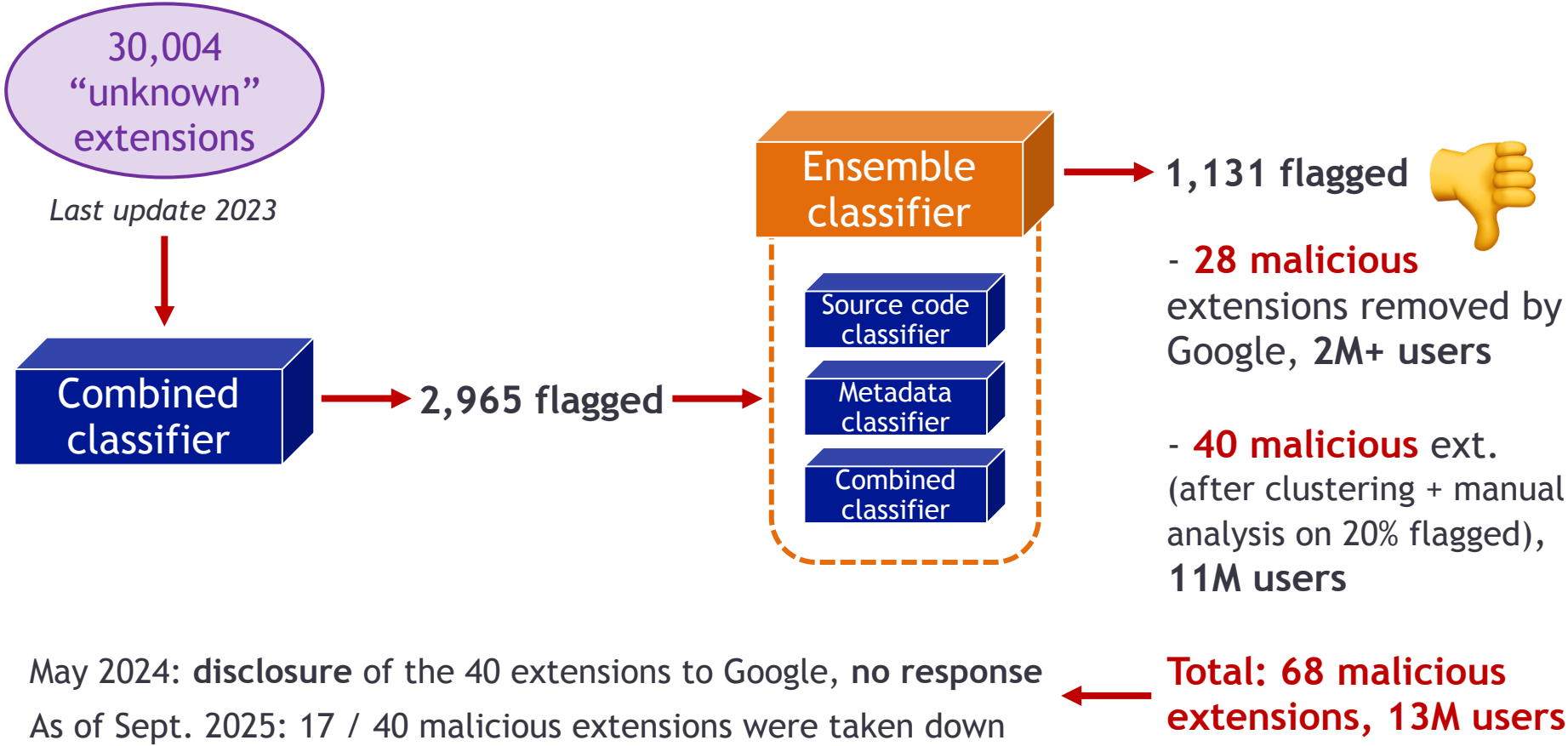
[3] Rosenzweig, Dalla Valle, Apruzzese, and Fass; *TWEB* 2026

Detecting Malicious Extensions — Real World



[3] Rosenzweig, Dalla Valle, Apruzzese, and Fass; *TWEB* 2026

Detecting Malicious Extensions — Real World



[3] Rosenzweig, Dalla Valle, Apruzzese, and Fass; *TWEB* 2026

Detecting Malicious Extensions — Lab Setting vs. Real World

- **Lab setting**: 98.37% accuracy
- **Real world**: 1,131 / 30,004 extensions flagged | 68 verified malicious extensions

???

[3] Rosenzweig, Dalla Valle, Apruzzese, and Fass; *TWEB* 2026

Detecting Malicious Extensions — Lab Setting vs. Real World

- **Lab setting**: 98.37% accuracy
- **Real world**: 1,131 / 30,004 extensions flagged | 68 verified malicious extensions

???

- **Concept drift**
  - **Intrinsic evolution** of extensions, hard for supervised ML tools to keep a (high) accuracy over time
  - **How** to validate concept drift? → see experiments in the paper
  - **Why** are extensions affected? → see paper (study feature importance)

[3] Rosenzweig, Dalla Valle, Apruzzese, and Fass; *TWEB* 2026

Detecting Malicious Extensions — Takeaways

- ML evaluations can be **misleading**: detectors performing well in a lab setting are **no guarantee of practical applicability** in the real world

- Detectors need to be **retrained regularly**

- Our code and datasets are **publicly available**:

https://github.com/its-not-easy/tweb25/

[3] Rosenzweig, Dalla Valle, Apruzzese, and Fass; *TWEB* 2026

Same Extension, Different Stores

Chaudhry et al.
MADWeb 2026

Two Heads are Better Than One:
Analysing Browser Extensions Across Stores

Abdullah Hassan Chaudhry
CISPA Helmholtz Center
for Information Security
abdullah.chaudry@cispa.de

Valentino Dalla Valle
CISPA Helmholtz Center
for Information Security
valentino.dalla-valle@cispa.de

Aurore Fass
Inria Centre at Université
Côte d'Azur
aurore.fass@inria.fr

***Abstract*—Browser extension stores operate independently of each other and each have their own governance structure, creating a situation where threats identified on one platform can persist on others. We present the first cross-store analysis of security inconsistencies between the Chrome Web Store (CWS) and Edge Add-ons Store (EAS). We study extensions published on both stores, and discover 11 malicious extensions (affecting almost 134k users) that were present on the EAS, despite having already been removed from the CWS for containing malware. These extensions persisted on Edge for an average of 551 days (1.5 years) *after* their Chrome counterparts were removed for malware, with some even receiving updates during this period.**

We additionally find that malicious extensions change their names and developer names more often than other extensions and that these changes are larger. We also examine extensions that have been reinstated after having been removed (e.g., for containing malware), revealing inconsistencies in extension store governance. These findings show that malicious actors can exploit the lack of coordination in an interconnected extension ecosystem.

I. Introduction

The Web has become the dominant global technology, with the Web Browser serving as its primary access point. Browser extensions are software components that users can install to augment browser functionality with features such as password managers, shopping assistants or ad blockers. These functionalities are enabled through powerful browser APIs that are not available to ordinary websites [23], [41]. Such APIs allow extensions to read browsing history, intercept and modify network requests, manipulate web page content, store data persistently across sessions, and download files directly to users' devices. While these capabilities are essential for many legitimate use cases, they also create opportunities for abuse.

Previous research has documented numerous instances in which extensions engage in harmful activities [23], [30], [34], [36], [37], including stealing login credentials, session cookies or browsing history, injecting ads, and affiliate fraud. Beyond intentional malicious behaviour, extensions may contain vulnerabilities that enable exploitation by third parties [22], [31], [44], [46]. Collectively, vulnerable and malicious extensions have been referred by prior work as *security noteworthy*, and their prevalence has been studied extensively [34].

The number of extensions available in browser extension stores further exacerbates these security challenges. As of December 2025, the Chrome Web Store (CWS) hosts nearly 200,000 active extensions [6], with thousands being added to the store each month [34]. Security-noteworthy extensions have been observed to persist in extension stores for extended periods, sometimes months or even years before being removed [34], [41]. Moreover, extensions that were initially benign may later introduce malicious functionality through updates [25], [29], [41], highlighting the need for continuous scrutiny. These factors collectively demand automated detection systems, though the expertise of human analysts remains invaluable [36], [41].

Chrome is the most popular web browser [5], and the CWS is the largest extension marketplace. By comparison, as of December 2025, the Edge Add-on Store (EAS) has under 28,000 active extensions [7], while the Firefox Add-on Store contains fewer than 57,000 [8]. As a result, academic research on browser extension security has predominantly focused on the CWS, leaving other major extension stores comparatively under explored.

In this paper, we address this gap by examining extensions across the CWS and EAS, with a particular focus on how the two stores classify and govern the same extensions. We use the cross-store extension mapping process from ChromeStats [20] that is based on metadata (e.g., developer names and extension descriptions) to identify a dataset of equivalent extensions (*counterparts*) on the CWS and EAS. We study extension counterparts where the Chrome extension was removed from the CWS for malware. We then analyse both historical and current versions of these extensions and apply code similarity analysis to identify malicious extensions that persist on EAS.

Our analysis uncovers 20 malicious extension versions on the EAS that were never removed by the store administrators. These versions correspond to 13 unique extensions, 11 of which remained active at the end of our study period (March 2025). We demonstrate that extensions removed from one store can remain active and continue to receive updates on another store for years, despite containing identical malicious payloads. Finally, we examine a potential evasion technique that hinders cross-store mapping and discuss its applicability

Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb) 2026
27 February 2026, San Diego, CA, USA
ISBN 978-1-970672-06-0
https://dx.doi.org/10.14722/madweb.2026.23027
www.ndss-symposium.org

> Two Heads are Better Than One: Analysing Extensions Across Stores

In *MADWeb 2026*. Abdullah Chaudhry, Valentino Dalla Valle, and Aurore Fass

Same Extension, Different Stores


Two Heads are Better Than One:
Analysing Browser Extensions Across Stores

Abdullah Hassan Chaudhry, CISPA Helmholtz Center for Information Security, abdullah.chaudry@cispa.de
Valentino Dalla Valle, CISPA Helmholtz Center for Information Security, valentino.dalla-valle@cispa.de
Aurore Fass, Inria Centre at Université Côte d'Azur, aurore.fass@inria.fr

Chaudhry et al.
MADWeb 2026

> Two Heads are Better Than One: Analysing Extensions Across Stores

In *MADWeb 2026*. Abdullah Chaudhry, Valentino Dalla Valle, and Aurore Fass

- A given extension can be removed for malware on Chrome…
- … but not on another store like Edge
- Open source: https://github.com/abdchau/two-heads-are-better

Summary

Dangerous Browser Extensions

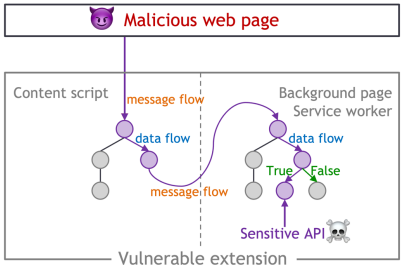
Hsu et al. AsiaCCS 2024

→ **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
- **Contain vulnerabilities:** designed by well-intentioned developers… but buggy
  - E.g., can lead to user-sensitive data exfiltration
- **Violate the Chrome Web Store policies**
  - E.g., deceive users, promote unlawful activities, lack a privacy policy
- **Be fingerprintable:** can be recognized and uniquely identified
  - E.g., can lead to user tracking or inferring of user personal information

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%**

Detecting Fingerprintable Extensions with Raider

Agarwal et al. CCS 2024

- 1) Extensions send **PostMessage** to web pages
- 2) Extensions store data on the client side through **storage APIs**
  (e.g., cookies, local/session storage, IndexedDB)
- 3) Extensions **inject JavaScript** code directly into web pages
  → registering global variables
  → invocation of global APIs and properties

Raider-ext/raider

➢ Raider detects **2,747** fingerprintable extensions | **169M users**

Detecting Malicious Extensions – Lab Setting vs. Real World

- **Lab setting:** 98.37% accuracy
- **Real world:** 1,131 / 30,004 extensions flagged | 68 verified malicious extensions

Rosenzweig et al. TWEB 2026

its-not-easy/tweb25

- **Concept drift**
  - **Intrinsic evolution** of extensions, hard for supervised ML tools to keep a (high) accuracy over time
  - **How** to validate concept drift? → see experiments in the paper
  - **Why** are extensions affected? → see paper (study feature importance)

Open Questions

REDACTED :)

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

- It's not Easy: Applying Supervised ML to Detect Malicious Extensions in the Chrome Web Store

Ben Rosenzweig, Valentino Dalla Valle, Giovanni Apruzzese, and Aurore Fass. In *ACM TWEB* 2026

- Two Heads are Better Than One: Analysing Extensions Across Stores

Abdullah Hassan Chaudhry, Valentino Dalla Valle, and Aurore Fass. In MADWeb 2026