

# **AN EVALUATION OF THE GOOGLE CHROME EXTENSION SECURITY ARCHITECTURE**

Nicholas Carlini, Adrienne Porter Felt, David Wagner  
University of California, Berkeley

← → ↻ [www.bellevue.hyatt.com/hyatt/hotels-bellevue/index.jsp?null](http://www.bellevue.hyatt.com/hyatt/hotels-bellevue/index.jsp?null) ☆

Customer Service VISIT HYATT.COM

**HYATT®**

Hyatt Regency  
Bellevue  
On Seattle's Eastside

ROOMS & RATES  
SPECIAL OFFERS  
DINING & ENTERTAINMENT  
ACTIVITIES  
GUEST SERVICES  
MEETINGS & EVENTS

Hyatt Home > Hotels & Resorts > Hyatt Regency Bellevue Hotel on Seattle's Eastside

**Find Rooms & Rates**

CHECK-IN DATE  
mm/dd/yyyy

CHECK-OUT DATE  
mm/dd/yyyy

ROOMS ADULTS CHILDREN  
1 1 0

RATE TYPE  
Best Available Rate

**Hyatt Regency Bellevue on Seattle's Eastside**  
900 Bellevue Way NE,  
Bellevue, Washington, USA 98004-4272  
Tel: +1 425 462 1234 Fax: +1 425 646 7567  
Email: [salesbelle@hyatt.com](mailto:salesbelle@hyatt.com)  
[Maps & Directions](#)

**Hotel Overview**  
Step into the sophisticated and feel an air of elegant tr...  
luxurious fabrics and a war...  
experience. Boasting a pre...

**Call +1 425 462 1234**

Phone to call with  
Google Talk  
Connect

**Google voice** (510) 394-5151

Call Text Inbox

+18048540981  
2 months ago  
+18048540981: Goi Vietnam Tu Do! khong tinh phut!  
Khong gioi han - \$20/Thang Am Thanh #1, Uy Tin! -  
hay goi 1-888-552-1586: re: STOP 2optout  
[Call](#) [Text](#) [Archive](#) [Delete](#)

+12535203127  
12 months ago  
Unable to transcribe this message.  
01:18  
[Call](#) [Text](#) [Archive](#) [Delete](#)

**Google Voice**  
3 years ago  
Welcome to Google Voice! Google Voice gives you a single phone number that rings all your phones, saves your voicemail online, and transcribes your voicemail to text. Other cool features include the ability to listen in on messages while they are being left and the ability to make low cost international calls. To start enjoying Google Voice, just give out your Google Voice number. You can record custom greetings for your favorite callers or block annoying callers by marking them as SPAM. Just click on the settings link at the top of your inbox. We hope you enjoy Google Voice.  
00:28  
[Close](#) | [Options](#) | [Go to inbox »](#)

# CHROME EXTENSIONS

www.bellevue.hyatt.com/hyatt/hotels-bellevue/index.jsp?null

Customer Service VISIT HYATT.CO

HYATT®

Hyatt Regency Bellevue  
On Seattle's Eastside

ROOMS & RATES  
SPECIAL OFFERS  
DINING & ENTERTAINMENT  
ACTIVITIES  
GUEST SERVICES  
MEETINGS & EVENTS

Hyatt Home > Hotels & Resorts > Hyatt Regency Bellevue Hotel on Seattle's Eastside

Find Rooms & Rates

CHECK-IN DATE  
mm/dd/yyyy

CHECK-OUT DATE  
mm/dd/yyyy

ROOMS ADULTS CHILDREN  
1 1 0

RATE TYPE  
Best Available Rate

Hyatt Regency Bellevue on Seattle's Eastside  
900 Bellevue Way NE,  
Bellevue, Washington, USA 98004-4272  
Tel: +1 425 462 1234 Fax: +1 425 646 7567  
Email: [salesbelle@hyatt.com](mailto:salesbelle@hyatt.com)  
[Maps & Directions](#)

Hotel Overview  
Step into the sophisticated  
and feel an air of elegant  
luxurious fabrics and a w  
experience. Boasting a p

Call +1 425 462 1234

Phone to call with  
Google Talk  
Connect

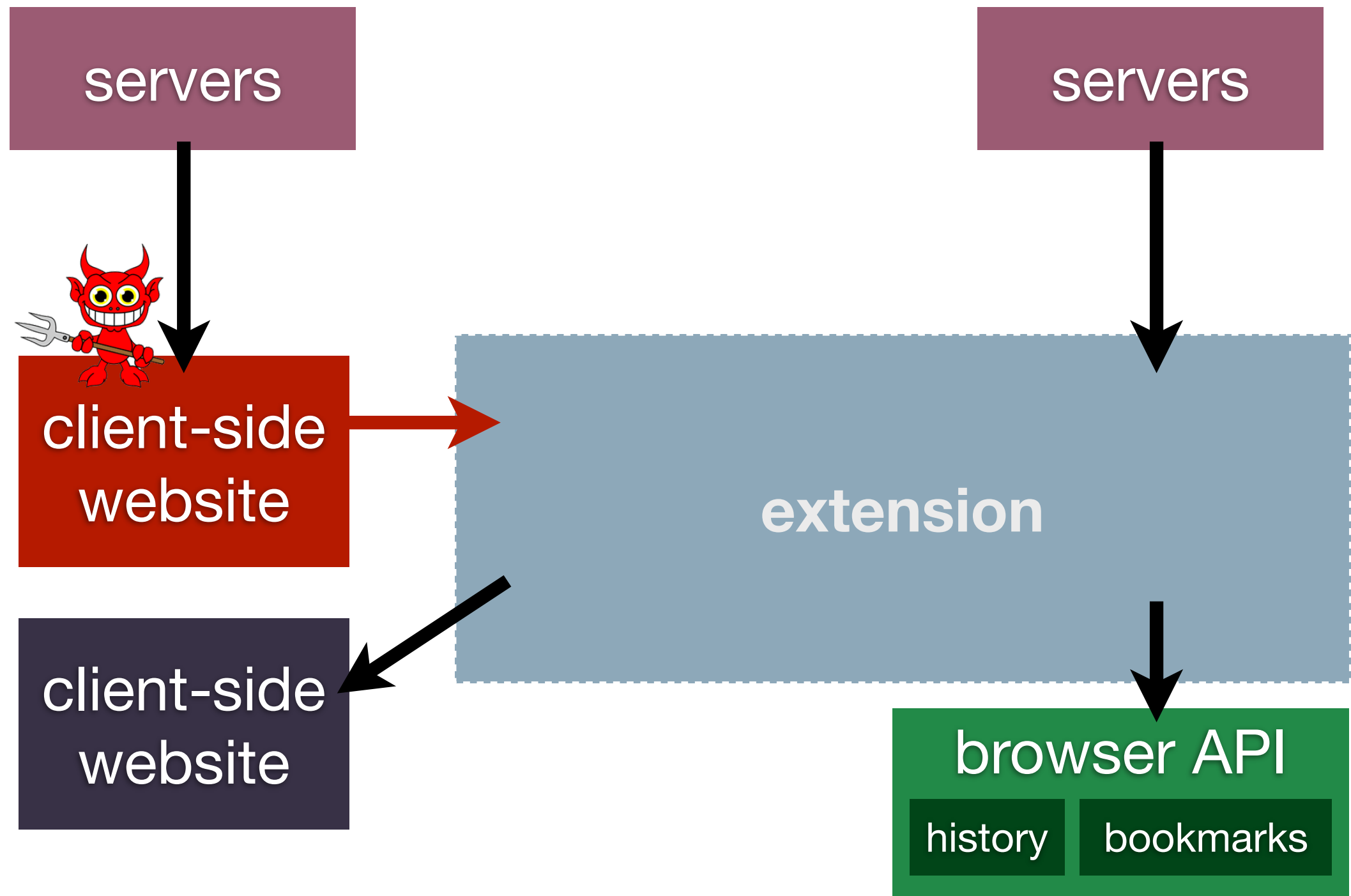
Google voice  
Call Text Inbox  
(510) 394-5151

+18048540981  
2 months ago  
+18048540981: Goi Vietnam Tu Do! khong tinh phut!  
Khong gioi han - \$20/Thang Am Thanh #1, Uy Tin! -  
hay goi 1-888-552-1586: re: STOP 2optout  
[Call](#) [Text](#) [Archive](#) [Delete](#)

+12535203127  
12 months ago  
Unable to transcribe this message.  
01:18  
[Call](#) [Text](#) [Archive](#) [Delete](#)

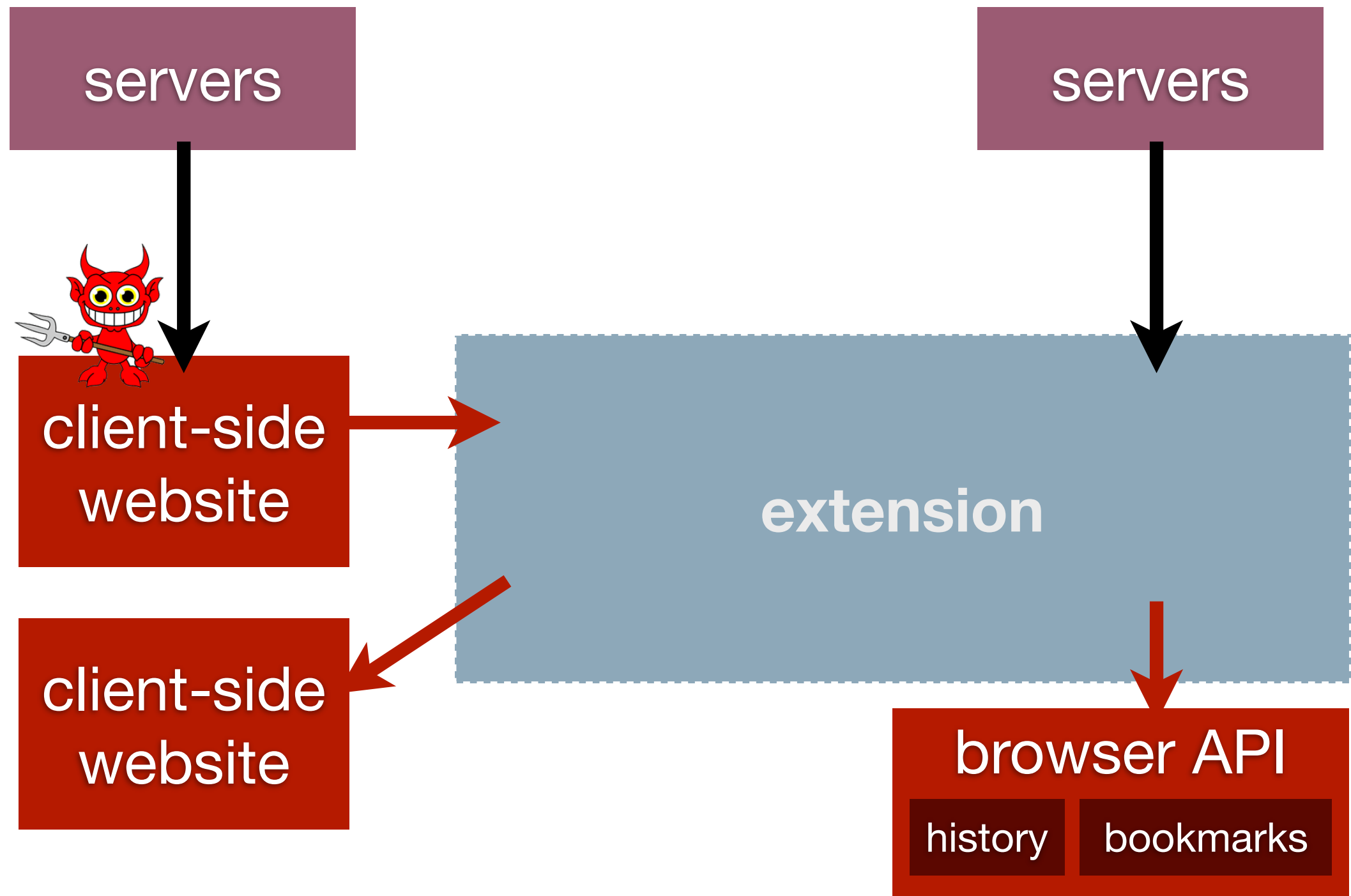
Google Voice  
3 years ago  
Welcome to Google Voice! Google Voice  
gives you a single phone number that rings  
all your phones, saves your voicemail online,  
and transcribes your voicemail to text. Other  
cool features include the ability to listen in on  
messages while they are being left and the  
ability to make low cost international calls.  
To start enjoying Google Voice, just give out  
your Google Voice number. You can record  
custom greetings for your favorite callers or  
block annoying callers by marking them as  
SPAM. Just click on the settings link at the  
top of your inbox. We hope you enjoy Google  
Voice.  
00:28  
[Close](#) | [Options](#) | [Go to inbox »](#)

# CHROME EXTENSIONS

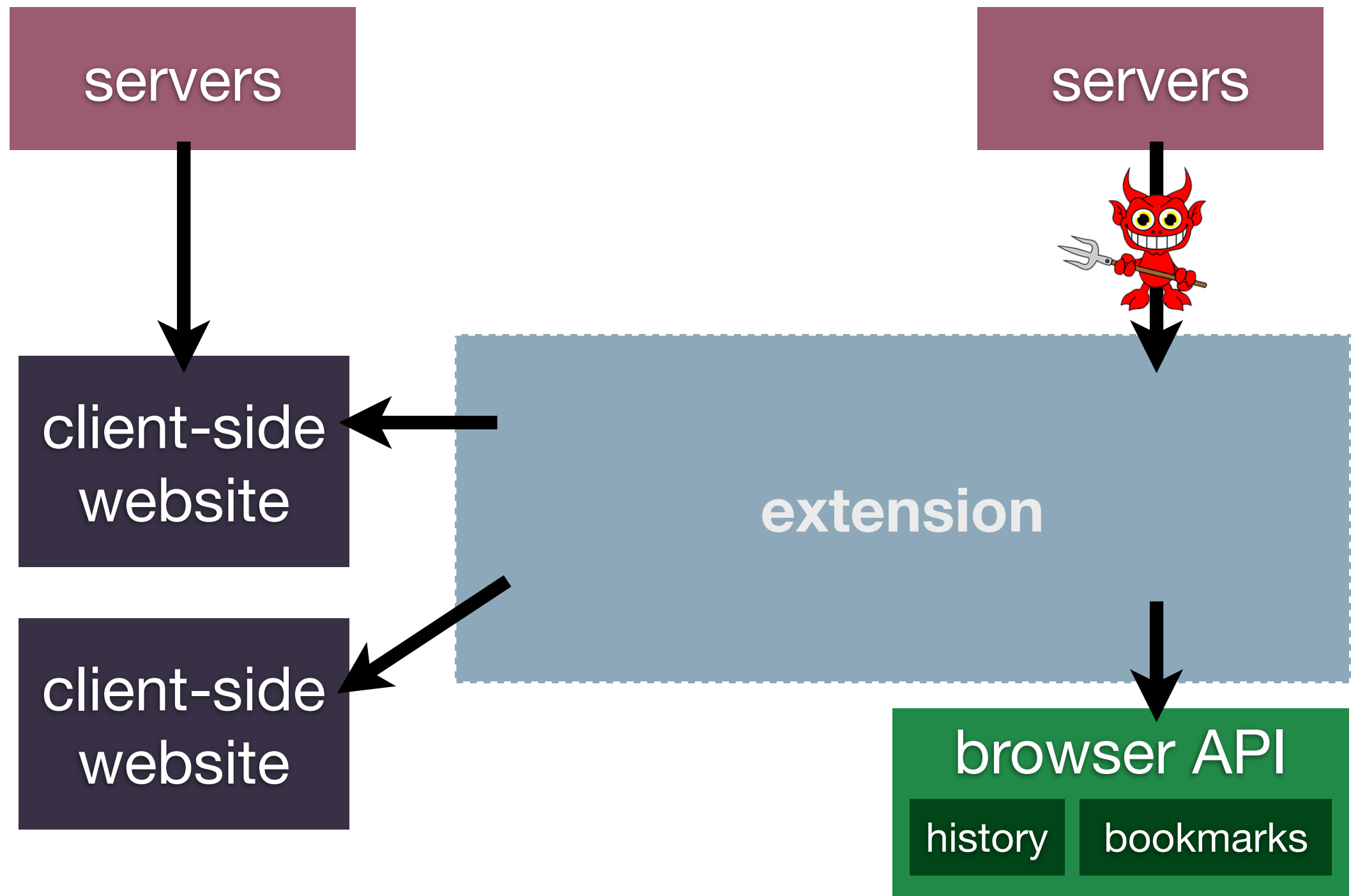


**WEB ATTACKER**

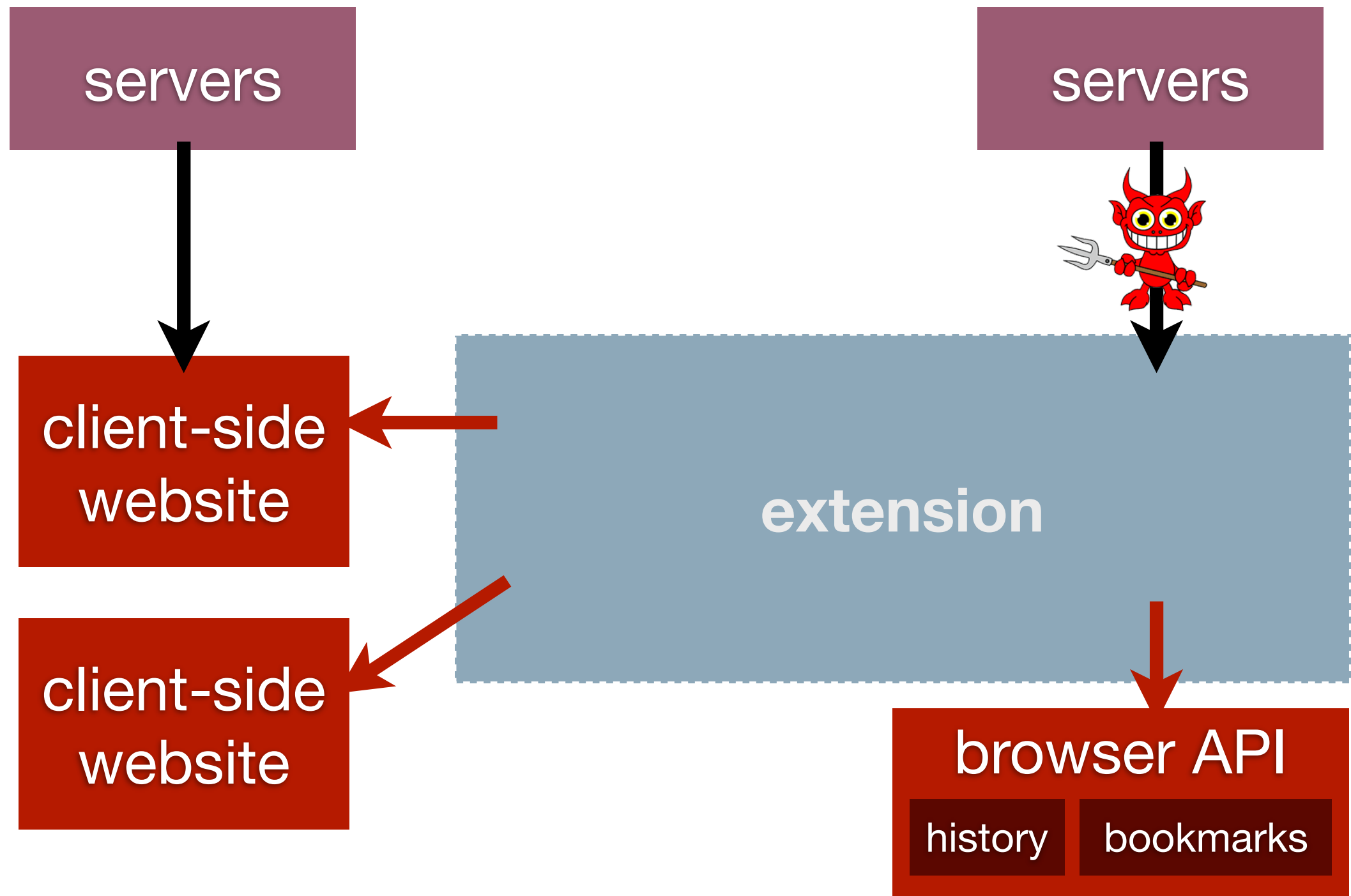




# WEB ATTACKER



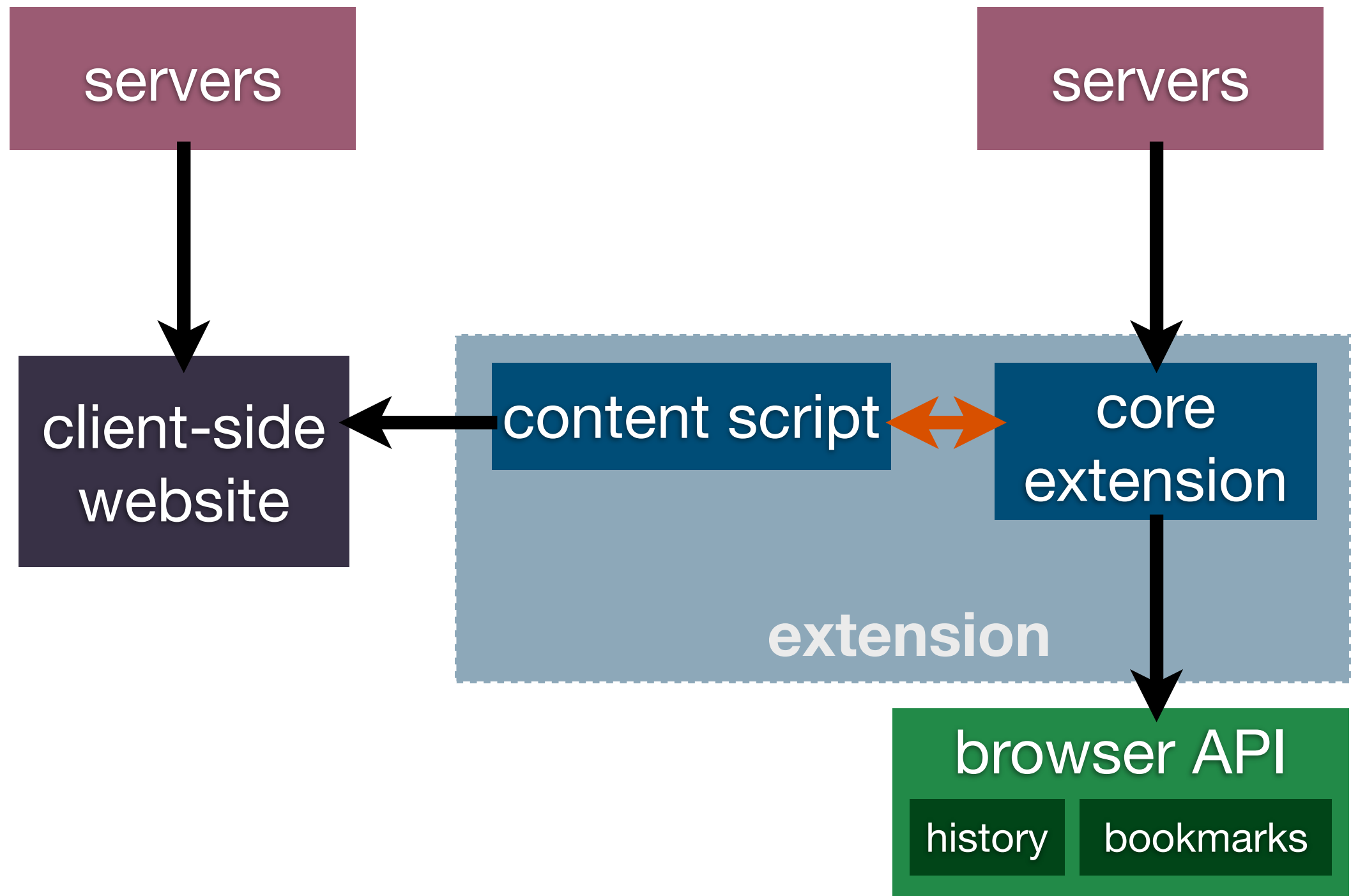
NETWORK ATTACKER



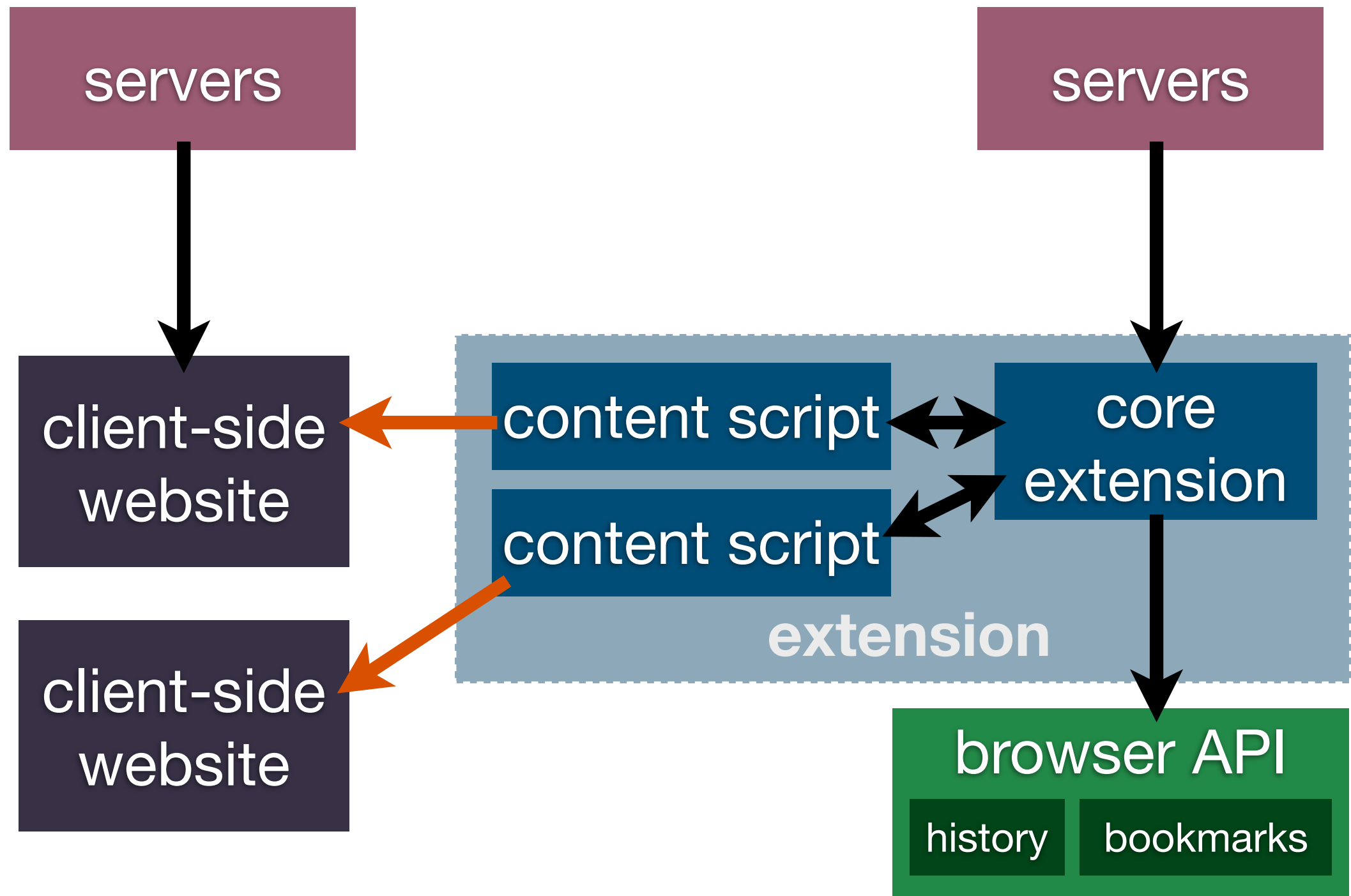
**NETWORK ATTACKER**

# **CHROME'S SECURITY MECHANISMS**

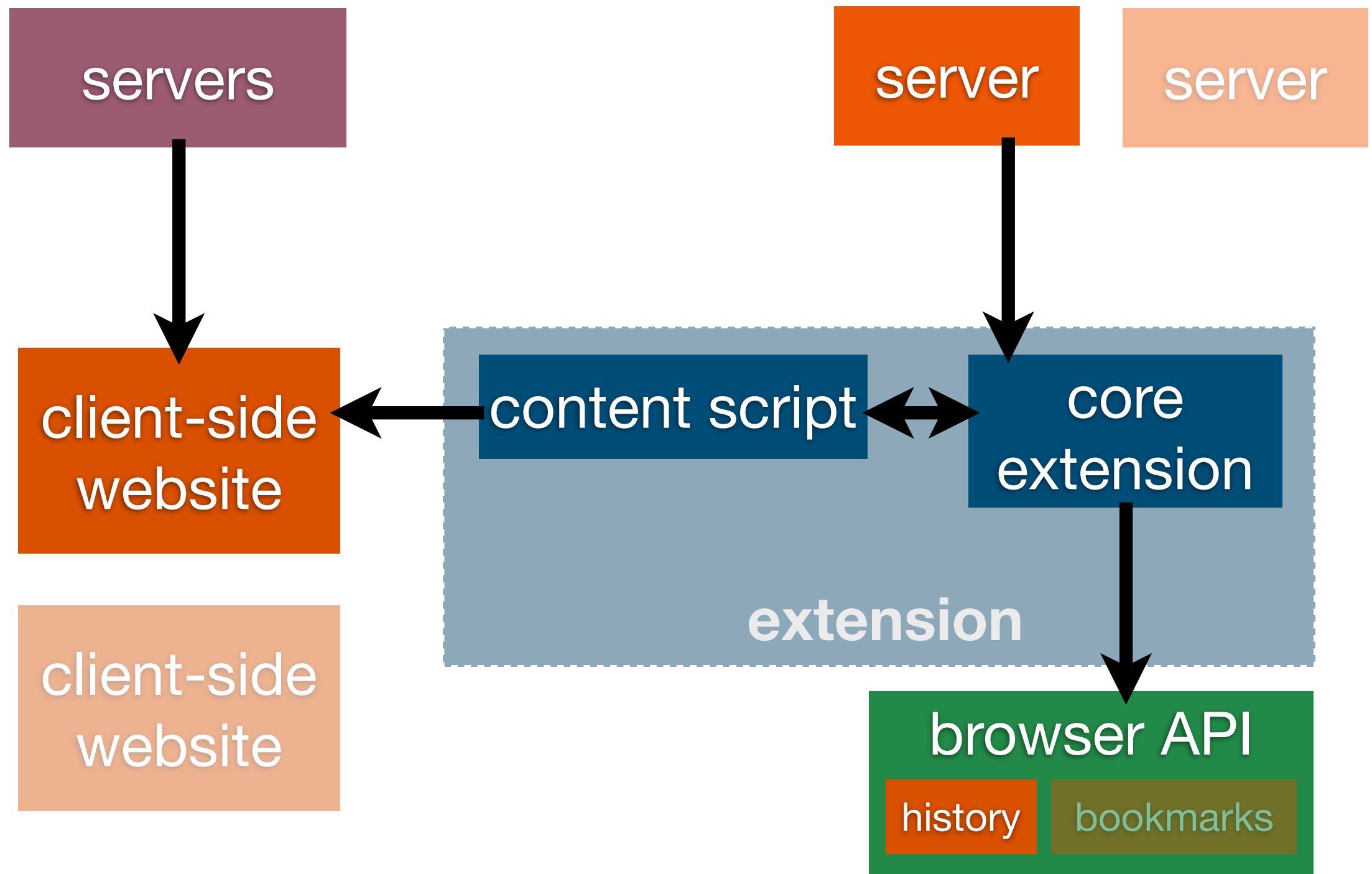




# PRIVILEGE SEPARATION



ISOLATED WORLDS



PERMISSIONS

**Vulnerabilities**

**Isolated worlds**

**Privilege separation**

**Permissions**

**New defenses**

**VULNERABILITIES**

# FINDING BUGS

## **SAMPLE**

50 most popular + 50 random extensions

## **METHODS**

Black-box testing + source code analysis

## **VERIFICATION**

Built exploits to confirm the vulnerabilities



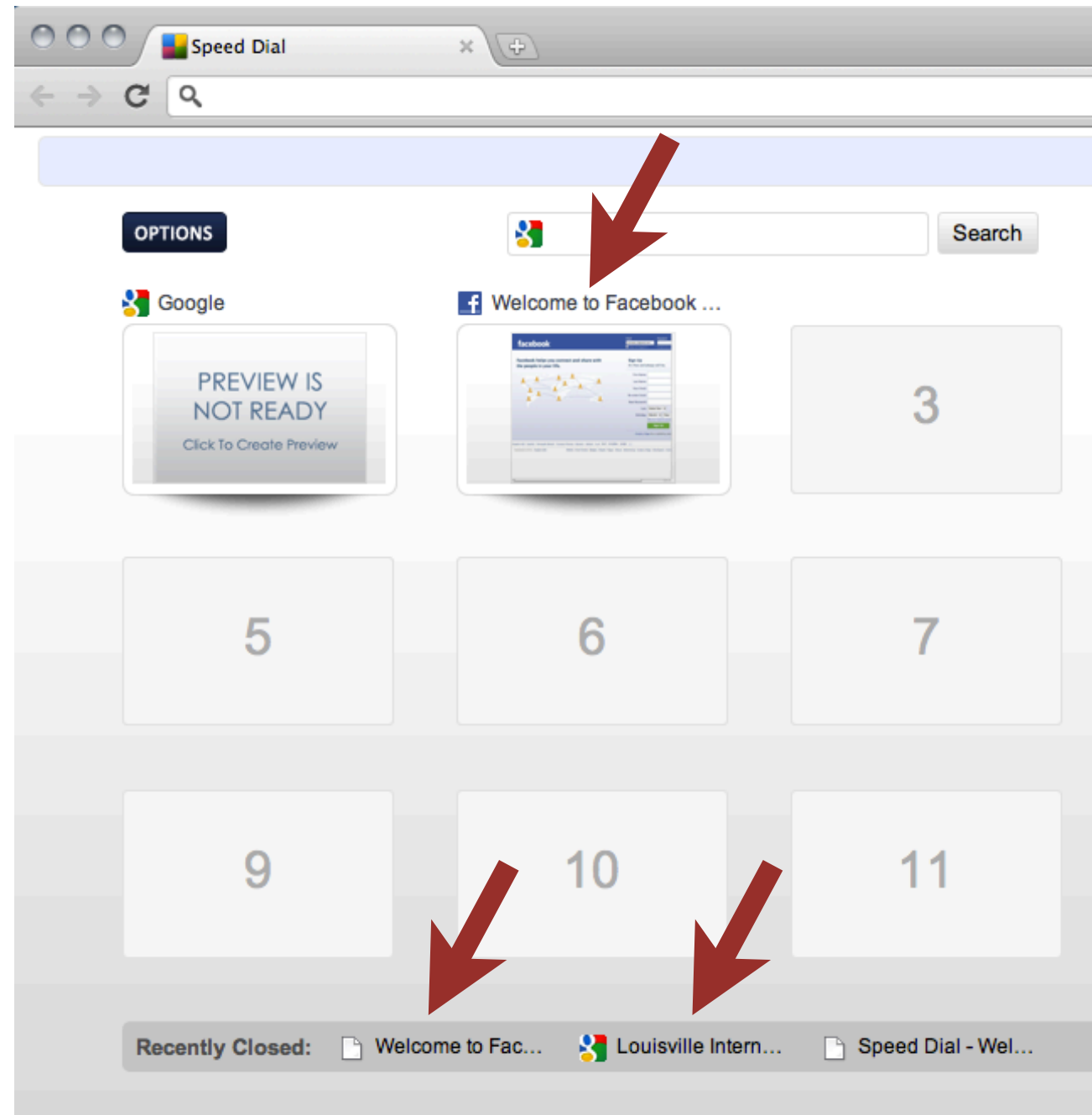
Vulnerability Location	Web Attacker	Network Attacker
Core	5	50
Content Script	3	1
Website	6	14

70 vulnerabilities in 40 extensions

# VULNERABILITIES

Popular	Random	Total
22	18	40

**VULNERABLE EXTENSIONS**



EXAMPLE: SPEED DIAL

**ISOLATED WORLDS**

**Isolated worlds:**

protect content scripts

from web attackers

**Vulnerability count:**

**3 content script vulns**



# DATA AS HTML

## **MISTAKE**

Insert data as HTML, where it can execute

## **MITIGATION**

Will execute in *website's* isolated world

## **VULNERABILITIES**

6 extensions have data-as-HTML bugs that *don't* cause content script vulnerabilities

# EVAL

## **MISTAKE**

Use eval to execute untrusted data

## **MITIGATION**

Isolated worlds does not mitigate this bug

## **VULNERABILITIES**

2 vulnerabilities due to this mistake

# CLICK INJECTION

## **MISTAKE**

Trusting event handlers on a website

## **MITIGATION**

Isolated worlds does not mitigate this bug

## **VULNERABILITIES**

1 vulnerability due to this mistake

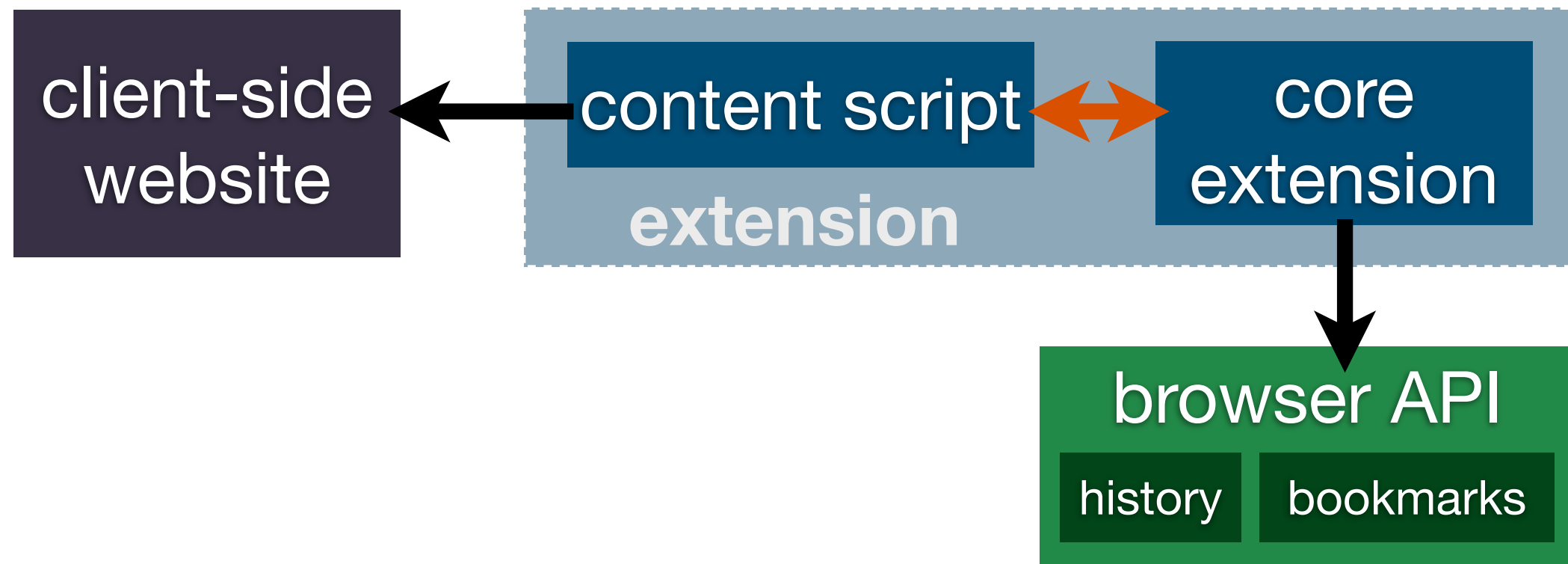
Isolated worlds is highly  
effective because it  
mitigates **common** bugs

# PRIVILEGE SEPARATION

**Privilege separation:**

protect core extensions





# PRIVILEGE SEPARATION

Can **regular** developers  
use privilege separation?

Permissions	Extensions
All of the extensions'	7%
Partial: XHRs	15%
Partial: tab control	8%
Partial: other	8%

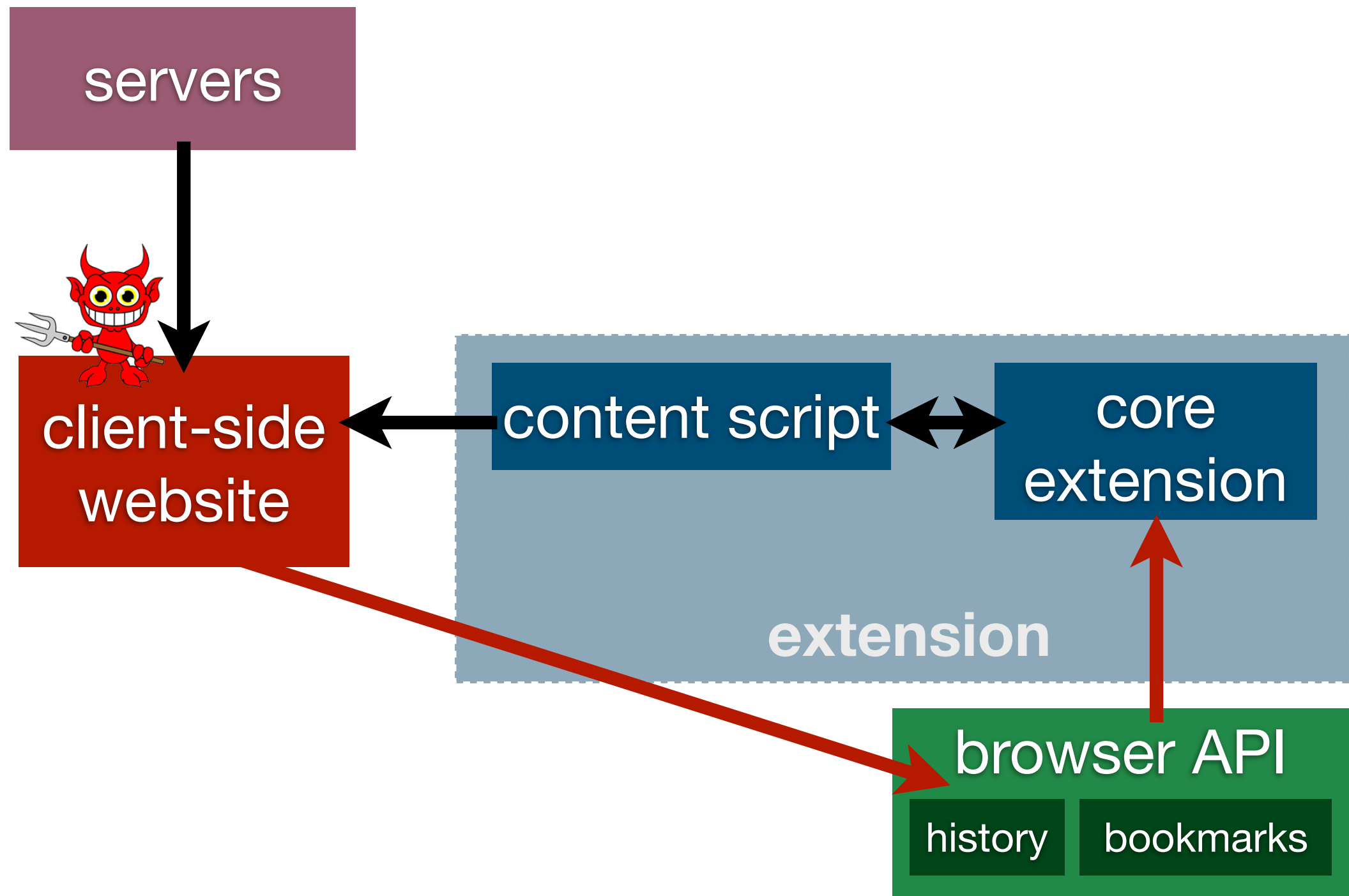
(Of the 61 extensions with content scripts)

**PRIVILEGE “LEAKAGE”**

**Privilege separation would  
fully protect most core  
extensions, but a third of  
developers circumvent it**

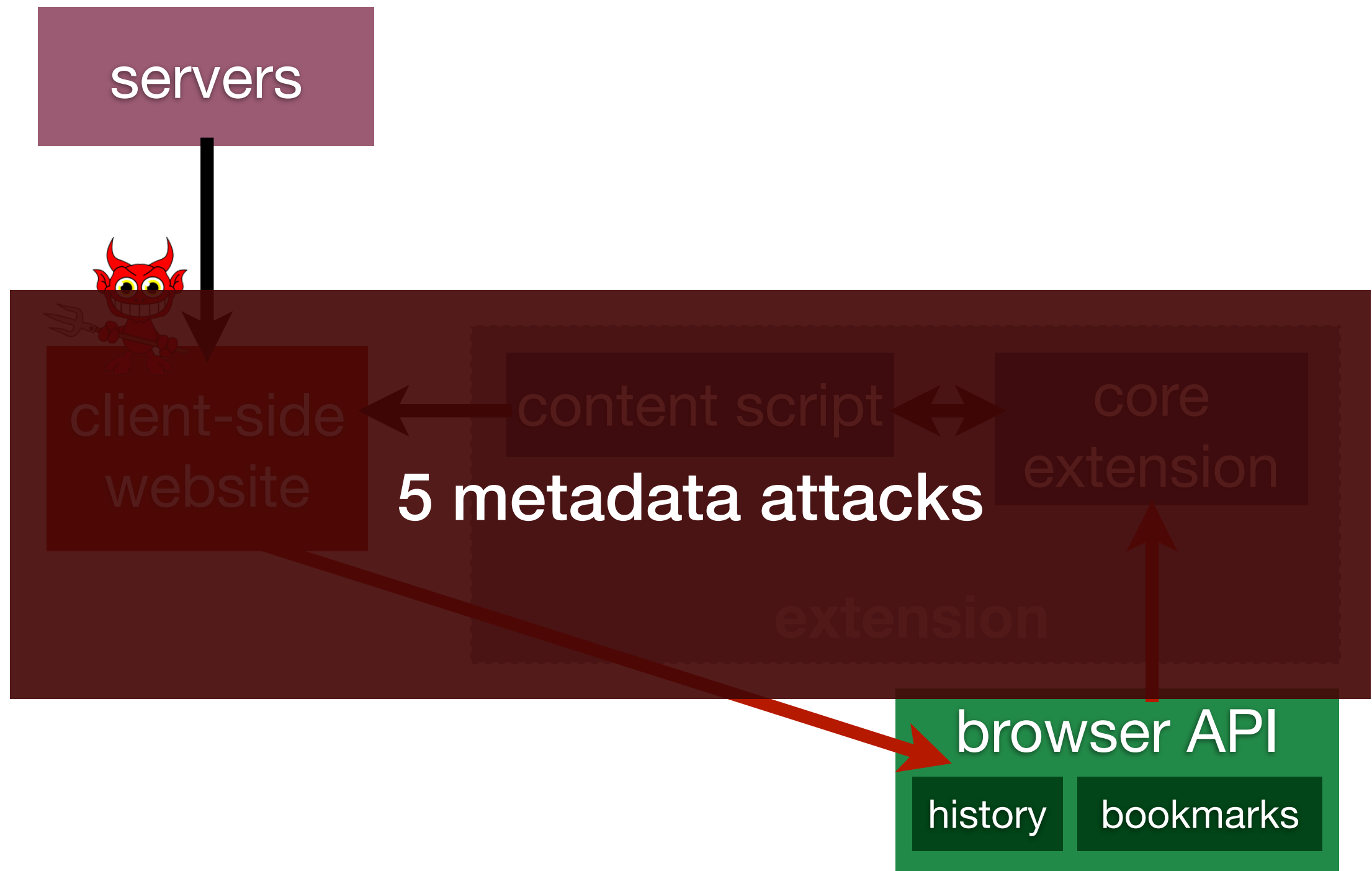
**Vulnerability count:**

**50 core extension vulns**

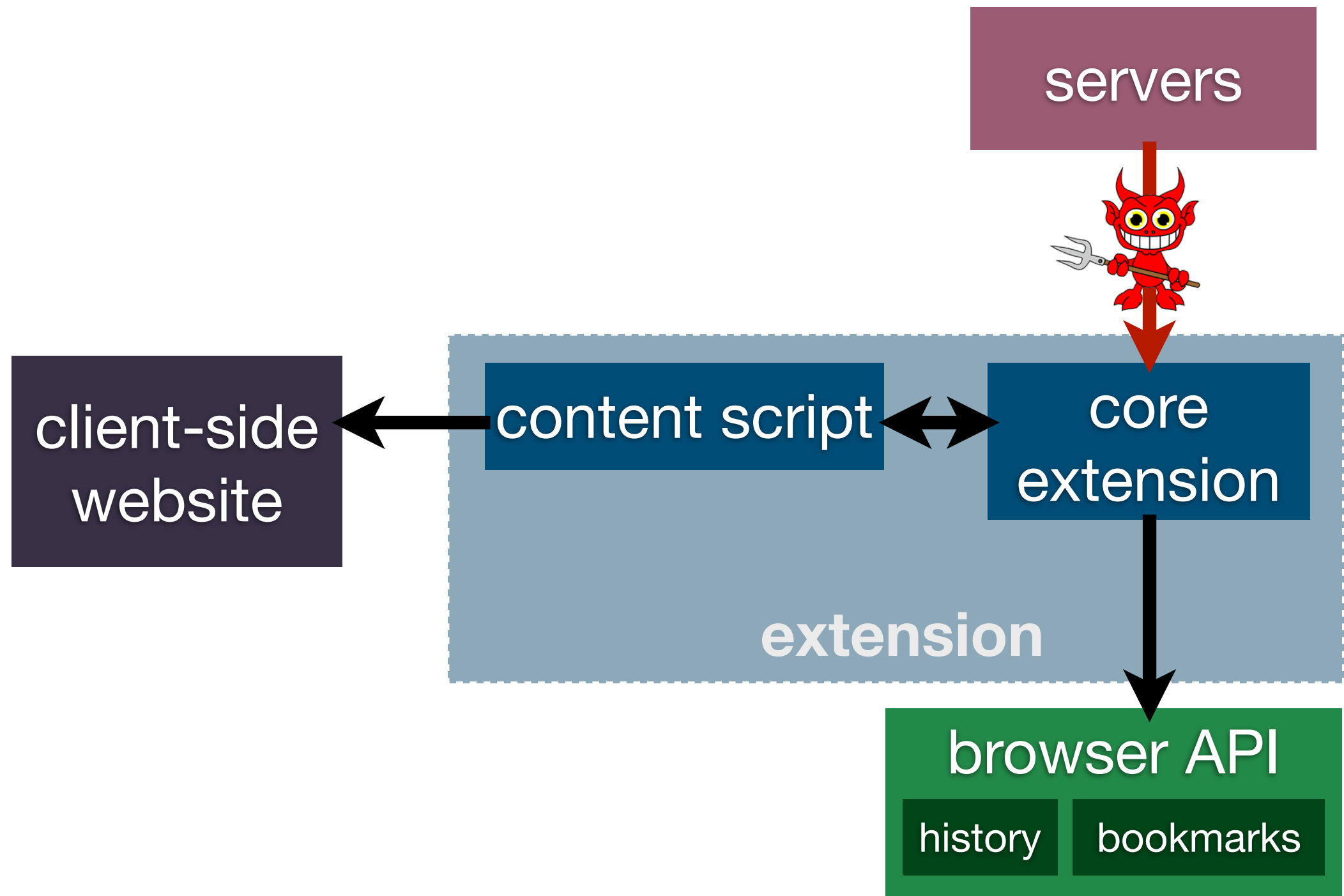


# METADATA ATTACK

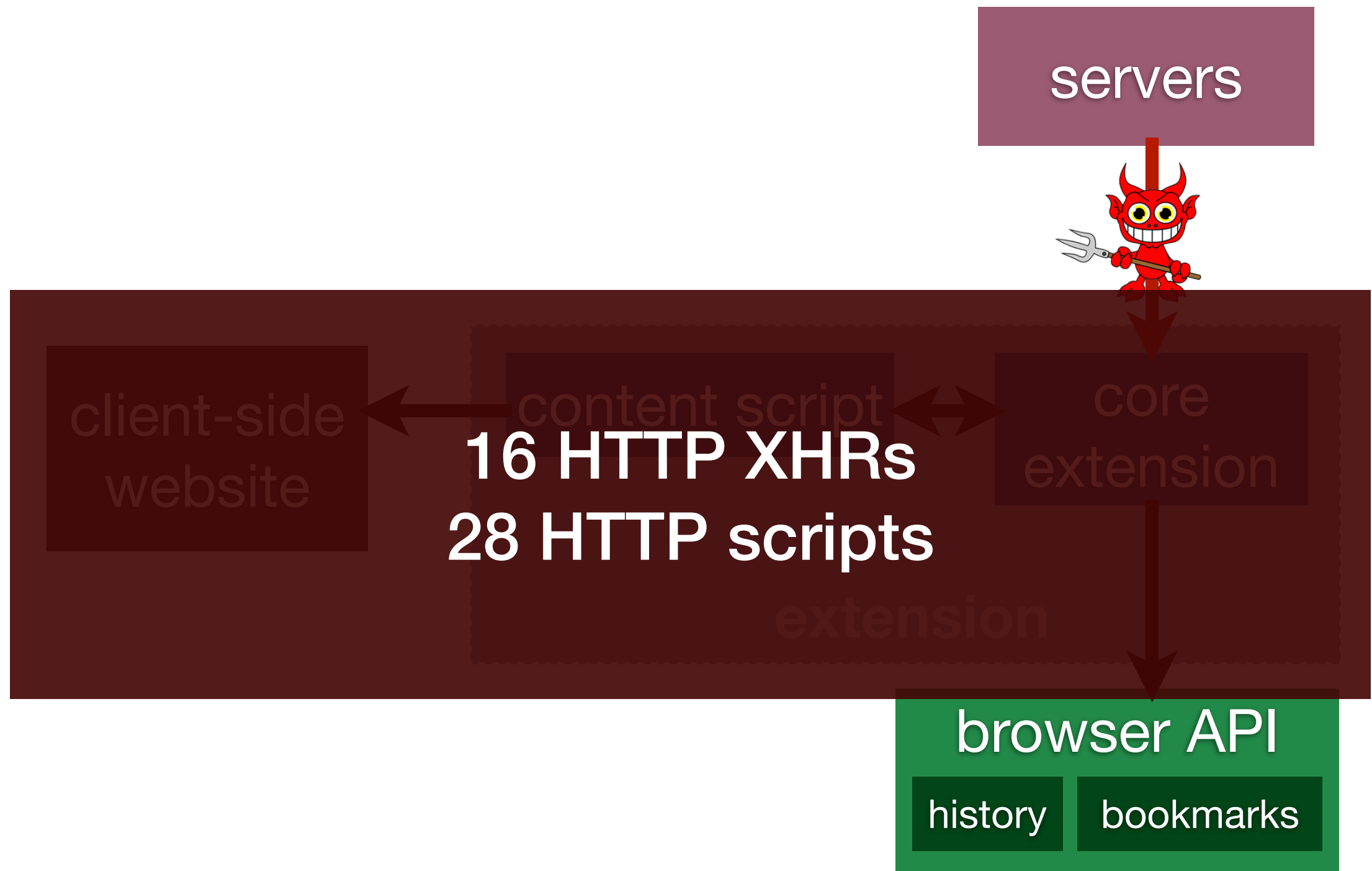




# METADATA ATTACK



# HTTP SCRIPTS/XHRS



# HTTP SCRIPTS/XHRS

Privilege separation can  
be powerful,  
**but its placement in the  
system matters**

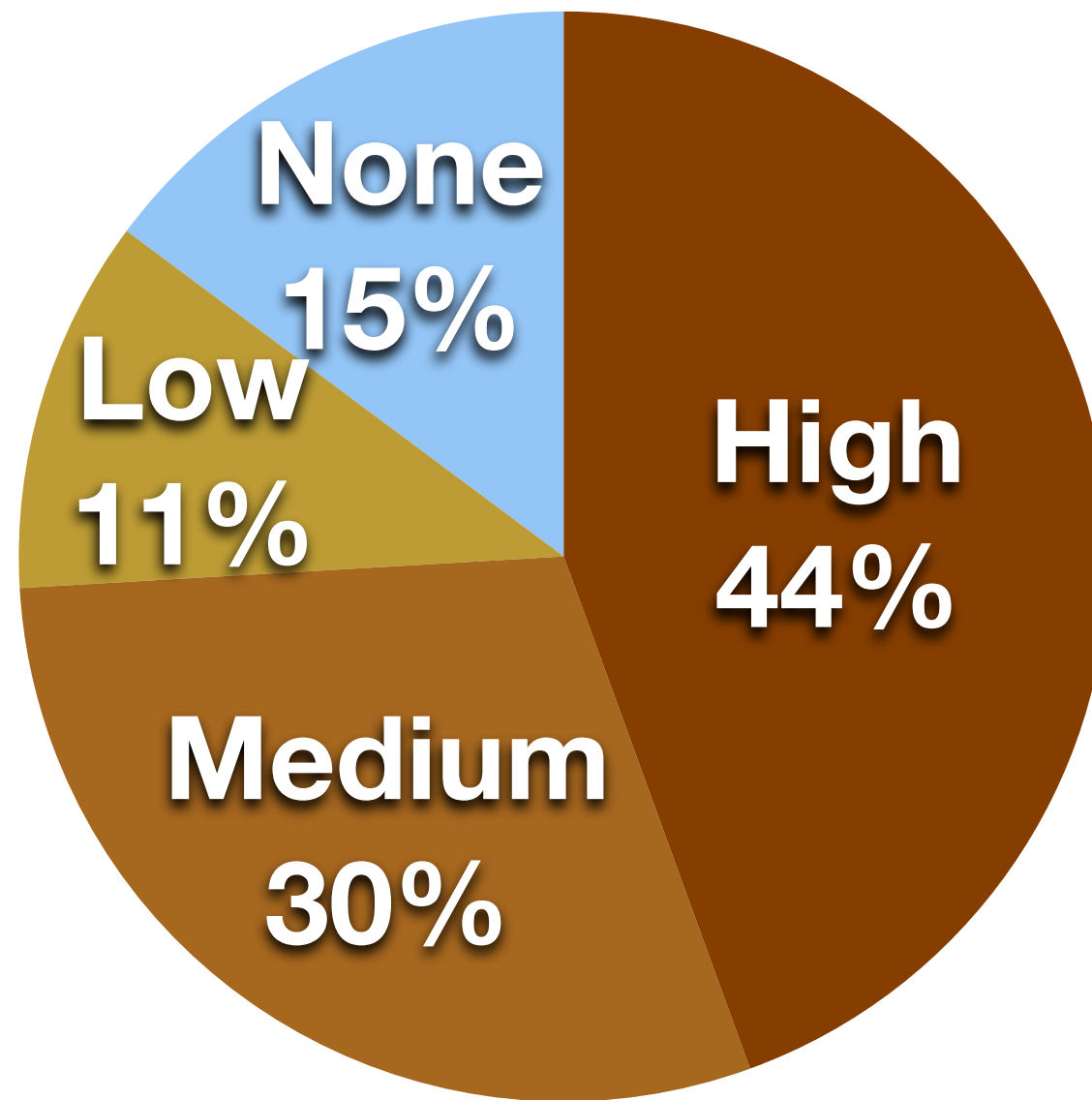
**Something else is needed  
to protect core extensions**

# PERMISSIONS

# **Permissions:**

**limit the scope of core**

**vulnerabilities**

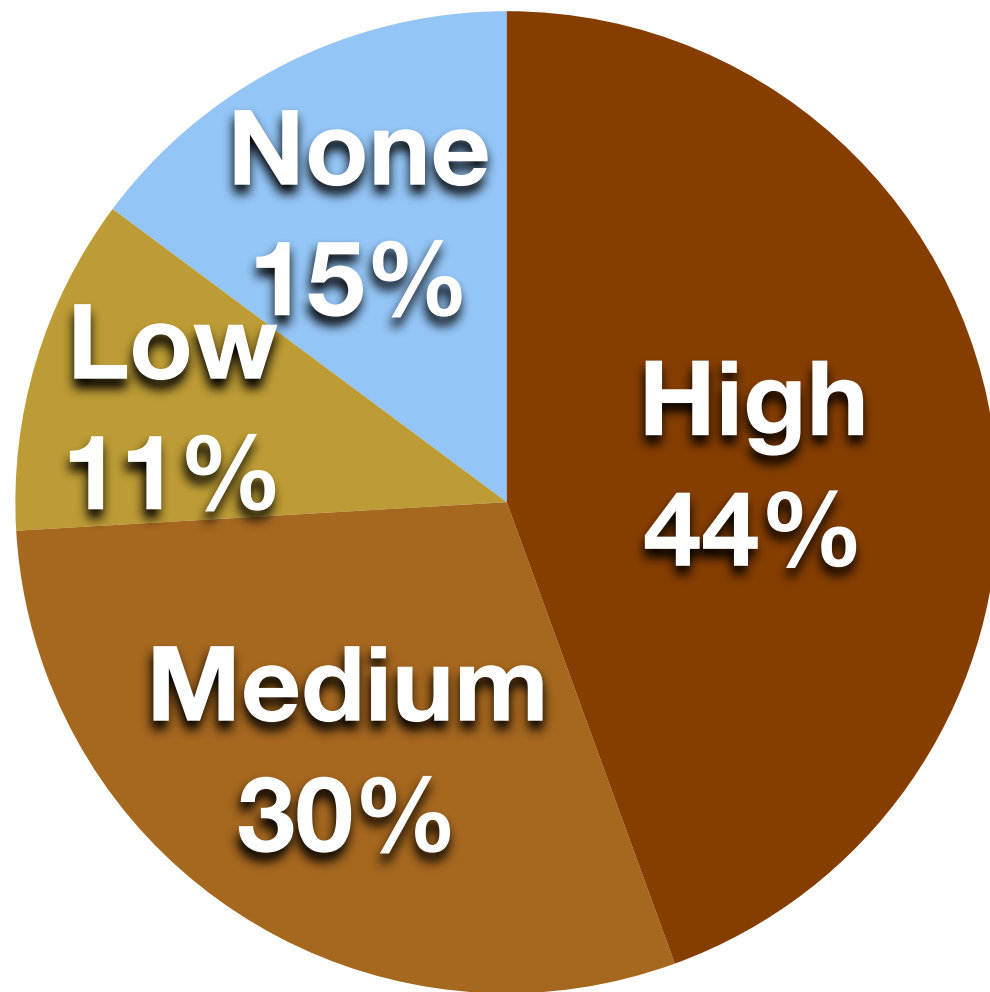


27 buggy extensions

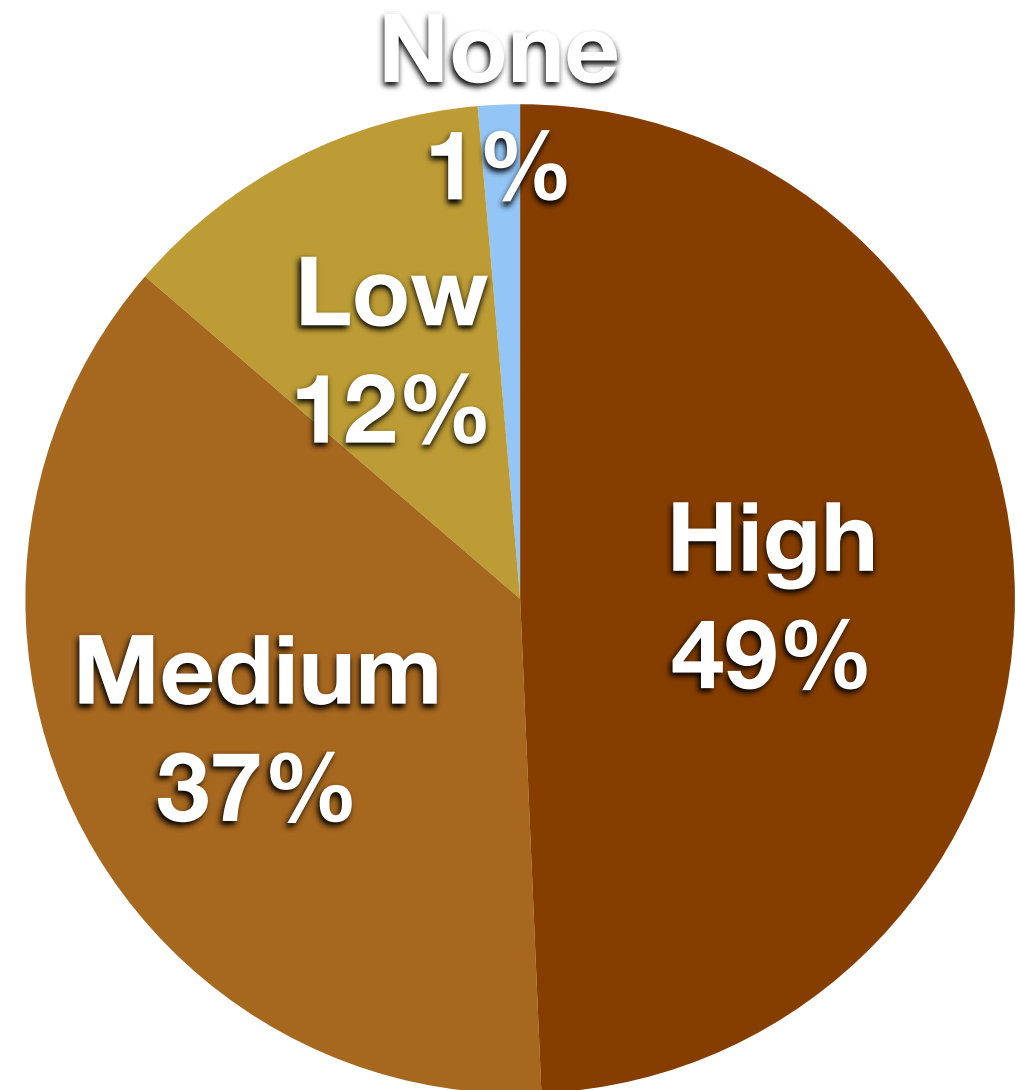
**PERMISSION RATE**



**Reduces potential for  
severe attacks by half**



with bugs



others

## RATE COMPARISON

**No correlation** between  
bugs and permissions

**Yes,** permissions limit the  
scope of vulnerabilities

**NEW DEFENSES**

**Use CSP to ban unsafe  
coding practices**

Restriction	Security Benefit	Broken, But Fixable	Broken And Unfixable	
No HTTP scripts in cores	15%	15%	0%	✓
No inline scripts	15%	79%	0%	✓
No eval	3%	30%	2%	✗
No HTTP XHRs	17%	29%	14%	✗

POTENTIAL BANS

Restriction	Security Benefit	Broken, But Fixable	Broken And Unfixable	
No HTTP scripts in cores	15%	15%	0%	✓
No inline scripts	15%	79%	0%	✓
No eval	3%	30%	2%	✗
No HTTP XHRs	17%	29%	14%	✗

**ADOPTION**



Restriction	Security Benefit	Broken, But Fixable	Broken And Unfixable
Chrome 18 policy	27%	85%	2%

**ADOPTION**

# CONCLUSION

- Isolated worlds prevents common bugs
- Some developers don't use privilege separation optimally
- Permissions reduce scope of vulns
- Recommend banning unsafe practices to protect core extensions

# QUESTIONS?

**adriennenefelt@gmail.com**

[www.adrienneporterfelt.com](http://www.adrienneporterfelt.com)