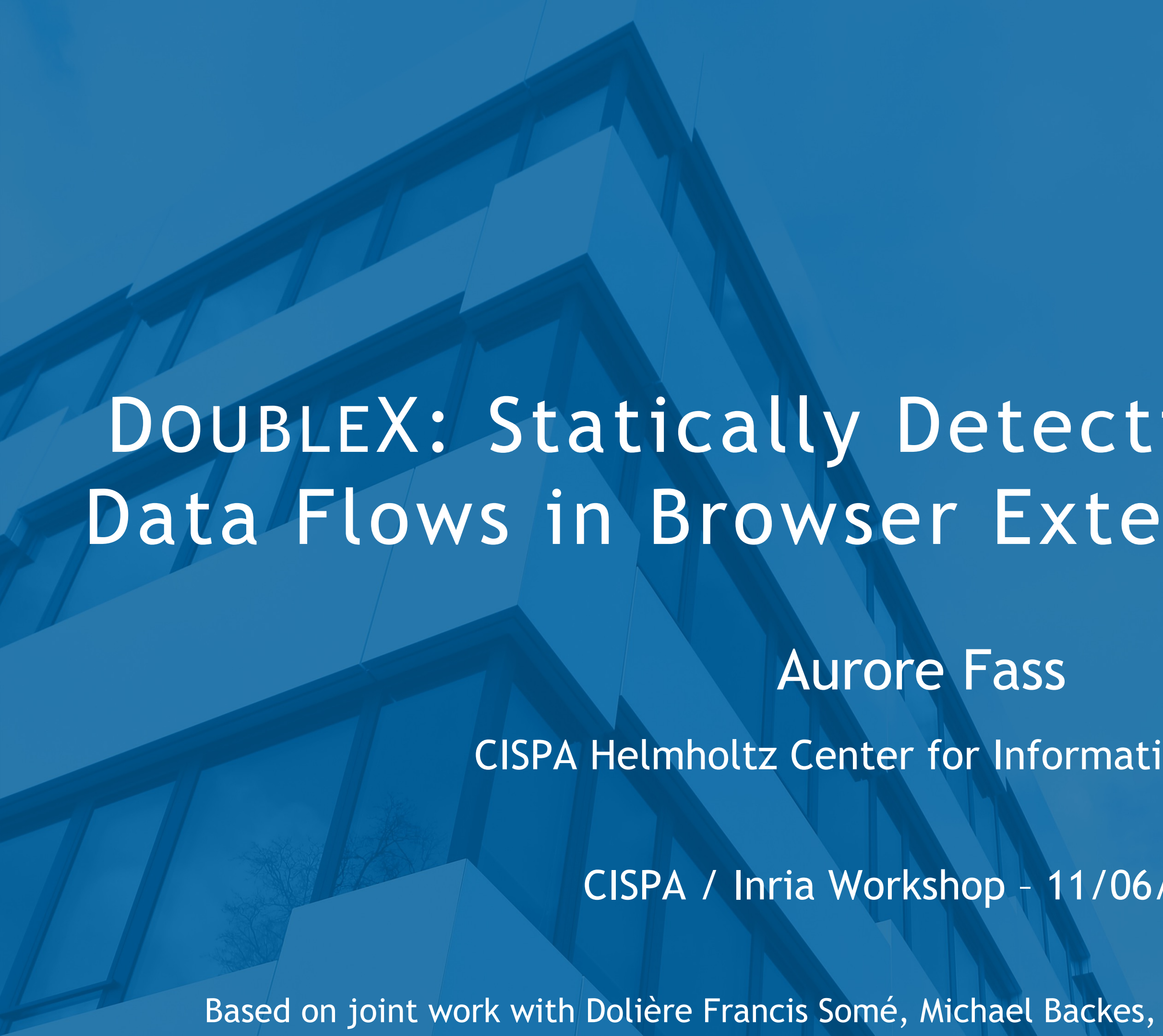


DoubleX: Statically Detecting Vulnerable Data Flows in Browser Extensions at Scale

Aurore Fass

CISPA Helmholtz Center for Information Security

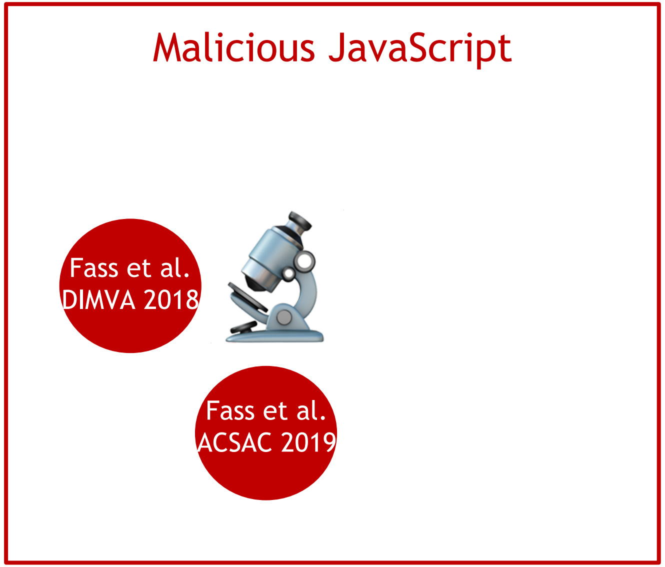
CISPA / Inria Workshop – 11/06/2023

Based on joint work with Dolière Francis Somé, Michael Backes, and Ben Stock at *ACM CCS 2021*

Aurore (/ɔʀɔʀ/)

- Graduated from TELECOM Nancy (2017)
- PhD Student + Postdoc at CISPA (2017—21)
- Visiting Assistant Professor at Stanford (2021—23)
- Tenure-Track Faculty at CISPA (2023—)

Research: Web Security, Privacy, Measurements

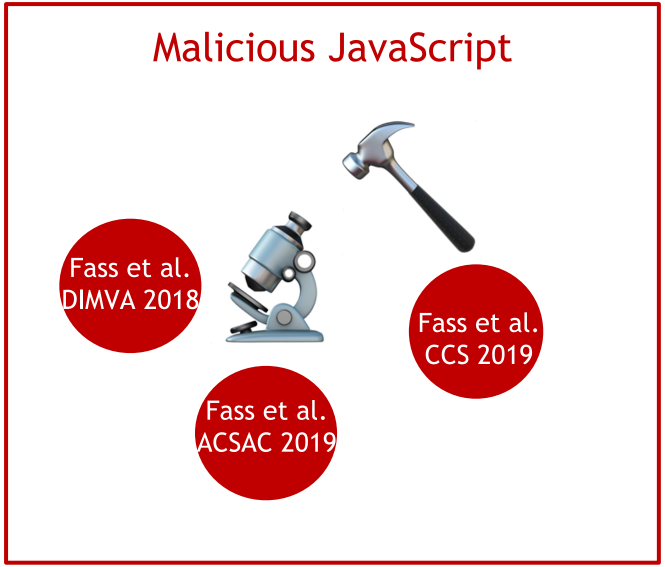


Malicious JavaScript

Fass et al.
DIMVA 2018

Fass et al.
ACSAC 2019

Research: Web Security, Privacy, Measurements



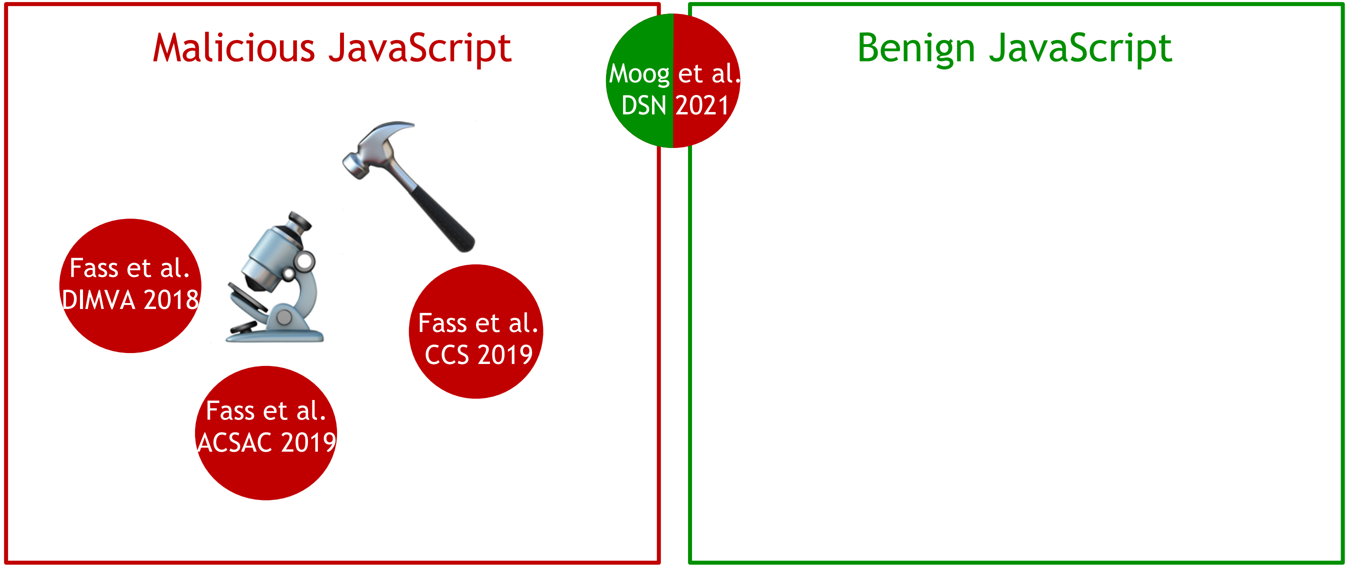
Malicious JavaScript

Fass et al.
DIMVA 2018

Fass et al.
CCS 2019

Fass et al.
ACSAC 2019

Research: Web Security, Privacy, Measurements



Malicious JavaScript

Fass et al. DIMVA 2018

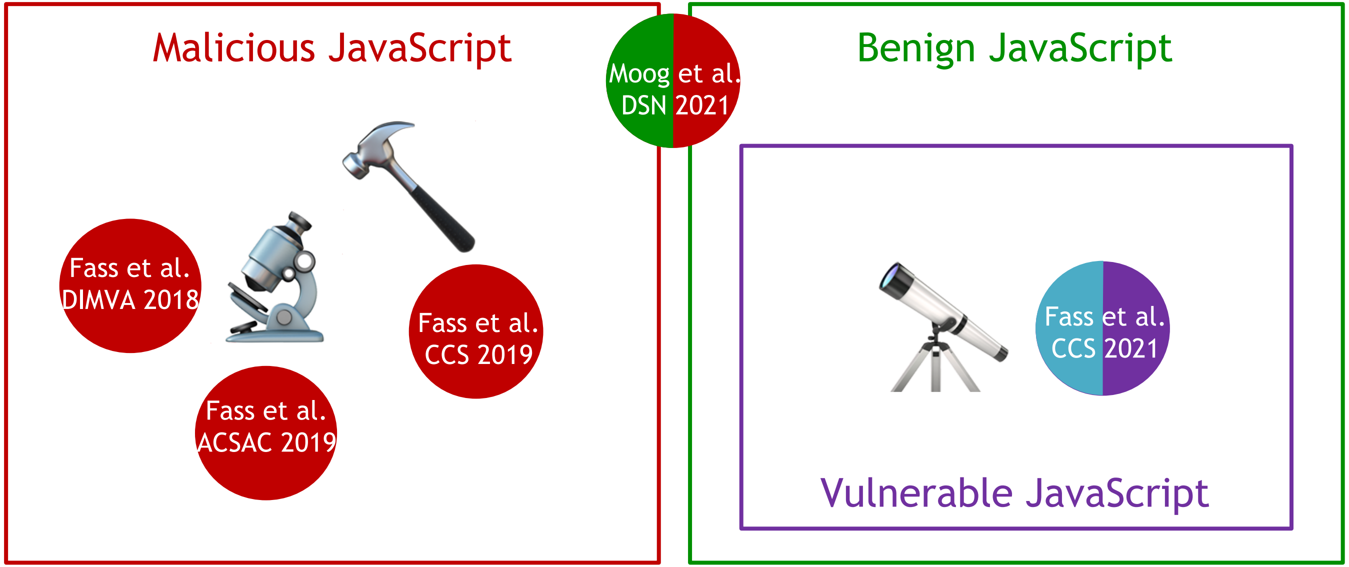
Fass et al. ACSAC 2019

Fass et al. CCS 2019

Moog et al. DSN 2021

Benign JavaScript

Research: Web Security, Privacy, Measurements



Malicious JavaScript

Fass et al. DIMVA 2018

Fass et al. CCS 2019

Fass et al. ACSAC 2019

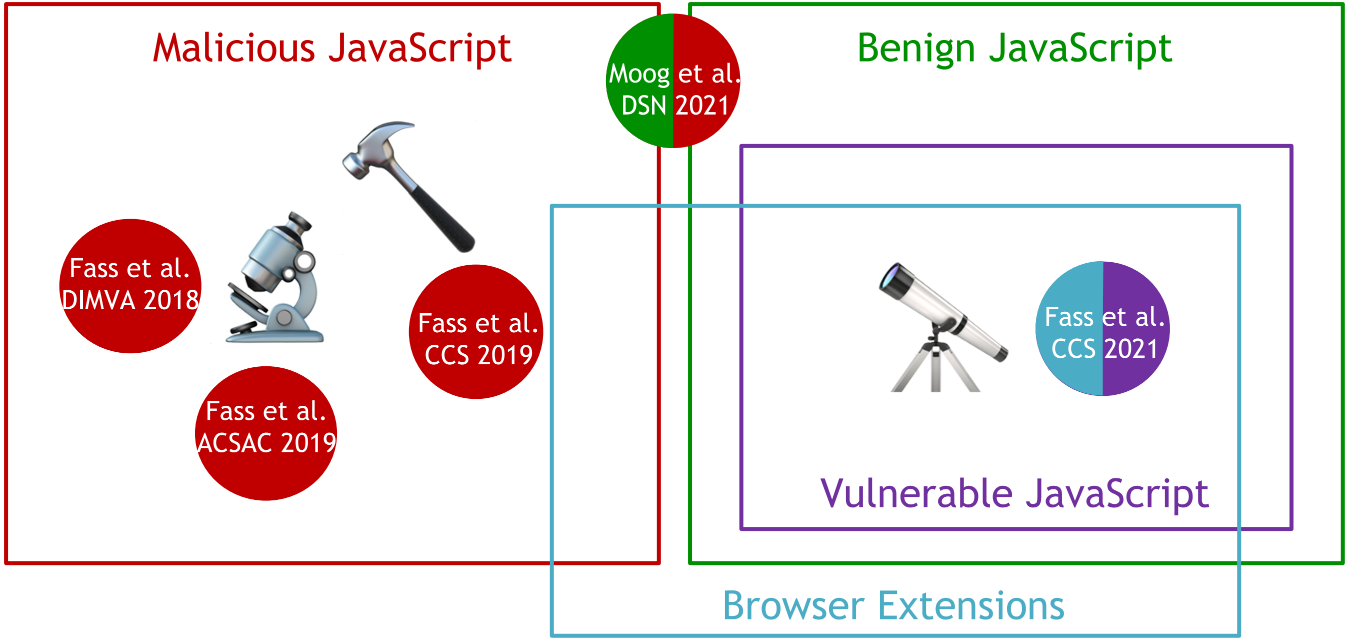
Moog et al. DSN 2021

Benign JavaScript

Fass et al. CCS 2021

Vulnerable JavaScript

Research: Web Security, Privacy, Measurements



Malicious JavaScript

Benign JavaScript

Moog et al.
DSN 2021

Fass et al.
DIMVA 2018

Fass et al.
CCS 2019

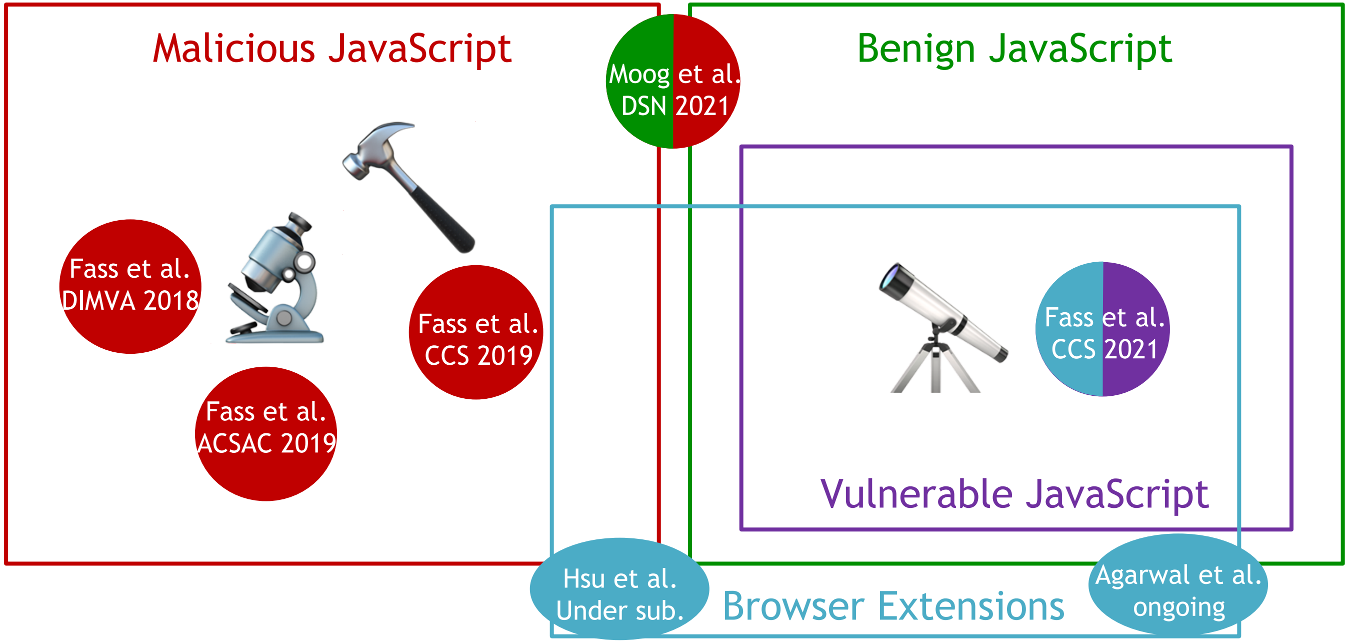
Fass et al.
ACSAC 2019

Fass et al.
CCS 2021

Vulnerable JavaScript

Browser Extensions

Research: Web Security, Privacy, Measurements



Malicious JavaScript

Fass et al. DIMVA 2018

Fass et al. CCS 2019

Fass et al. ACSAC 2019

Moog et al. DSN 2021

Benign JavaScript

Fass et al. CCS 2021

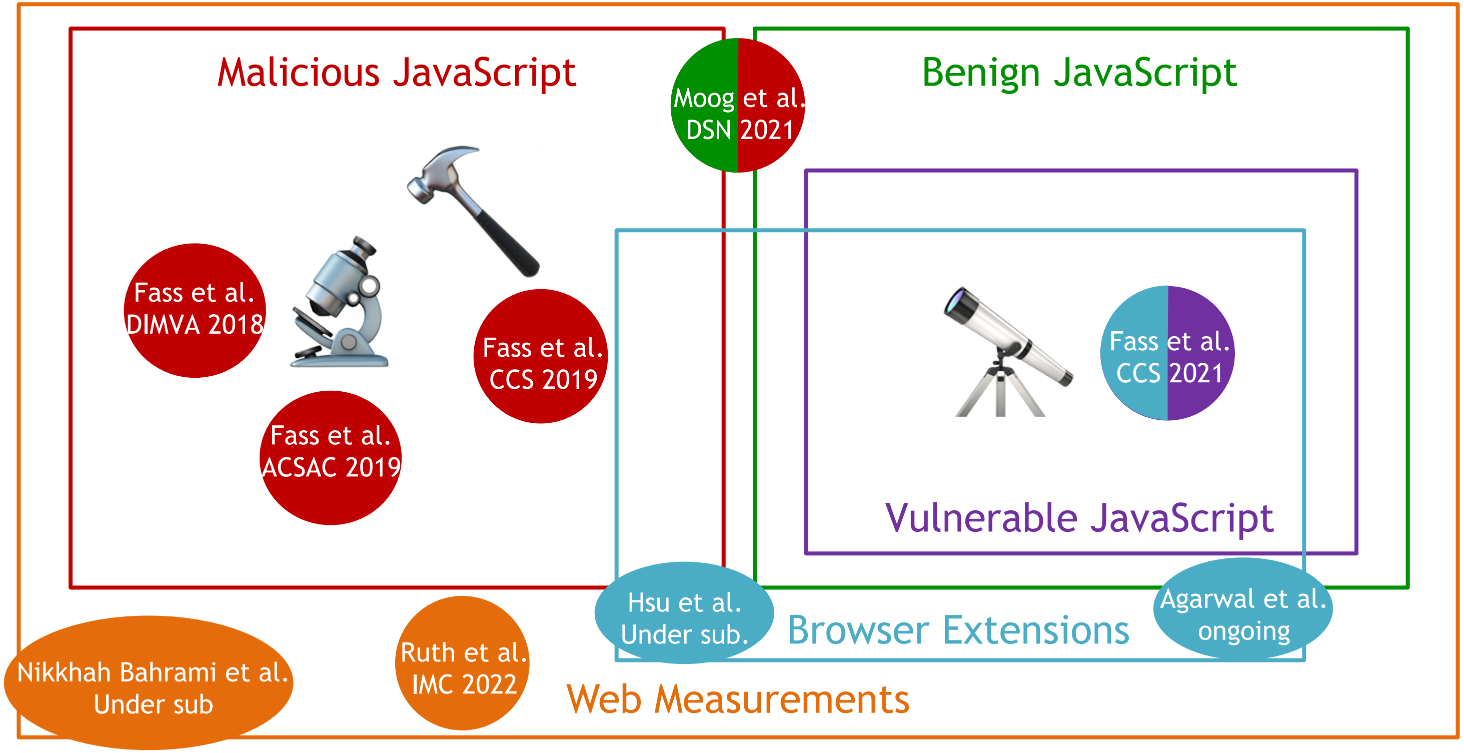
Vulnerable JavaScript

Hsu et al. Under sub.

Browser Extensions

Agarwal et al. ongoing

Research: Web Security, Privacy, Measurements



Malicious JavaScript

Benign JavaScript

Moog et al. DSN 2021

Fass et al. DIMVA 2018

Fass et al. CCS 2019

Fass et al. ACSAC 2019

Fass et al. CCS 2021

Vulnerable JavaScript

Hsu et al. Under sub.

Browser Extensions

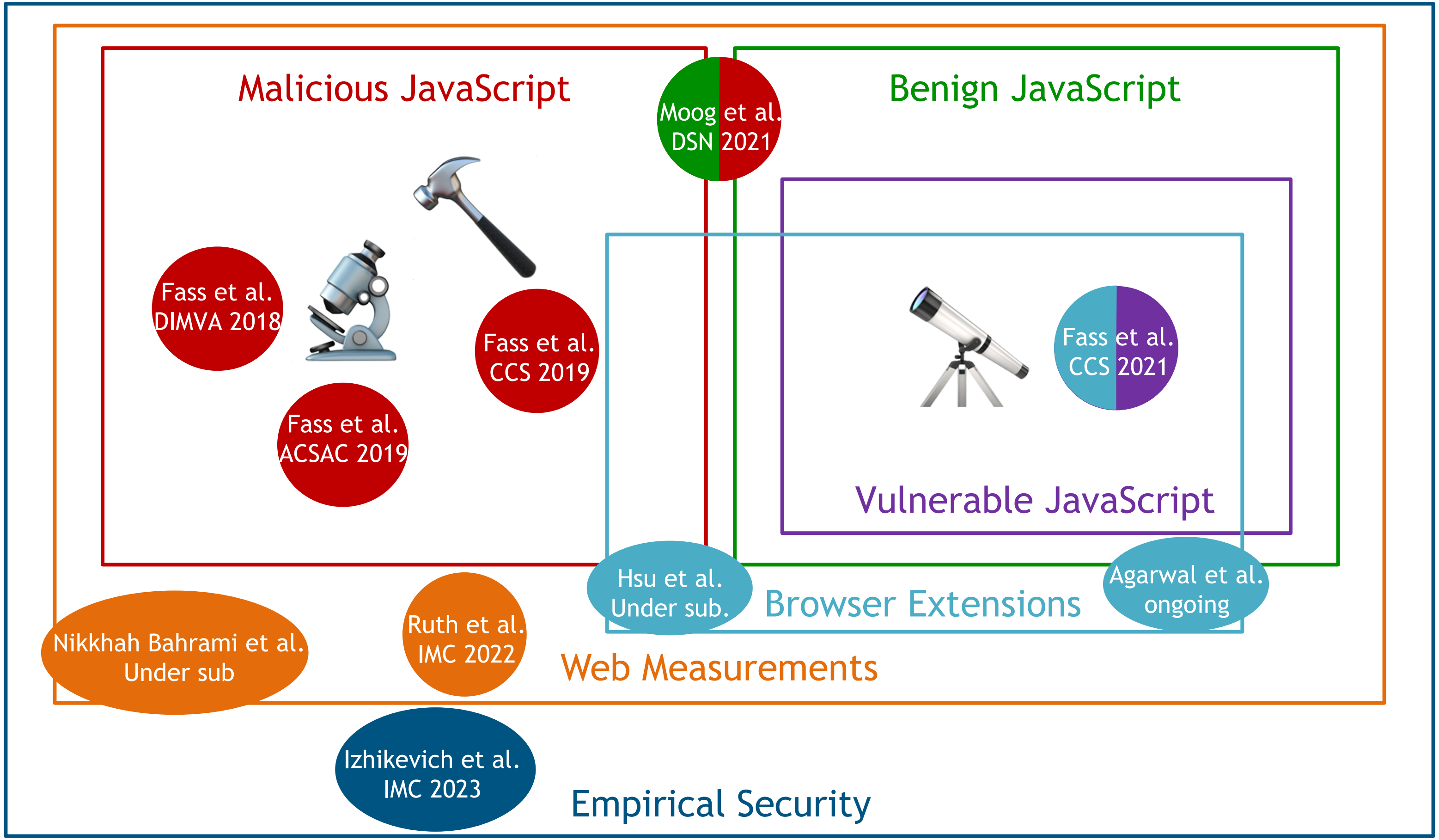
Agarwal et al. ongoing

Nikkhah Bahrami et al. Under sub

Ruth et al. IMC 2022

Web Measurements

Research: Web Security, Privacy, Measurements



Malicious JavaScript

Fass et al. DIMVA 2018

Fass et al. CCS 2019

Fass et al. ACSAC 2019

Moog et al. DSN 2021

Benign JavaScript

Vulnerable JavaScript

Fass et al. CCS 2021

Browser Extensions

Hsu et al. Under sub.

Agarwal et al. ongoing

Web Measurements

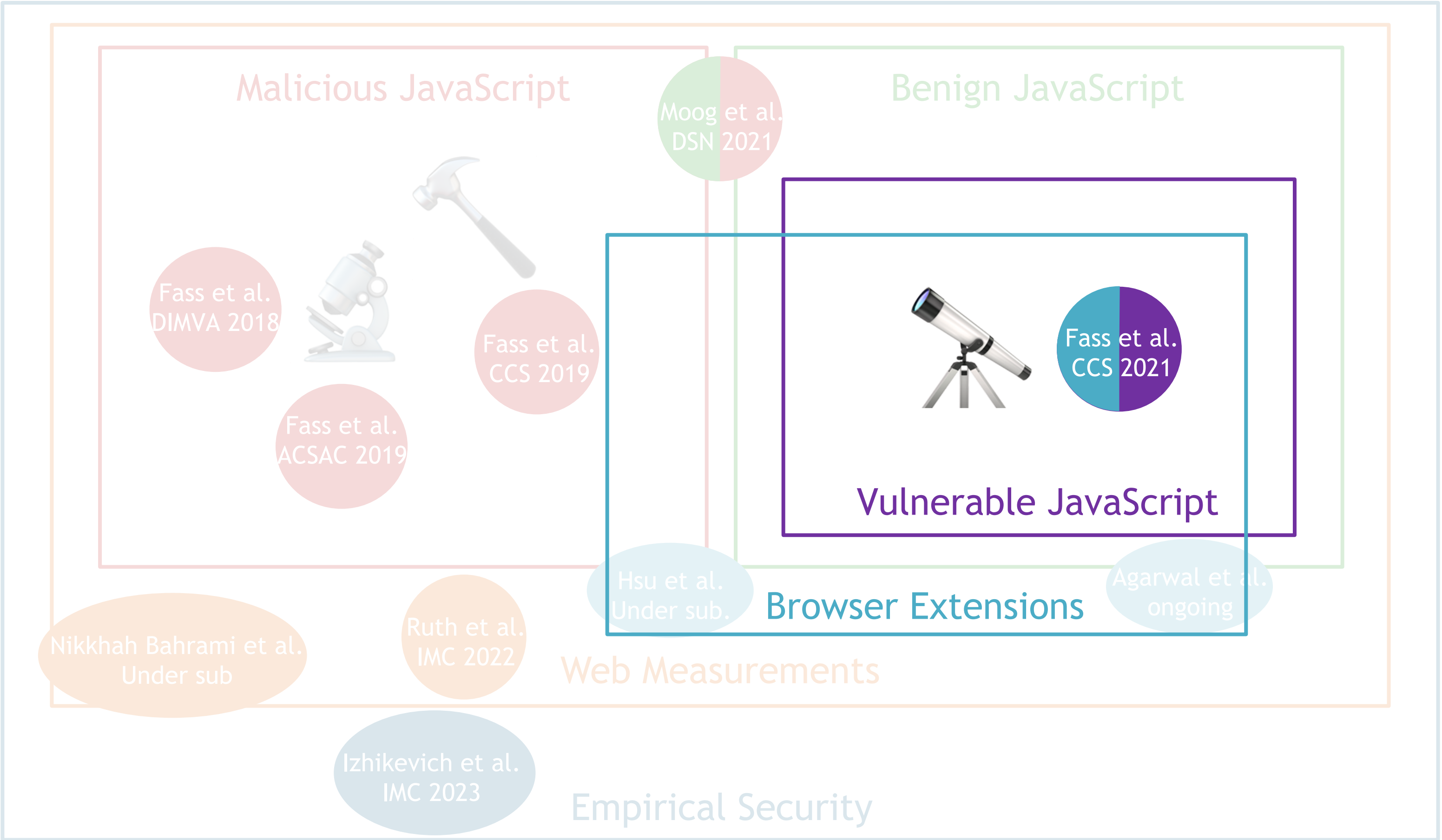
Nikkhah Bahrami et al. Under sub

Ruth et al. IMC 2022

Empirical Security

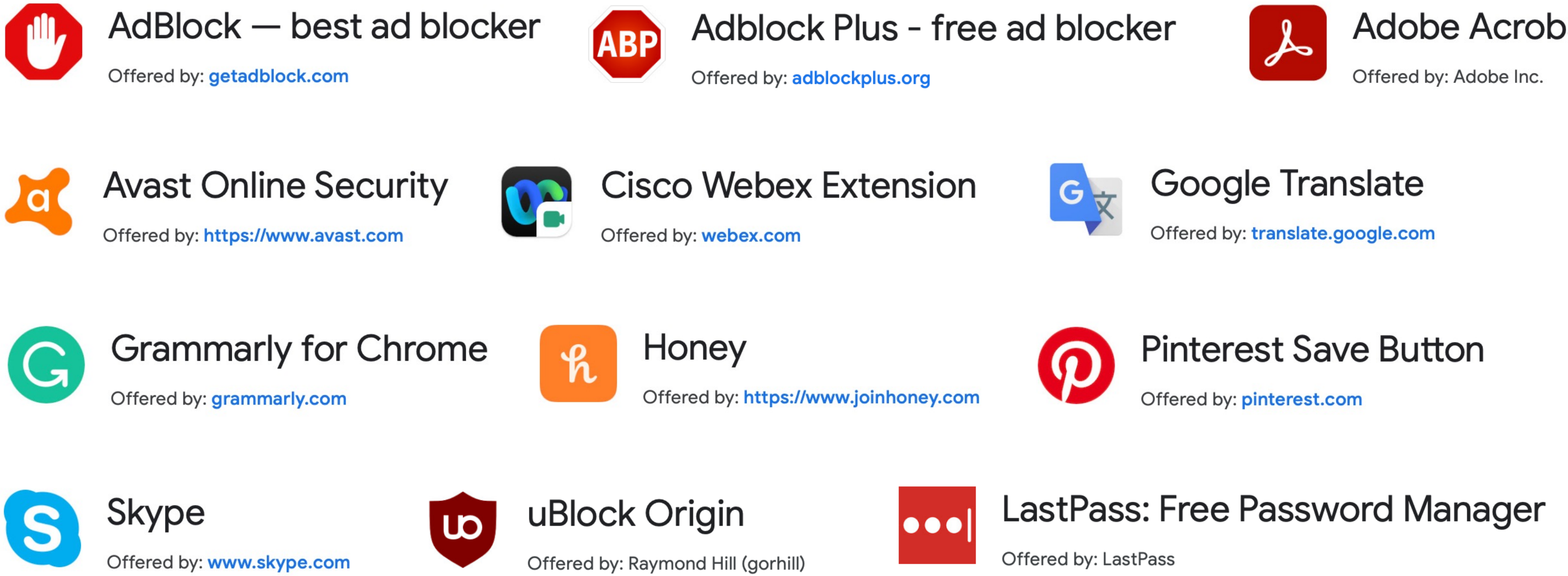
Izhikevich et al. IMC 2023

Research: Web Security, Privacy, Measurements



Browser Extensions…

are popular to improve user browsing experience



AdBlock — best ad blocker
Offered by: getadblock.com

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

Adobe Acrobat
Offered by: Adobe Inc.

Avast Online Security
Offered by: https://www.avast.com

Cisco Webex Extension
Offered by: webex.com

Google Translate
Offered by: translate.google.com

Grammarly for Chrome
Offered by: grammarly.com

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

Pinterest Save Button
Offered by: pinterest.com

Skype
Offered by: www.skype.com

uBlock Origin
Offered by: Raymond Hill (gorhill)

LastPass: Free Password Manager
Offered by: LastPass

Browser Extensions…

are popular to improve user browsing experience

BUT

AdBlock — best ad blocker

Offered by: getadblock.com

Adblock Plus - free ad blocker

Offered by: adblockplus.org

Adobe Acrobat

Offered by: Adobe Inc.

Avast Online Security

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

Cisco Webex Extension

Offered by: webex.com

Google Translate

Offered by: translate.google.com

Grammarly for Chrome

Offered by: grammarly.com

Honey

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

Pinterest Save Button

Offered by: pinterest.com

Skype

Offered by: www.skype.com

uBlock Origin

Offered by: Raymond Hill (gorhill)

LastPass: Free Password Manager

Offered by: LastPass

Browser Extensions…

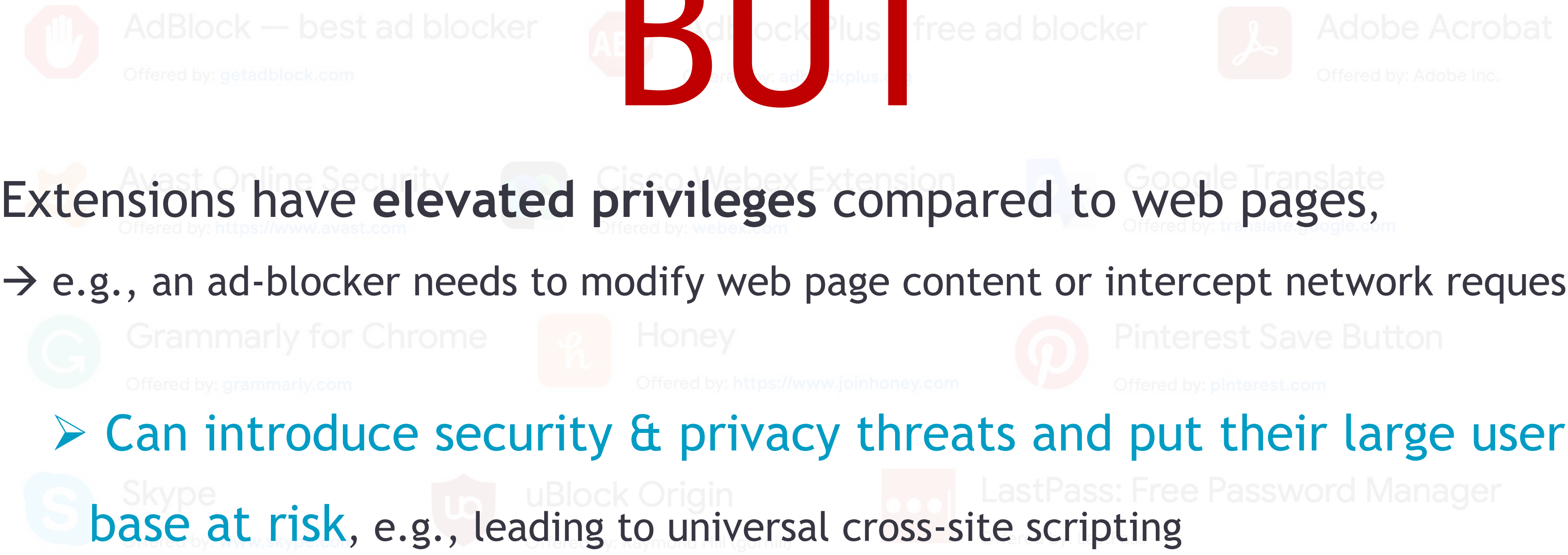
are popular to improve user browsing experience

BUT

Extensions have **elevated privileges** compared to web pages,

→ e.g., an ad-blocker needs to modify web page content or intercept network requests

➢ Can introduce security & privacy threats and put their large user base at risk, e.g., leading to universal cross-site scripting



AdBlock — best ad blocker
Offered by: getadblock.com

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

Adobe Acrobat
Offered by: Adobe Inc.

Avast Online Security
Offered by: https://www.avast.com

Cisco Webex Extension
Offered by: webex.com

Google Translate
Offered by: translate.google.com

Grammarly for Chrome
Offered by: grammarly.com

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

Pinterest Save Button
Offered by: pinterest.com

Skype
Offered by: www.skype.com

uBlock Origin
Offered by: Raymond Hill (gorhill)

LastPass: Free Password Manager
Offered by: LastPass

Motivation — Detecting *Vulnerable* Extensions

- Prior work: focus on *malicious* extensions [1—4]

[1] Chen et al., ACM CCS 2018
[2] Jagpal et al., USENIX Security 2015
[3] Kapravelos et al., USENIX Security 2014
[4] Pantelaios at al., ACM CCS 2020

→ Vetting process before an extension is published on the Chrome Web Store

[5] Somé, IEEE S&P 2019

Motivation – Detecting *Vulnerable* Extensions

- Prior work: focus on *malicious* extensions [1–4]

  [1] Chen et al., ACM CCS 2018
  [2] Jagpal et al., USENIX Security 2015
  [3] Kapravelos et al., USENIX Security 2014
  [4] Pantelaios at al., ACM CCS 2020

  → Vetting process before an extension is published on the Chrome Web Store

- Our focus: **vulnerable extensions** (= benign but buggy)
  - Designed by **well-intentioned developers** but contain vulnerabilities that an attacker could exploit
  - **Challenging to detect**, due to their inherently benign intent
  - Prior work mostly manual + 95% false positives [5]

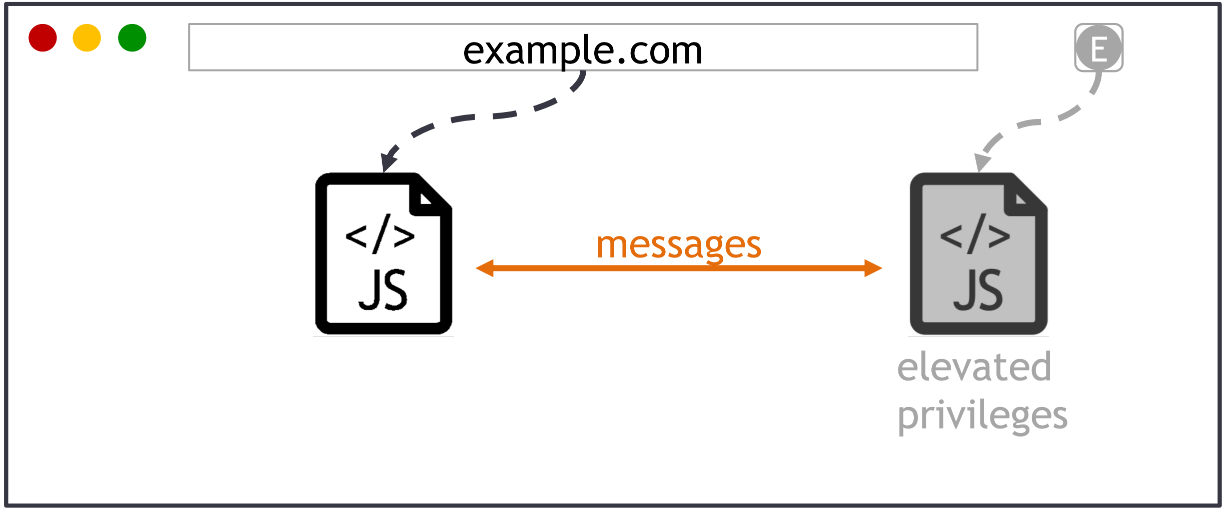
[5] Somé, IEEE S&P 2019

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

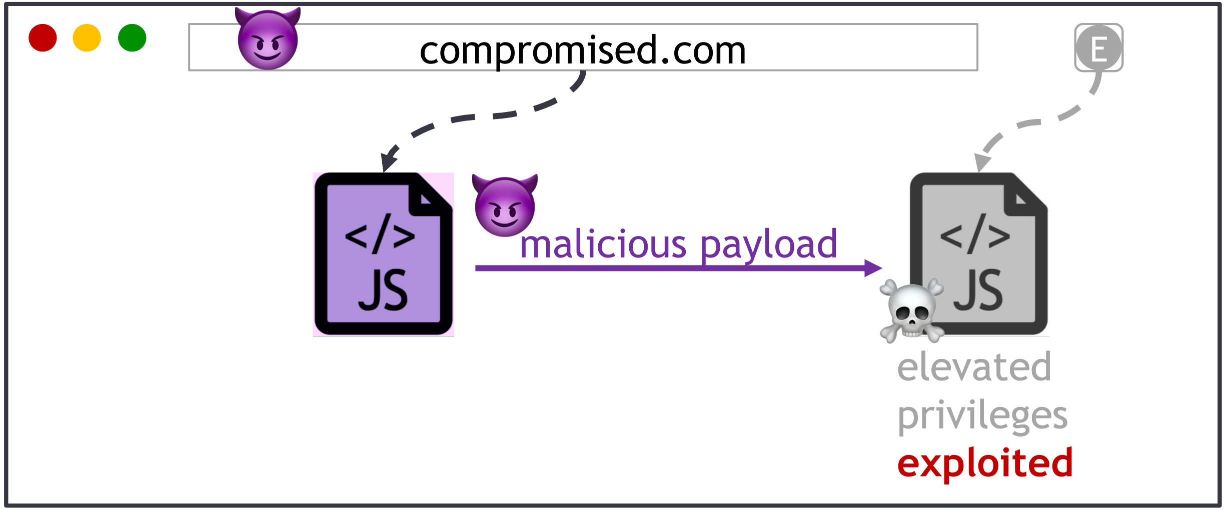
Aurore Fass, Dolière Francis Somé, Michael Backes, and Ben Stock

ACM CCS 2021

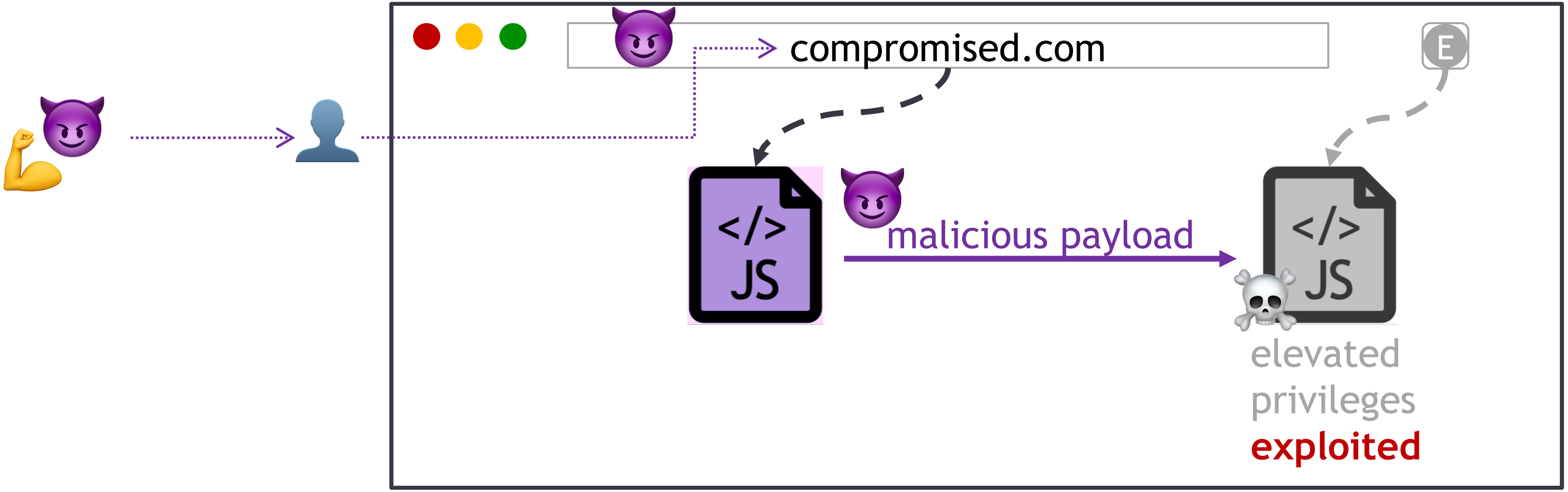
Exploiting Vulnerable Extensions



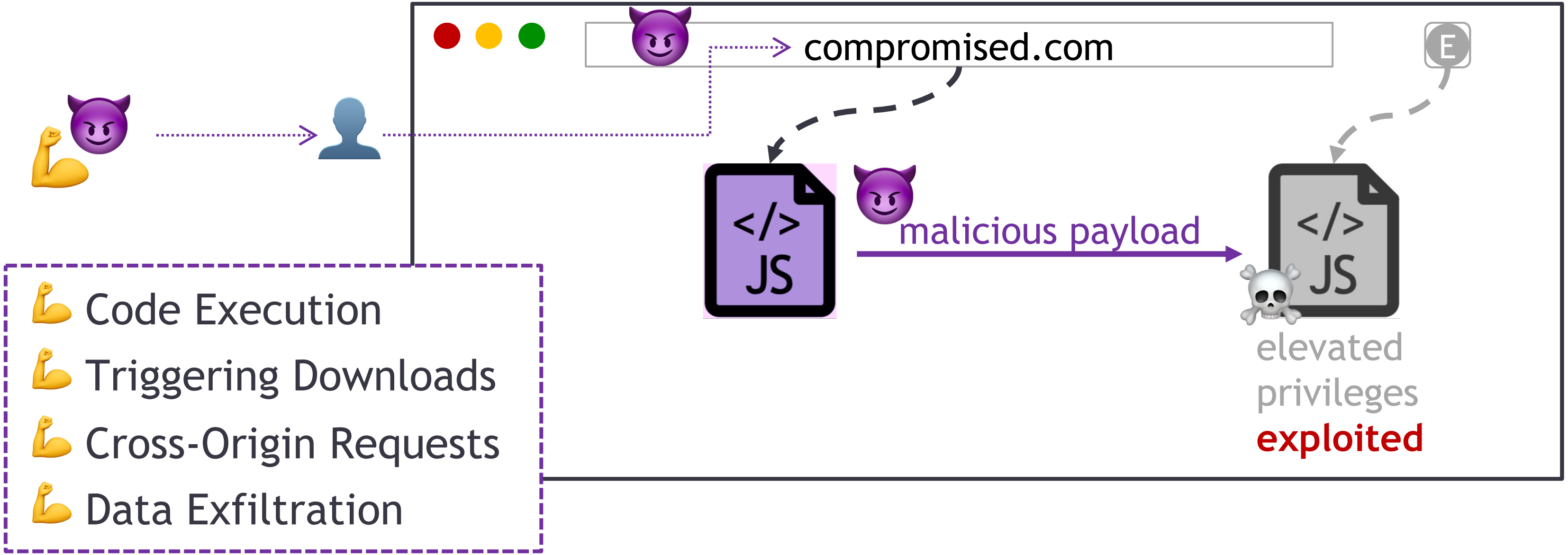
Exploiting Vulnerable Extensions



Exploiting Vulnerable Extensions

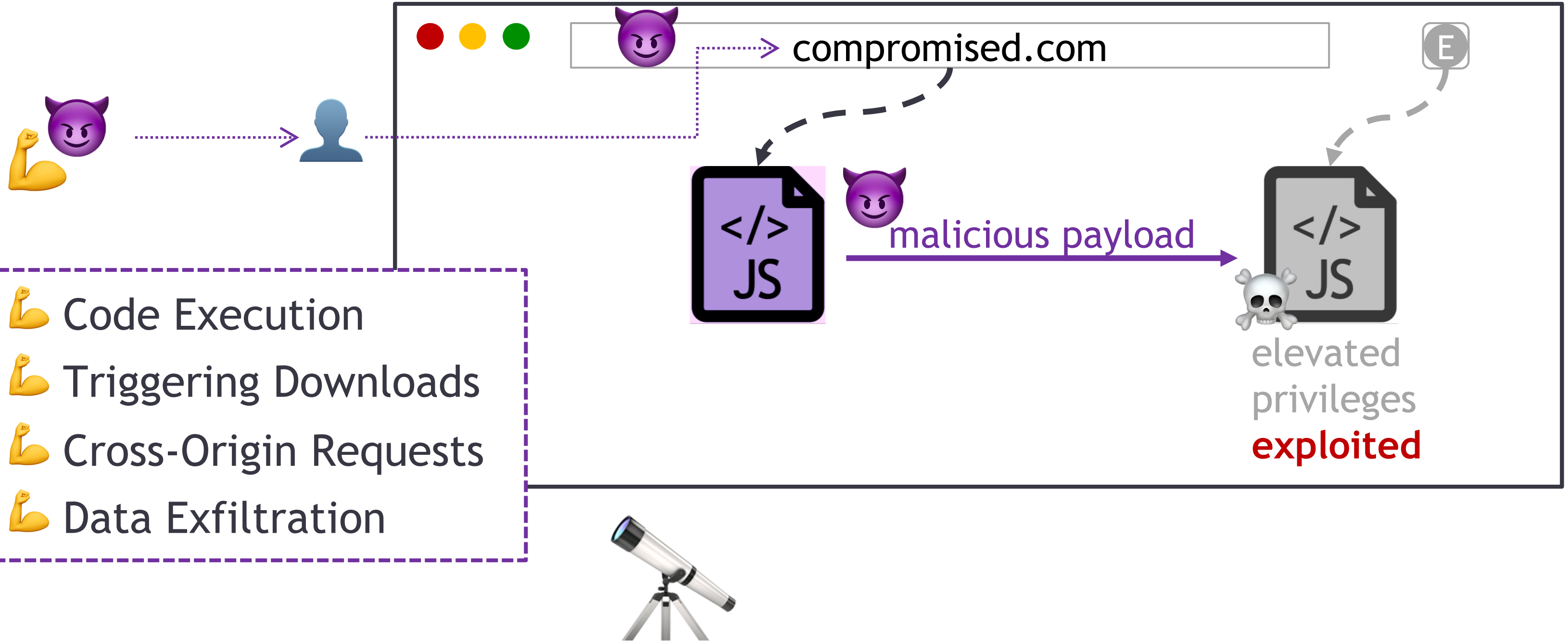


Exploiting Vulnerable Extensions



- 💪 Code Execution
- 💪 Triggering Downloads
- 💪 Cross-Origin Requests
- 💪 Data Exfiltration

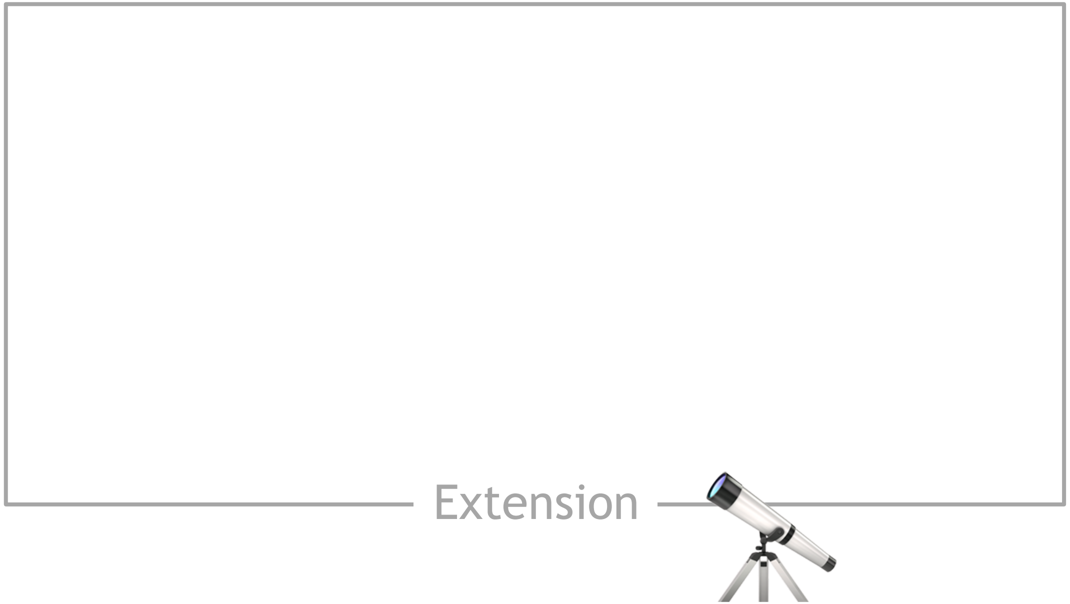
Exploiting Vulnerable Extensions



- 💪 Code Execution
- 💪 Triggering Downloads
- 💪 Cross-Origin Requests
- 💪 Data Exfiltration

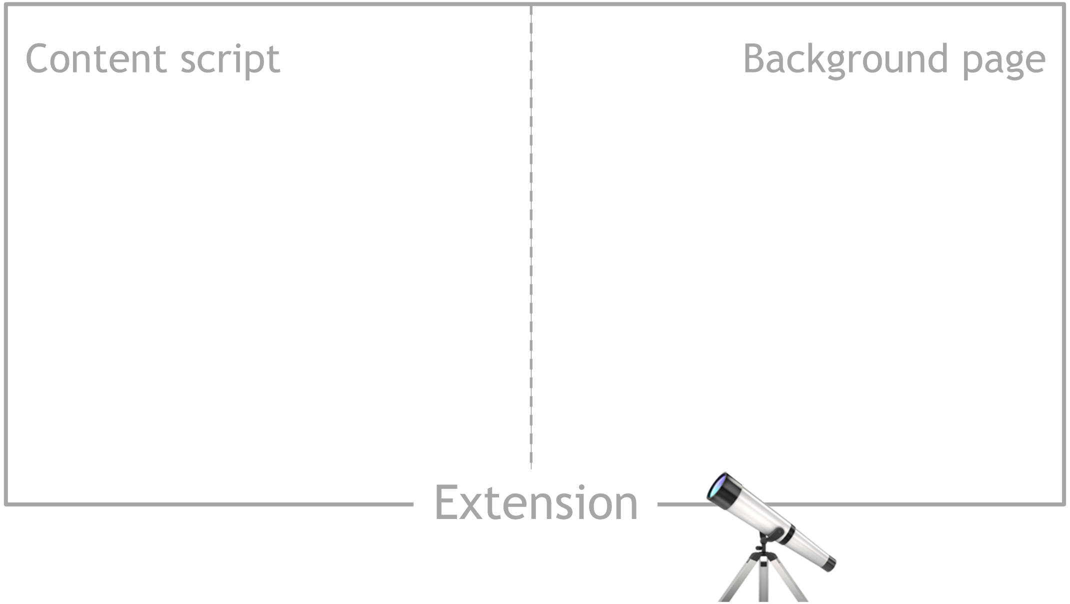
→ **DOUBLEX: detects suspicious data flows from and toward an extension privileged context**

Extension Architecture and Communication



→ **DoubleX: detects suspicious data flows from and toward an extension privileged context**

Extension Architecture and Communication



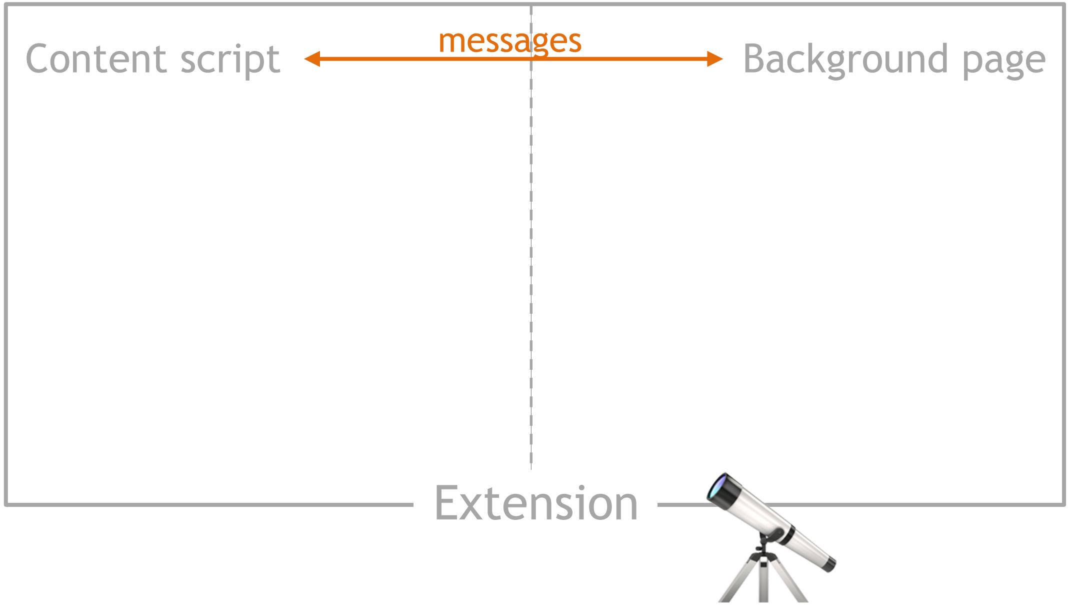
Content script

Background page

Extension

→ **DoubleX: detects suspicious data flows from and toward an extension privileged context**

Extension Architecture and Communication



Content script

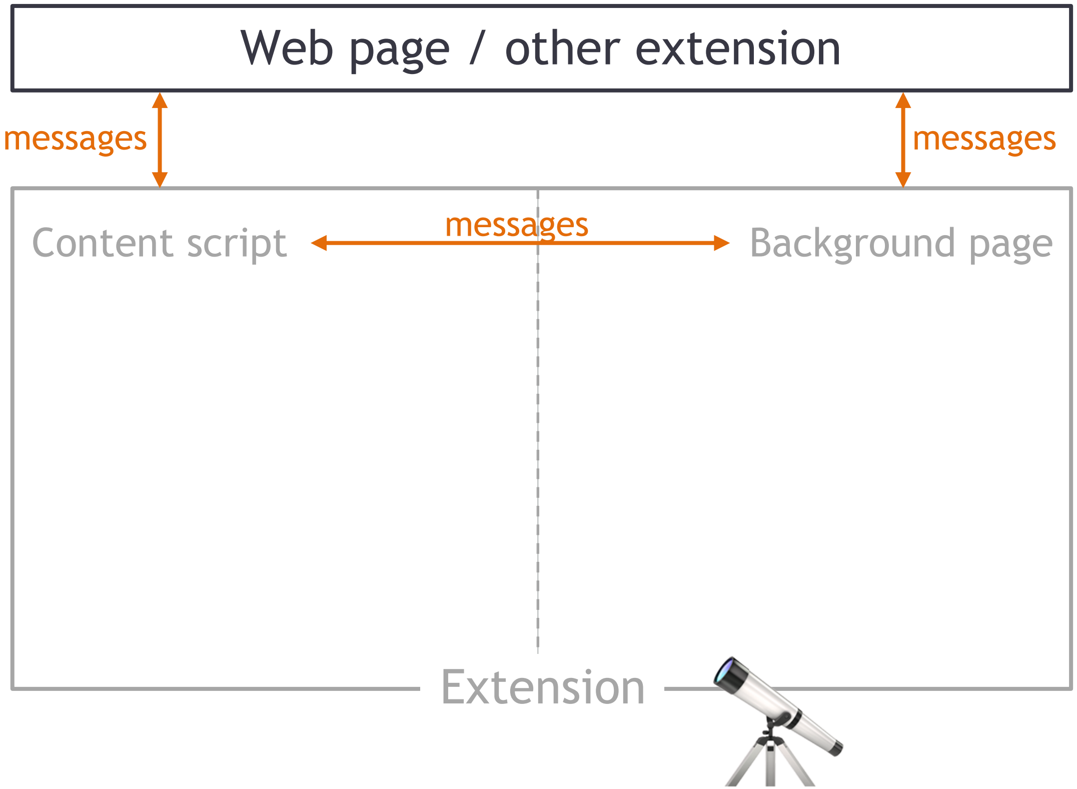
messages

Background page

Extension

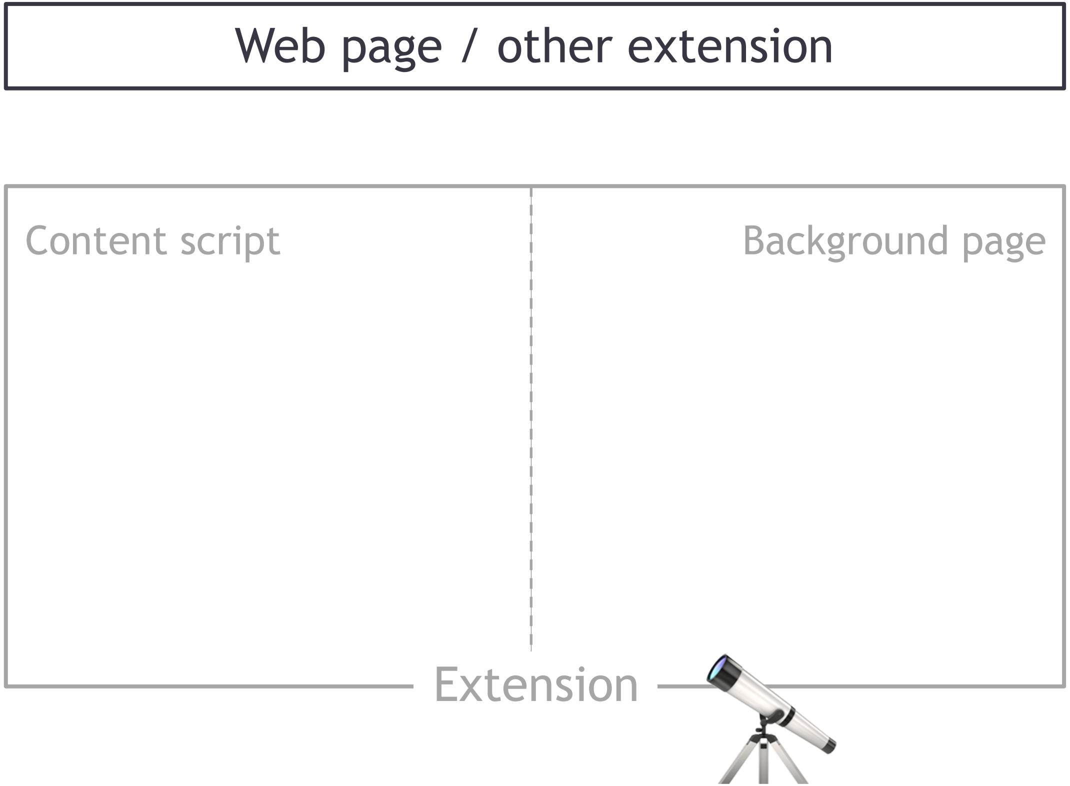
→ **DoubleX: detects suspicious data flows from and toward an extension privileged context**

Extension Architecture and Communication



→ DOUBLEX: detects suspicious data flows from and toward an extension privileged context

DoubleX: Suspicious Data Flow Detection



Web page / other extension

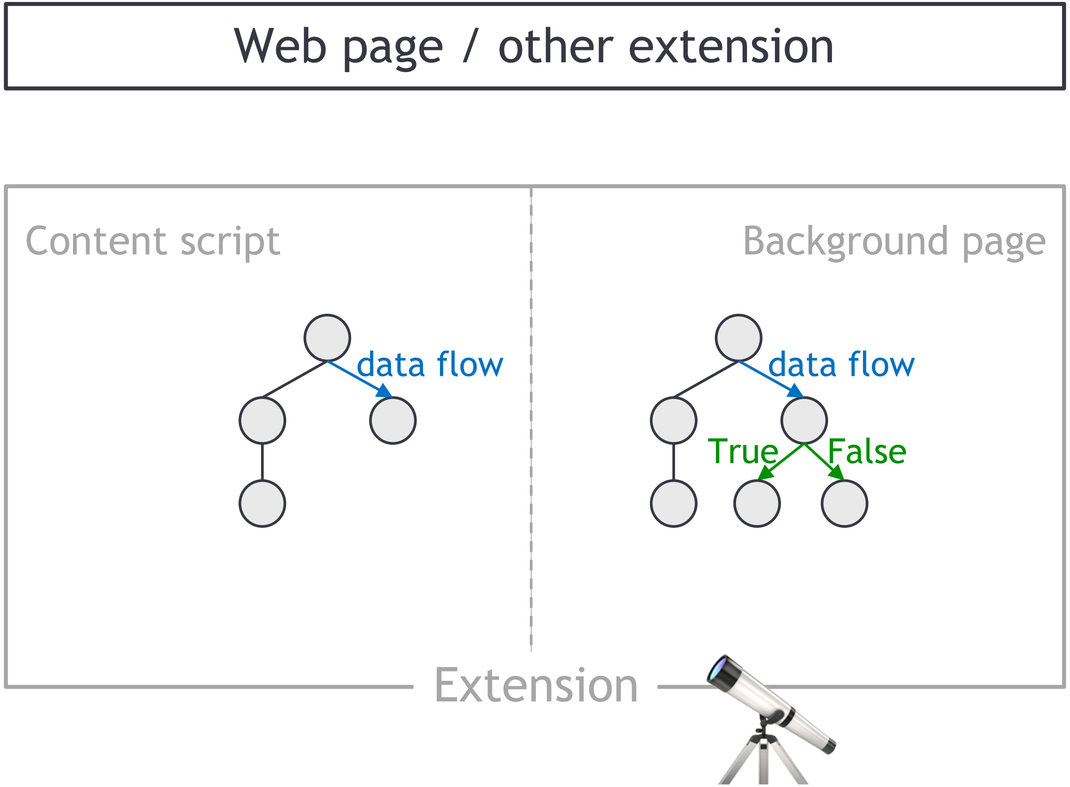
Content script

Background page

Extension

→ DoubleX: detects suspicious data flows from and toward an extension privileged context

DOUBLEX: Suspicious Data Flow Detection

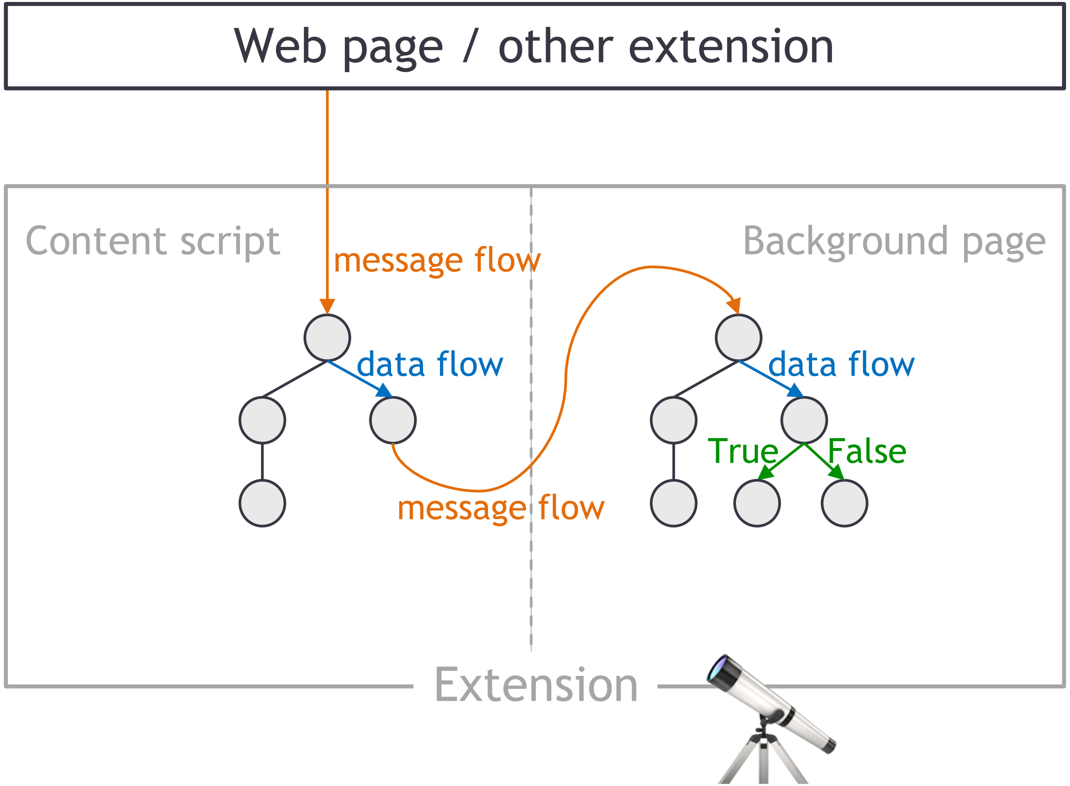


Per-component JS code abstraction

- AST
- Control flow
- Data flow
- Pointer analysis

→ DOUBLEX: detects suspicious data flows from and toward an extension privileged context

DOUBLEX: Suspicious Data Flow Detection



Per-component JS code abstraction

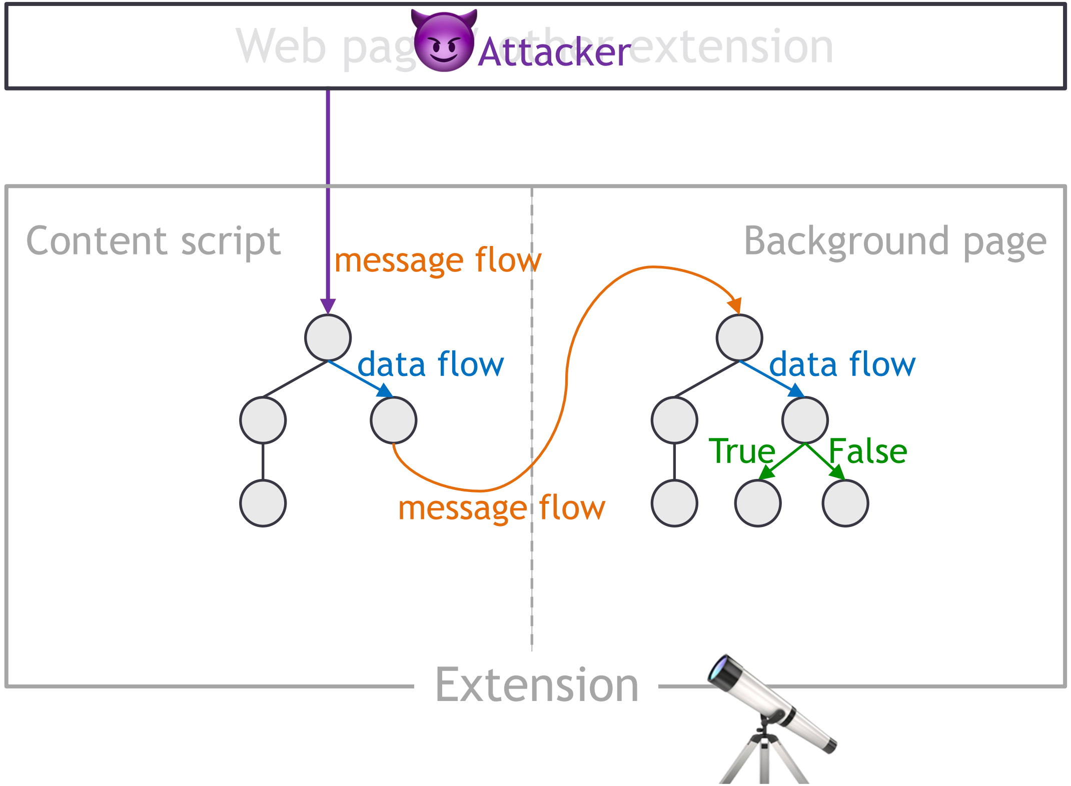
- AST
- Control flow
- Data flow
- Pointer analysis

Extension Dependence Graph (EDG)

➢ Message interactions

→ DOUBLEX: detects suspicious data flows from and toward an extension privileged context

DoubleX: Suspicious Data Flow Detection



Per-component JS code abstraction

- AST
- Control flow
- Data flow
- Pointer analysis

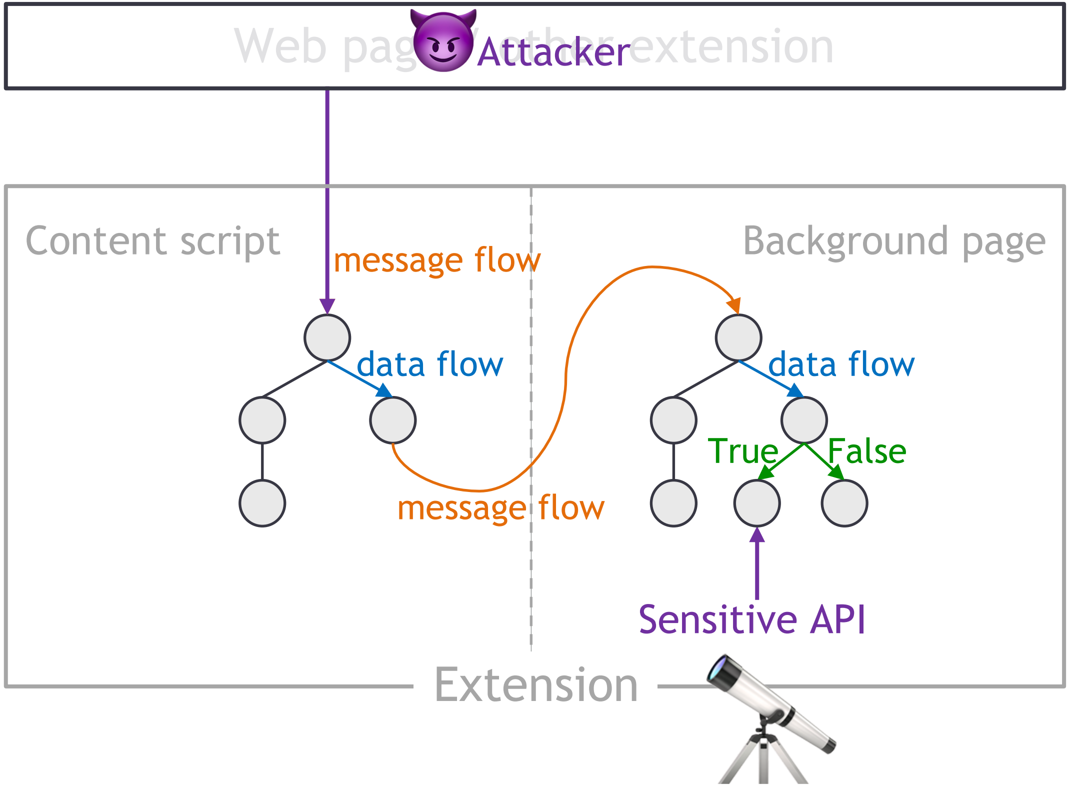
Extension Dependence Graph (EDG)

➢ Message interactions

Suspicious data flow tracking

→ DoubleX: detects suspicious data flows from and toward an extension privileged context

DOUBLEX: Suspicious Data Flow Detection



→ DOUBLEX: detects suspicious data flows from and toward an extension privileged context

Per-component JS code abstraction

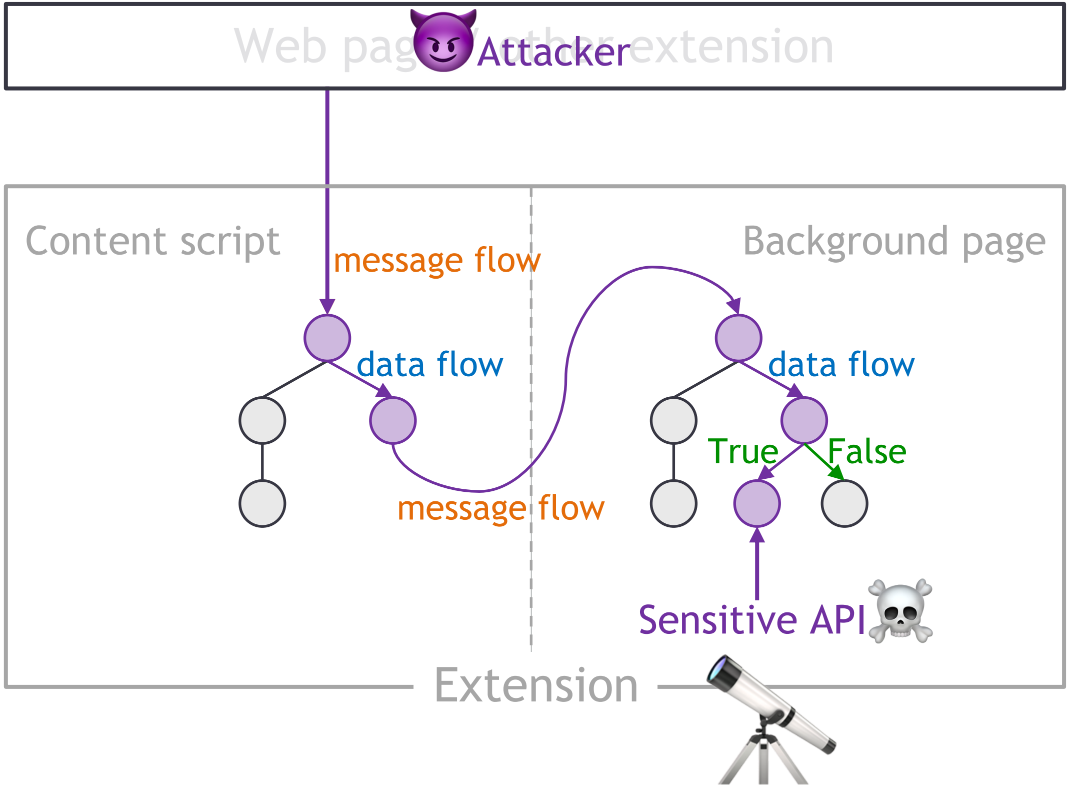
- AST
- Control flow
- Data flow
- Pointer analysis

Extension Dependence Graph (EDG)

➢ Message interactions

Suspicious data flow tracking

DOUBLEX: Suspicious Data Flow Detection



→ DOUBLEX: detects suspicious data flows from and toward an extension privileged context

Per-component JS code abstraction

- AST
- Control flow
- Data flow
- Pointer analysis

Extension Dependence Graph (EDG)

➢ Message interactions

Suspicious data flow tracking

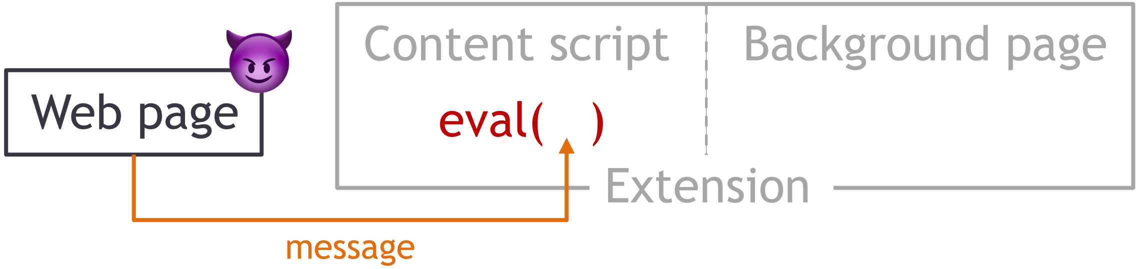
➢ Detects any path between an attacker & sensitive APIs

↓

Data flow report

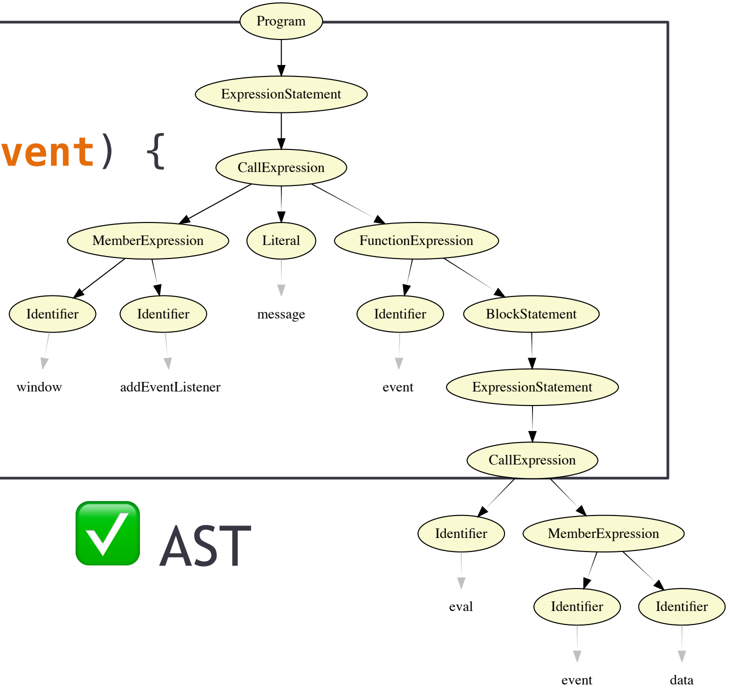
Per-Component JS Code Abstraction

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

    eval(event.data);

})
```



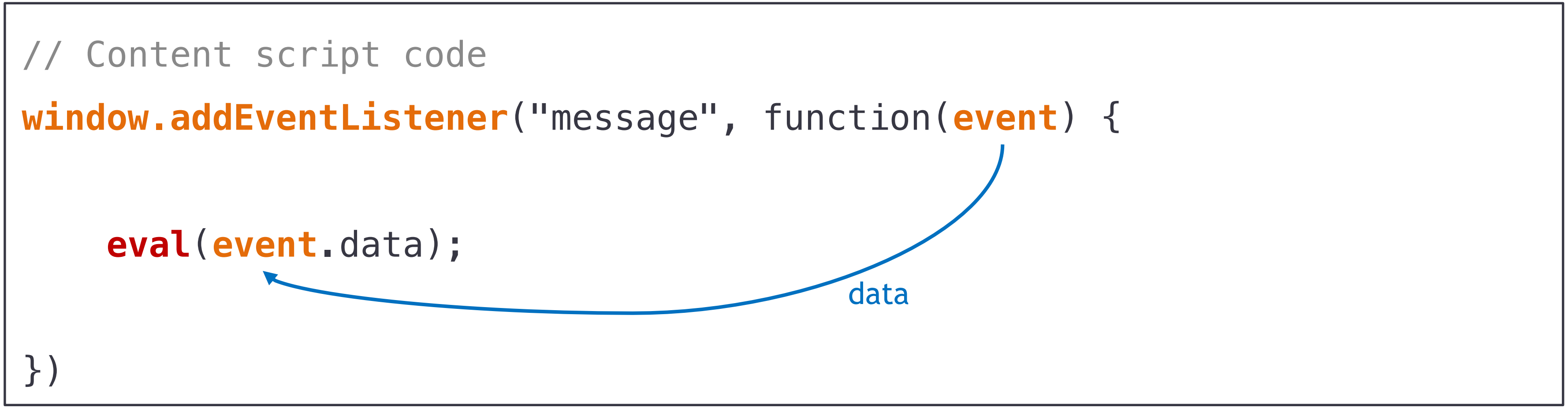
Per-Component JS Code Abstraction

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


    eval(event.data);


})
```



Abstract code representation → ✅ AST

Per-Component JS Code Abstraction

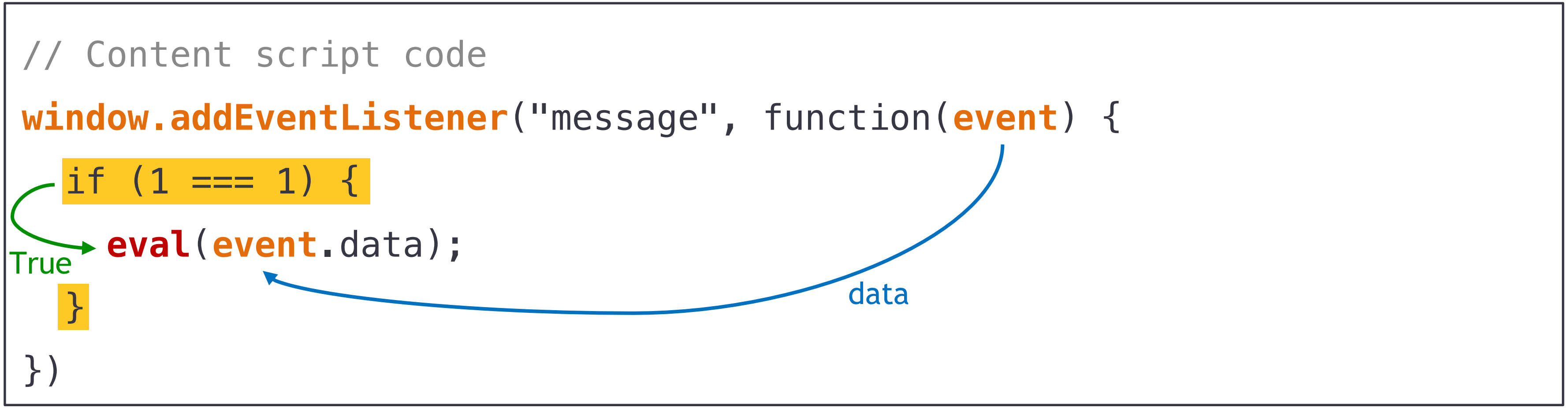


```
// Content script code
window.addEventListener("message", function(event) {

    eval(event.data);

})
```

Abstract code representation → ✅ AST

– variable dependencies → ✅ data flow

Per-Component JS Code Abstraction

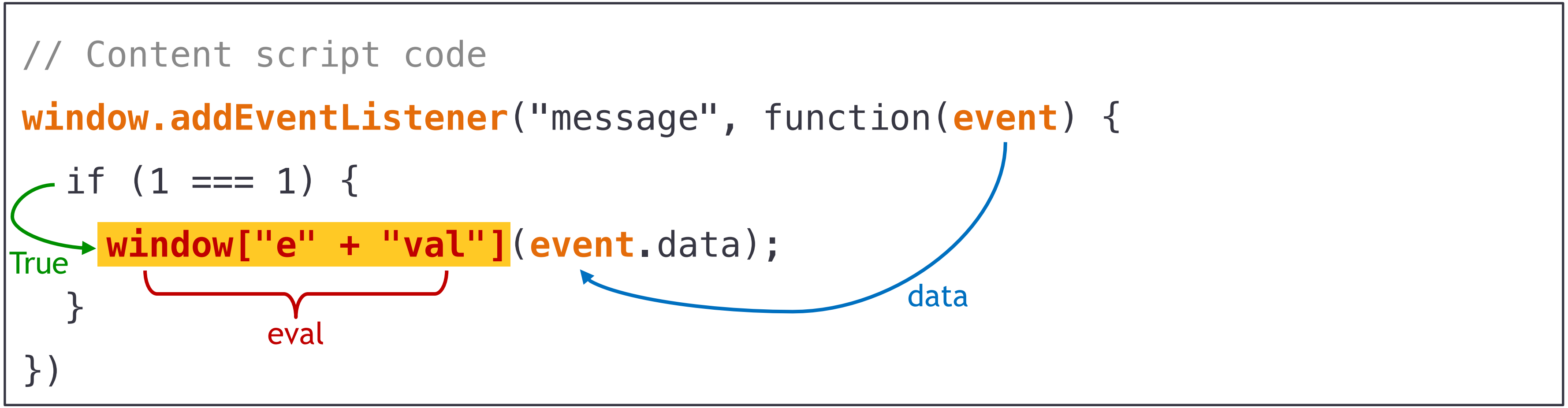


```
// Content script code
window.addEventListener("message", function(event) {
   if (1 === 1) {
     eval(event.data);
   }
})
```

Abstract code representation → ✓ AST

- conditions → ✓ control flow
- variable dependencies → ✓ data flow

Per-Component JS Code Abstraction



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

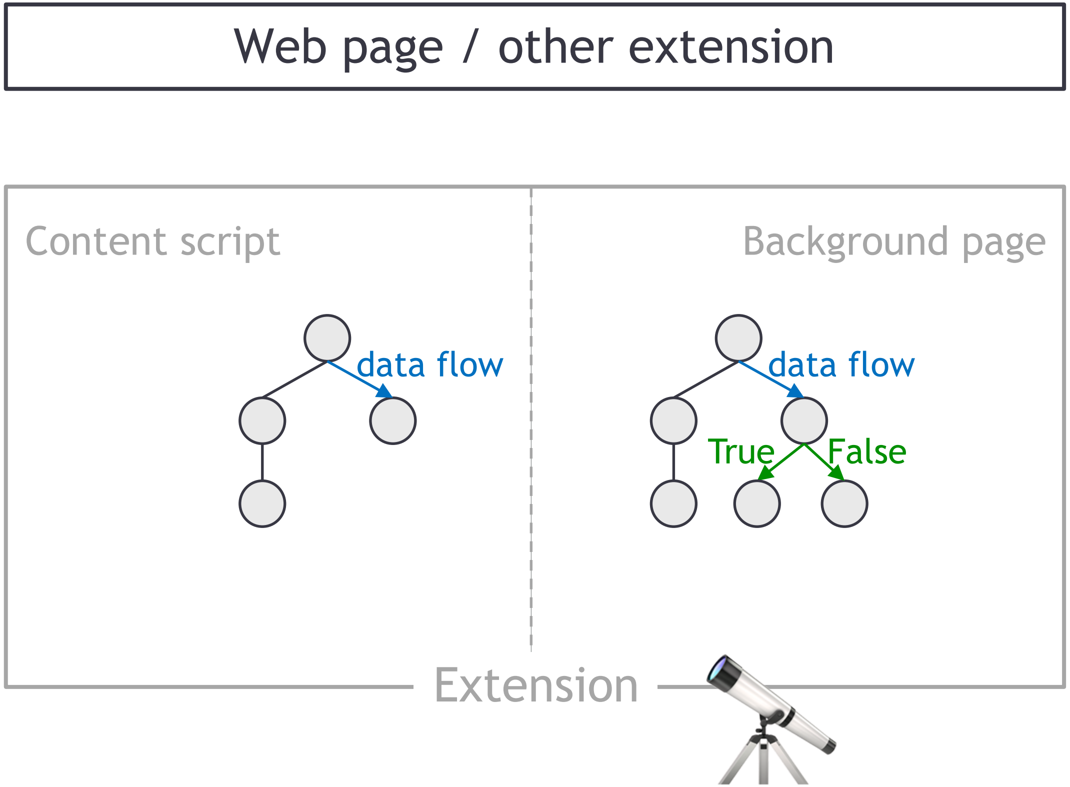
Abstract code representation → ✅ AST

– conditions → ✅ control flow

– variable dependencies → ✅ data flow

– variable values → ✅ pointer analysis

DoubleX: Suspicious Data Flow Detection



Per-component JS code abstraction

- AST
- Control flow
- Data flow
- Pointer analysis

Extension Dependence Graph (EDG)

➢ Message interactions

Suspicious data flow tracking

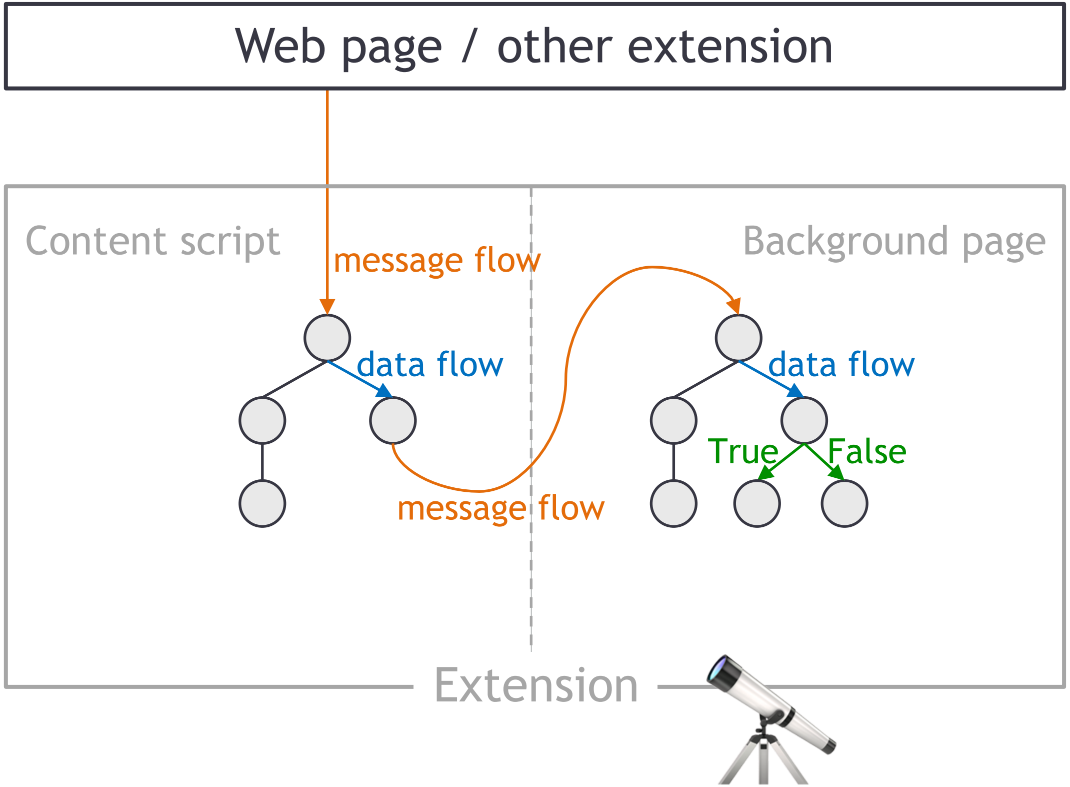
➢ Detects any path between an attacker & sensitive APIs

↓

Data flow report

→ **DoubleX: detects suspicious data flows from and toward an extension privileged context**

DoubleX: Suspicious Data Flow Detection



Web page / other extension

Content script

Background page

message flow

data flow

message flow

data flow

True

False

Extension

Per-component JS code abstraction

- AST
- Control flow
- Data flow
- Pointer analysis

Extension Dependence Graph (EDG)

➢ Message interactions

Suspicious data flow tracking

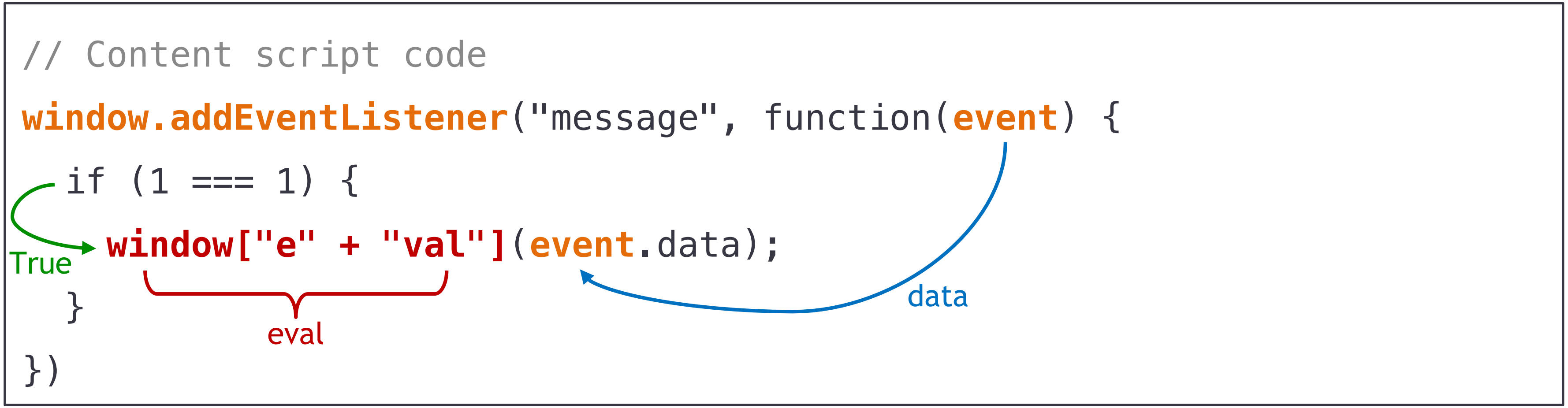
➢ Detects any path between an attacker & sensitive APIs

↓

Data flow report

→ DoubleX: detects suspicious data flows from and toward an extension privileged context

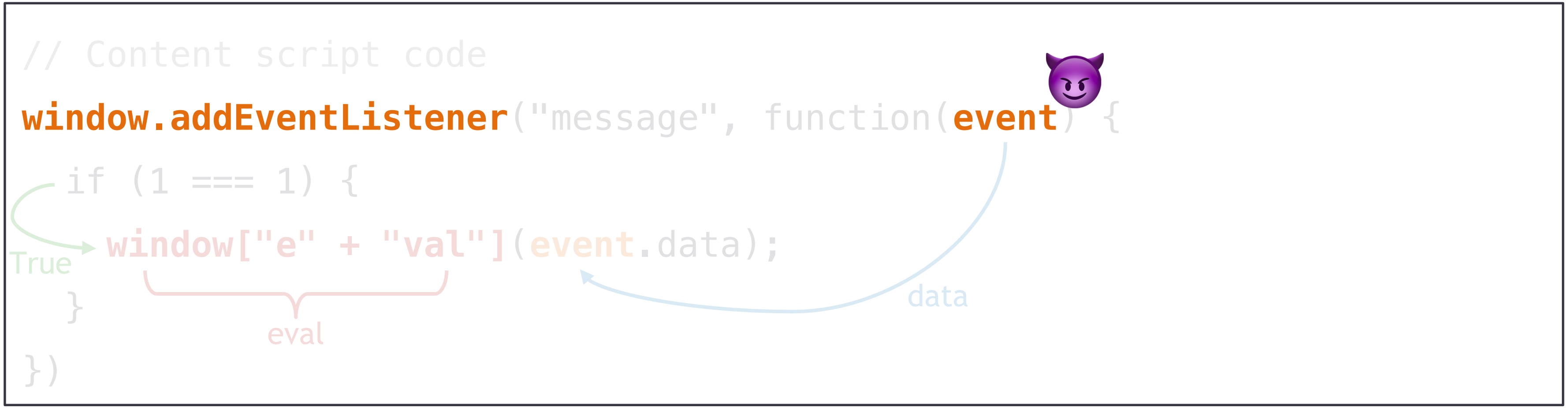
Extension Dependence Graph



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

- external messages
- internal messages

Extension Dependence Graph



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

- external messages ✅
- internal messages

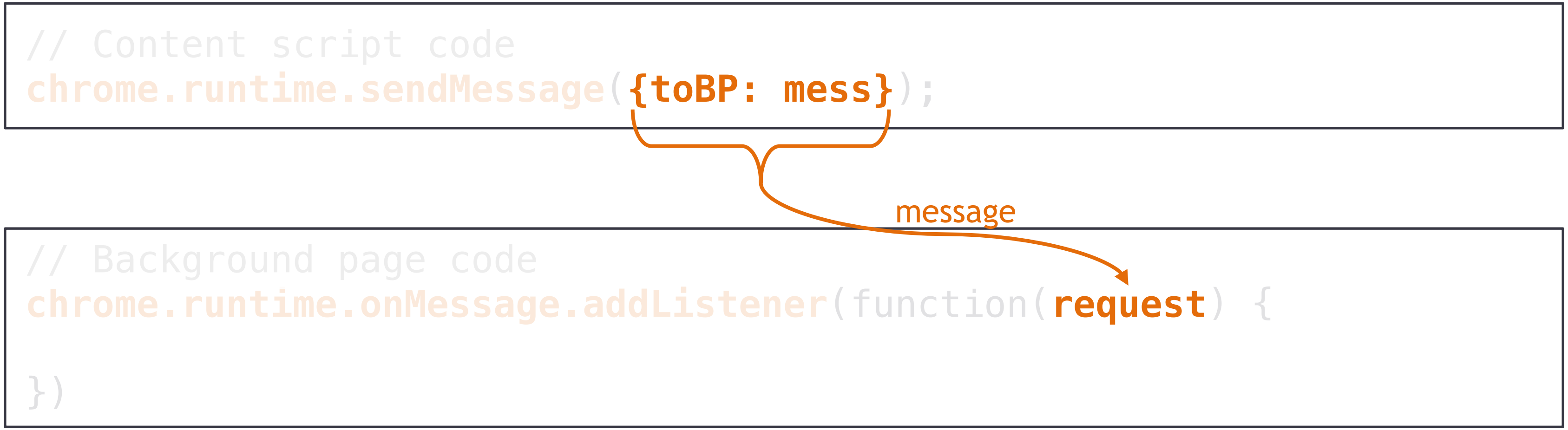
Extension Dependence Graph

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

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

})
```

- external messages ✅
- internal messages

Extension Dependence Graph

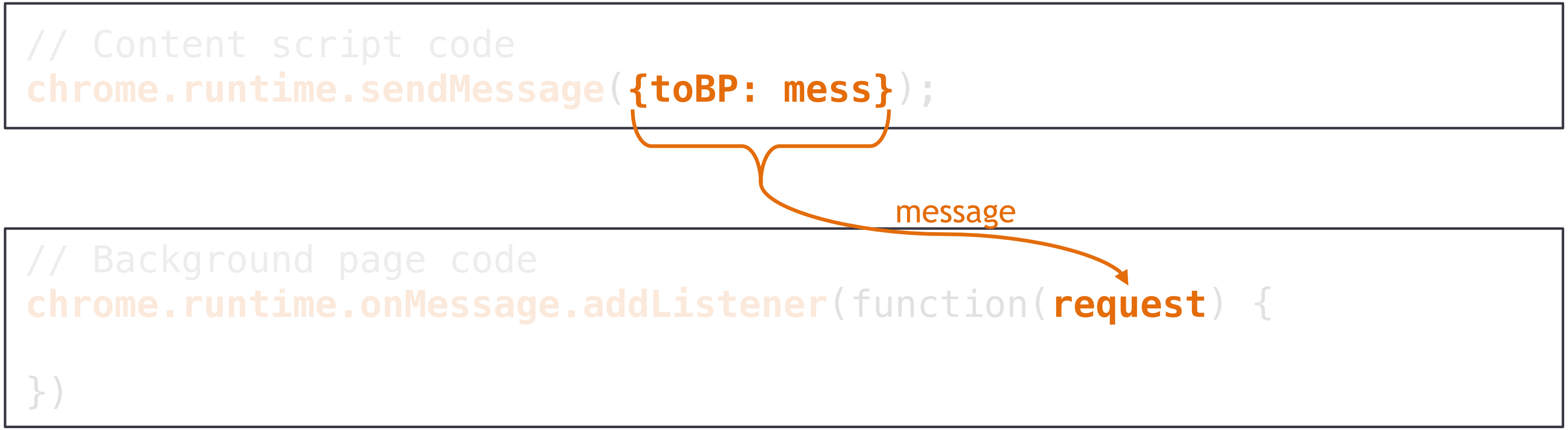


```
// Content script code
chrome.runtime.sendMessage({toBP: mess});
```

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

})
```

- external messages ✓
- internal messages ✓

Extension Dependence Graph



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

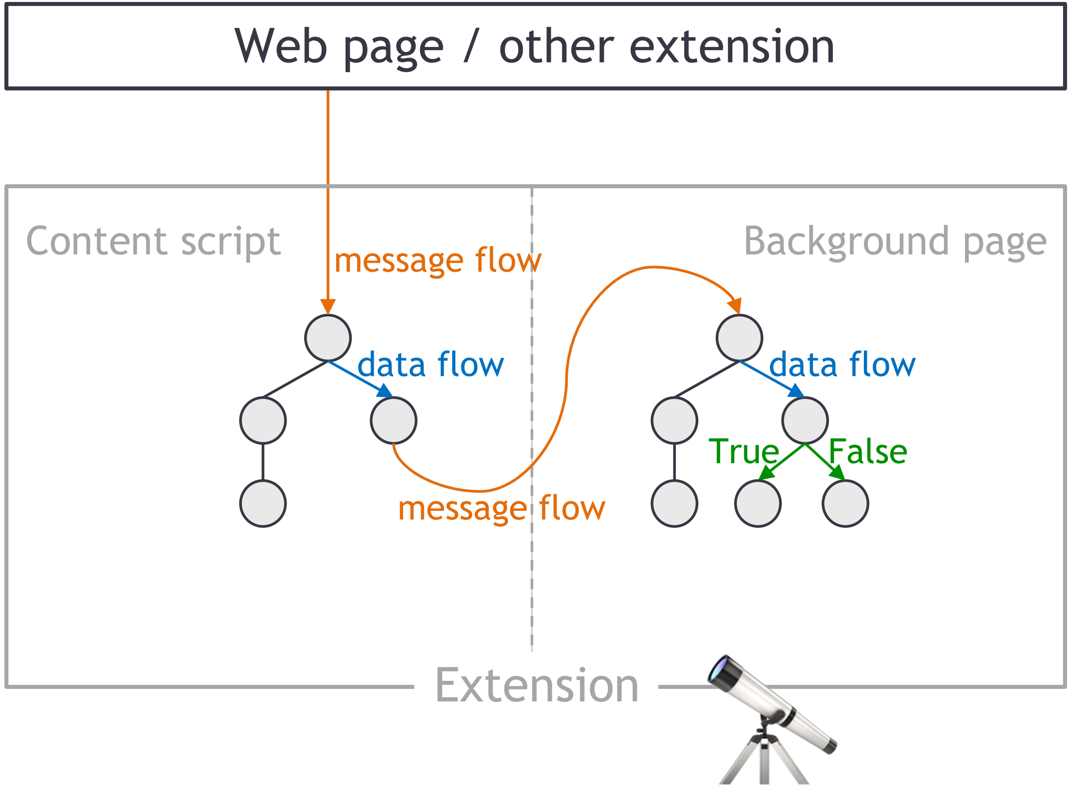
```
// Background page code
chrome.runtime.onMessage.addListener(function(request) {

})
```

– external messages ✅

– internal messages ✅

➢ Models message interaction within and outside of an extension

DoubleX: Suspicious Data Flow Detection



→ DoubleX: detects suspicious data flows from and toward an extension privileged context

Per-component JS code abstraction

- AST
- Control flow
- Data flow
- Pointer analysis

Extension Dependence Graph (EDG)

➢ Message interactions

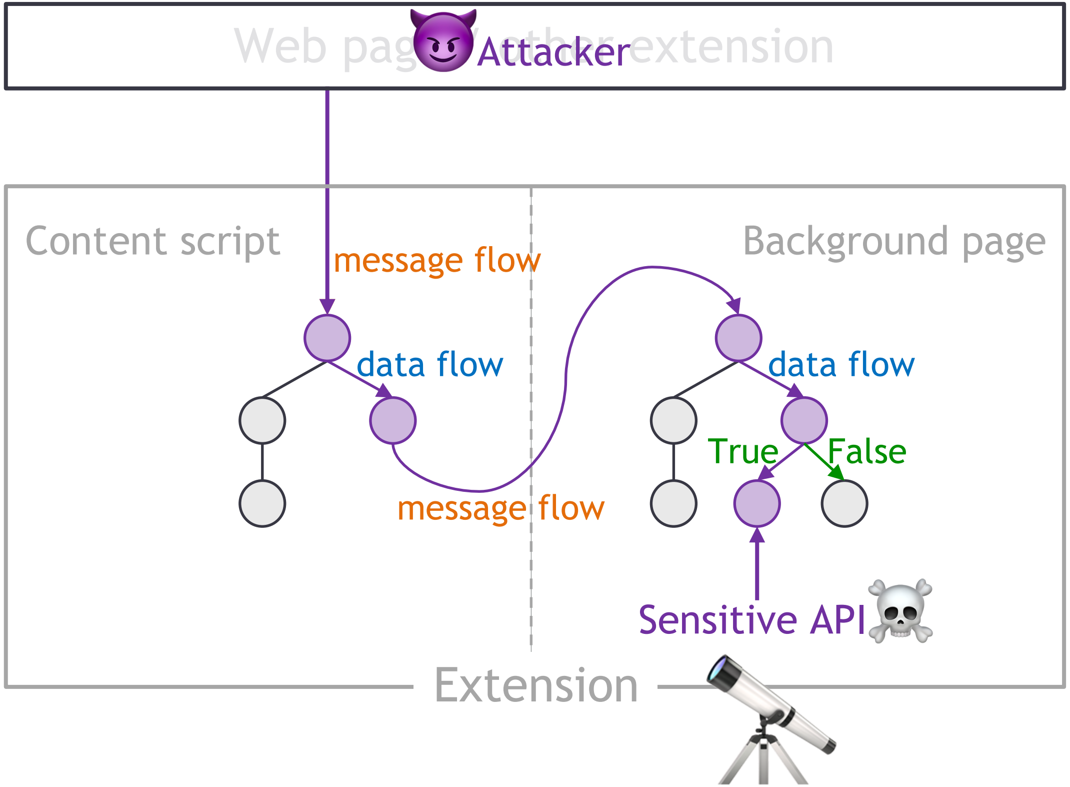
Suspicious data flow tracking

➢ Detects any path between an attacker & sensitive APIs

↓

Data flow report

DoubleX: Suspicious Data Flow Detection



→ DoubleX: detects suspicious data flows from and toward an extension privileged context

Per-component JS code abstraction

- AST
- Control flow
- Data flow
- Pointer analysis

Extension Dependence Graph (EDG)

➢ Message interactions

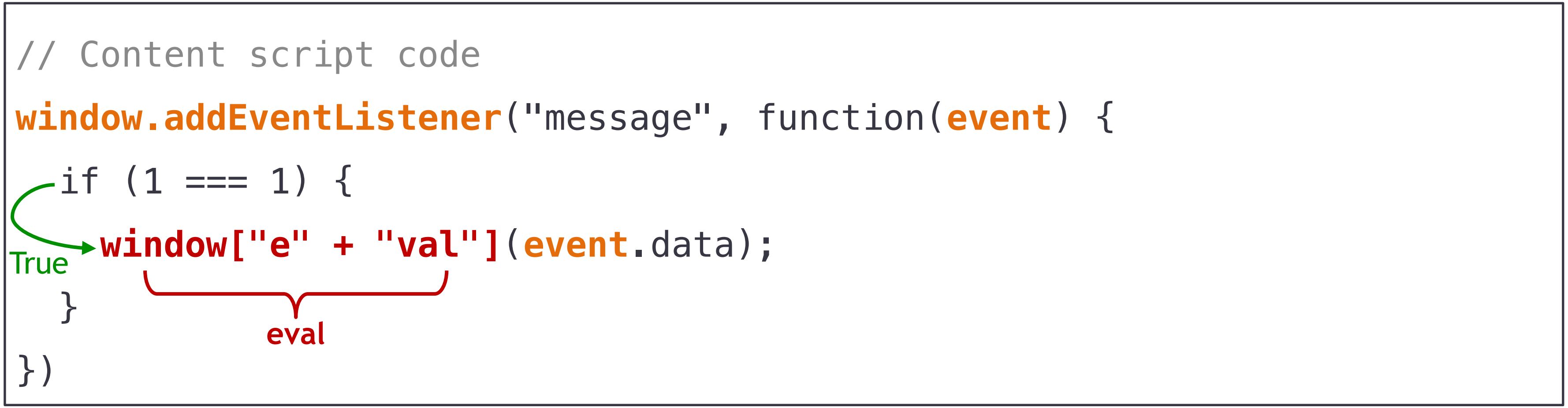
Suspicious data flow tracking

➢ Detects any path between an attacker & sensitive APIs

↓

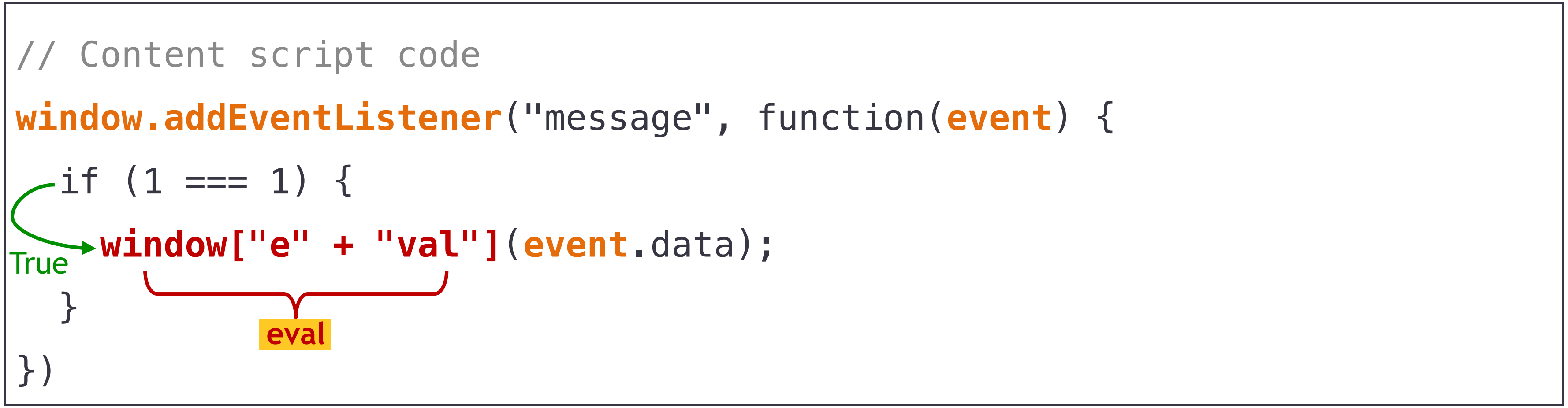
Data flow report

Suspicious Data Flow Tracking



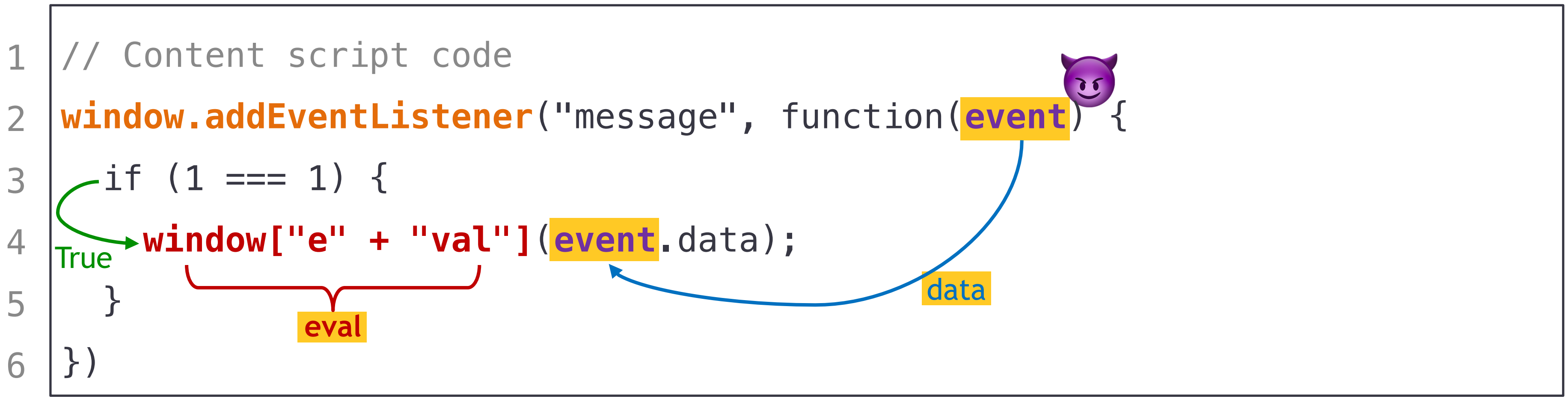
```
// Content script code
window.addEventListener("message", function(event) {
  if (1 === 1) {
   window["e" + "val"](event.data);
  }
})
```

Suspicious Data Flow Tracking



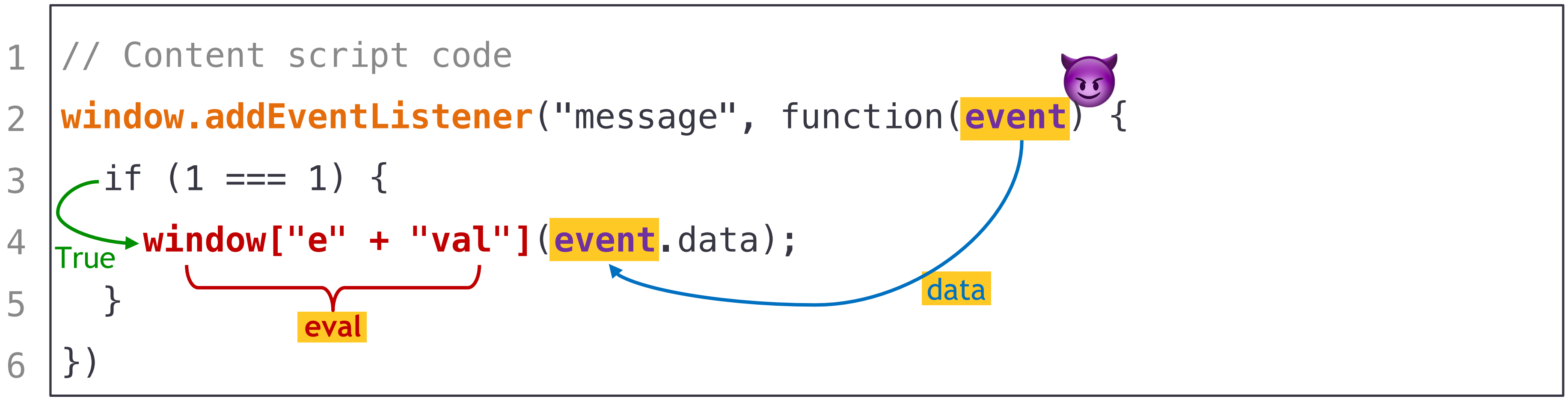
```
// Content script code
window.addEventListener("message", function(event) {
  if (1 === 1) {
    window["e" + "val"](event.data);
  }
})
```

Suspicious Data Flow Tracking

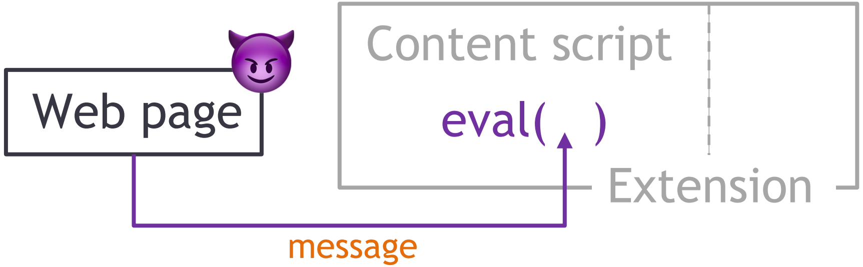


```
// Content script code
window.addEventListener("message", function(event) {
   if (1 === 1) {
     window["e" + "val"](event.data);
   }
})
```

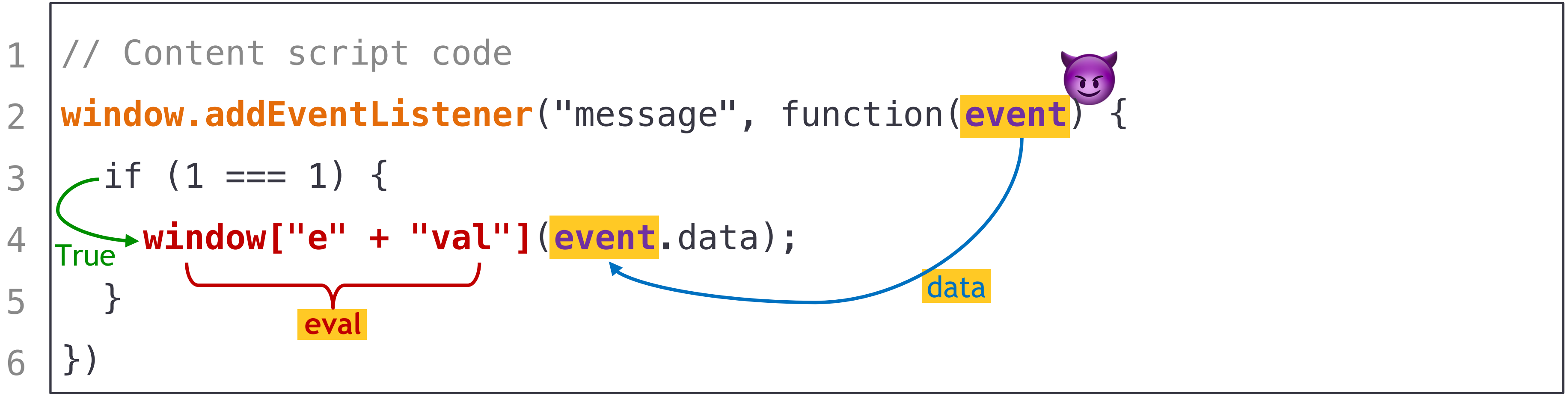
Suspicious Data Flow Tracking



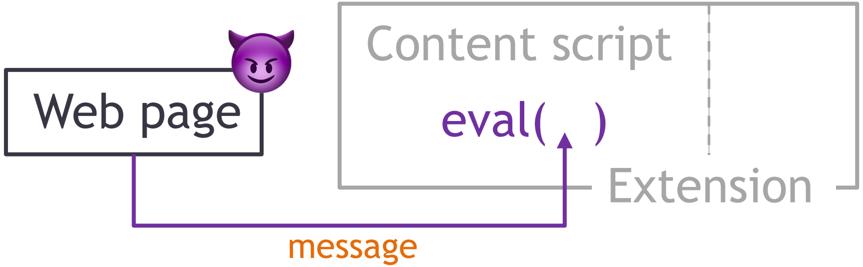
```
// Content script code
window.addEventListener("message", function(event) {
  if (1 === 1) {
    window["e" + "val"](event.data);
  }
})
```



Suspicious Data Flow Tracking



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

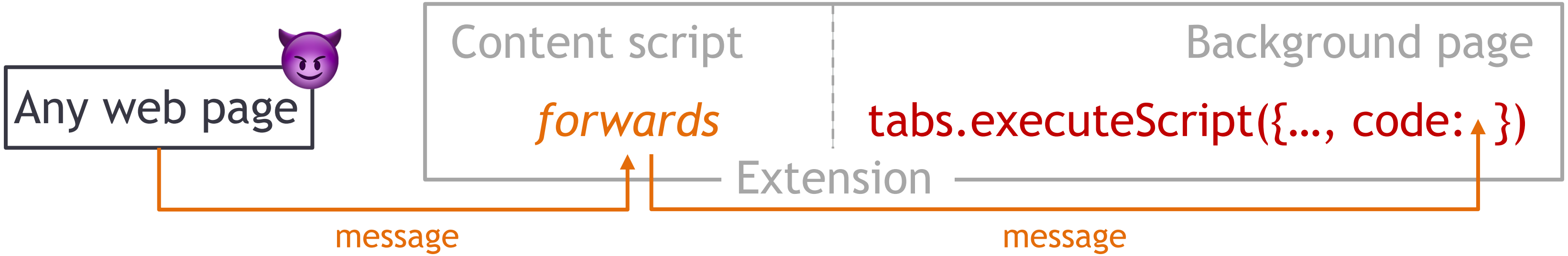


```
// Data flow report
{"direct-danger1": "eval",
"value": "eval(event.data)",
"line": "4 - 4",
"dataflow": true,
"param1": {
  "received": "event",
  "line": "2 - 2"}}
```

Case Studies of Vulnerable Chrome Extensions

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

- Arbitrary code execution (*cdi…*, 4k+ users)



Any web page 😈

Content script

forwards

Background page

tabs.executeScript({…, code: })

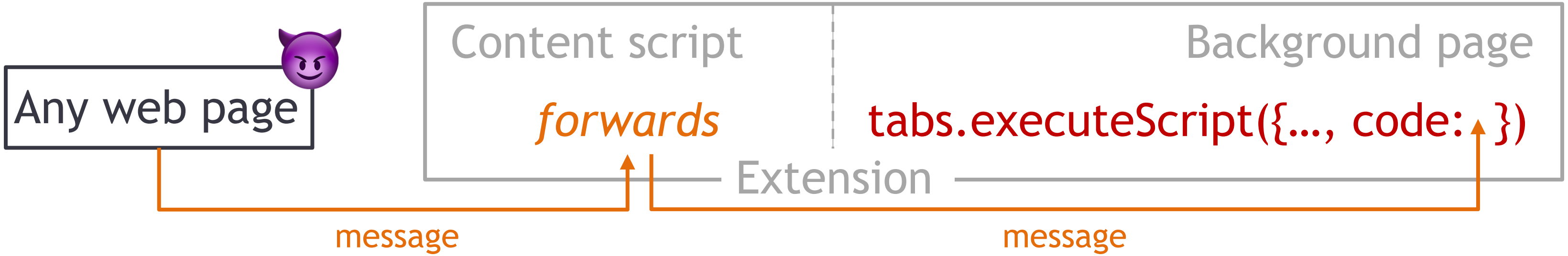
Extension

message

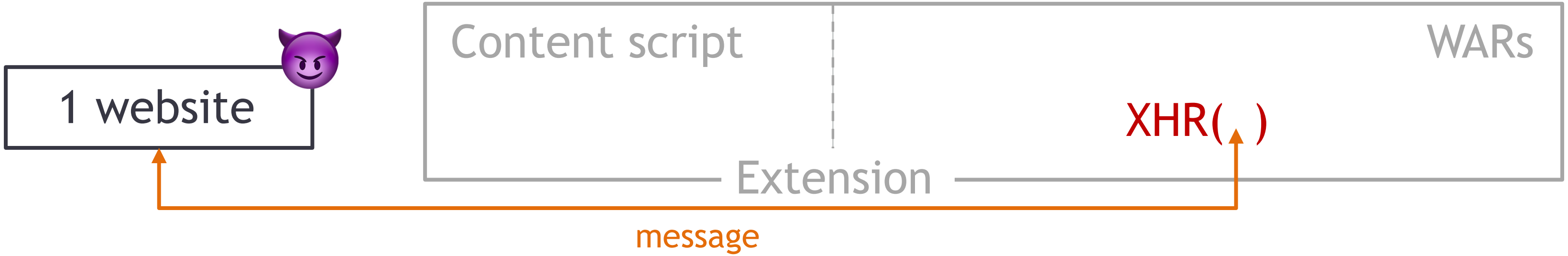
message

Case Studies of Vulnerable Chrome Extensions

- Arbitrary code execution (*cdi*…, 4k+ users)



- Cross-origin requests (*koh*…, 200k+ users)



Large-Scale Analysis of Chrome Extensions

- Analyzed 155k Chrome extensions from 2021 with DOUBLEX
  - 278 suspicious extensions reported (309 suspicious data flows)

    → **Precision: 89%** (manually) verified dangerous data flows (275 / 309)

Attacker capabilities	#Reports	#Verified data flow	#Exploitable
Code Execution	113	102	63
Triggering Downloads	21	21	21
Cross-Origin Requests	95	75	49
Data Exfiltration	80	77	76
Sum	309	275	209

Large-Scale Analysis of Chrome Extensions

- Analyzed 155k Chrome extensions from 2021 with DOUBLEX
  - 278 suspicious extensions reported (309 suspicious data flows)
    - → **Precision: 89%** (manually) verified dangerous data flows (275 / 309)

  → **184 confirmed vulnerable extensions**
    - 2.4 – 2.9 million users impacted
    - 36% can be exploited by *any* websites or extensions

- Analyzed known vulnerable extensions with DOUBLEX [5]
  - → **Recall: 93%** of known vulnerabilities are detected (151 / 163)

[5] Somé, IEEE S&P 2019

Life Cycle of Vulnerable Chrome Extensions

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

Life Cycle of Vulnerable Chrome Extensions

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

- Comparison of vulnerable extensions in 2020 vs. 2021
  - not in the Store anymore: 30 / 193
  - vulnerability fixed: 3 / 193
  - turned vulnerable: 5 / 184
  - new vulnerable: 19 / 184
  - ➢ **still vulnerable: 160 (87%!)**

Life Cycle of Vulnerable Chrome Extensions

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

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

➢ **still vulnerable: 160 (87%!)** ➢ **Need to prevent vulnerable extensions from entering the Store → DOUBLEX**

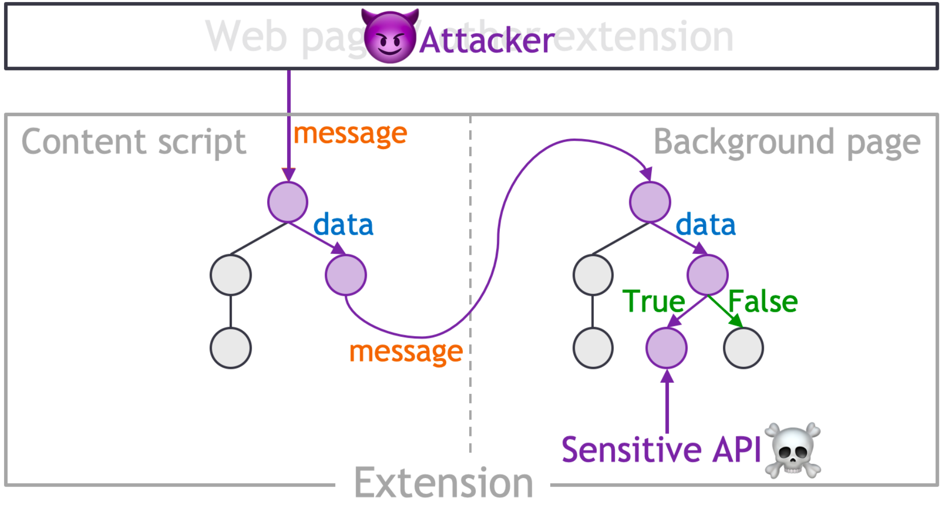
Takeaway

unintentionally

Extensions are popular… but may introduce security & privacy threats

→ Because **highly privileged**

→ Due to their **communication with websites** / other extensions



DoubleX: detects suspicious data flows in extensions

- 184 vulnerable extensions (87% already vulnerable the year before)
- **Precision: 89%**
- **Recall: 93%**

Aurore54F/DoubleX

@AuroreFass

Fork 9 ▾ ☆ Star 47 ▾