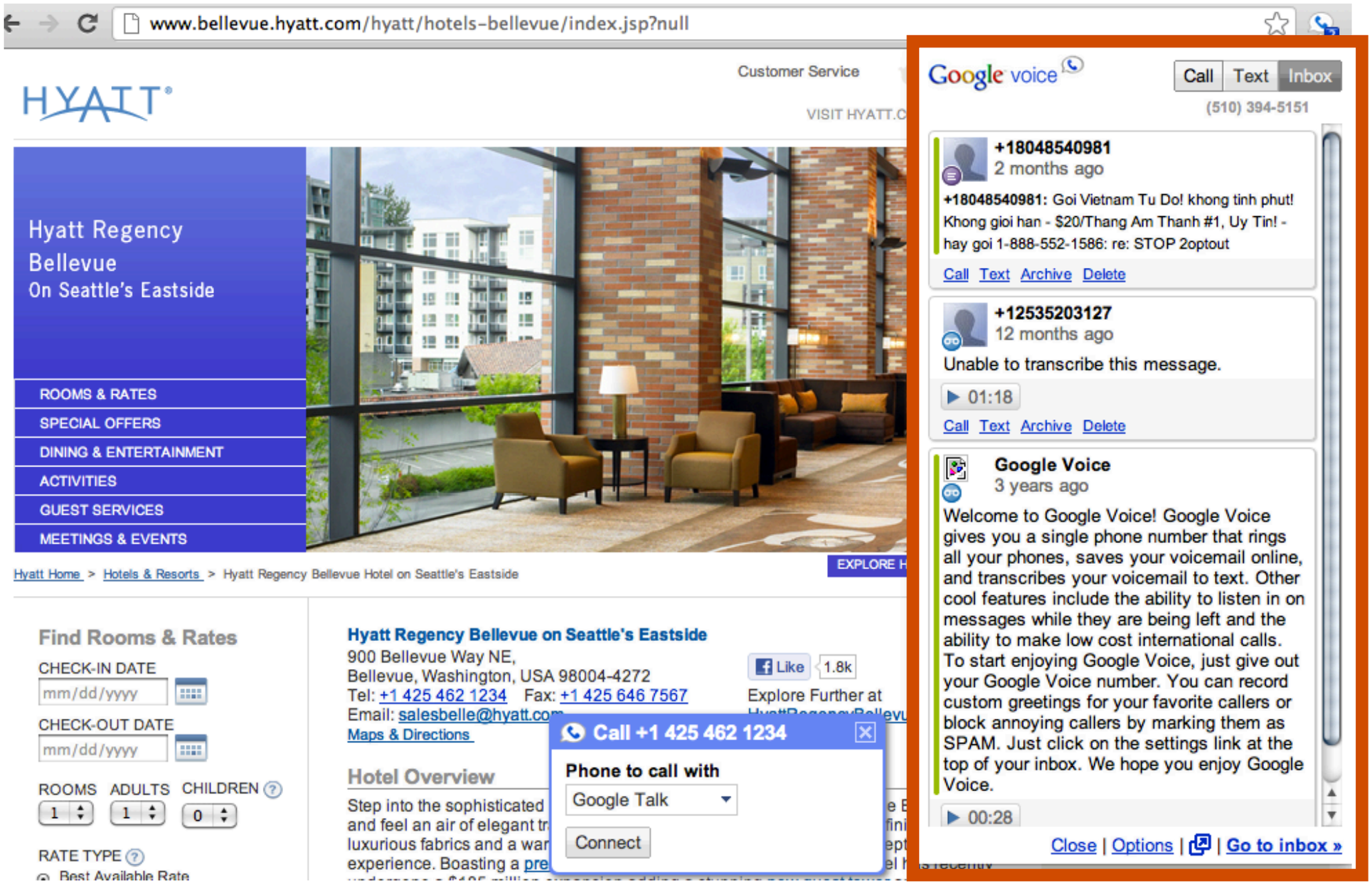
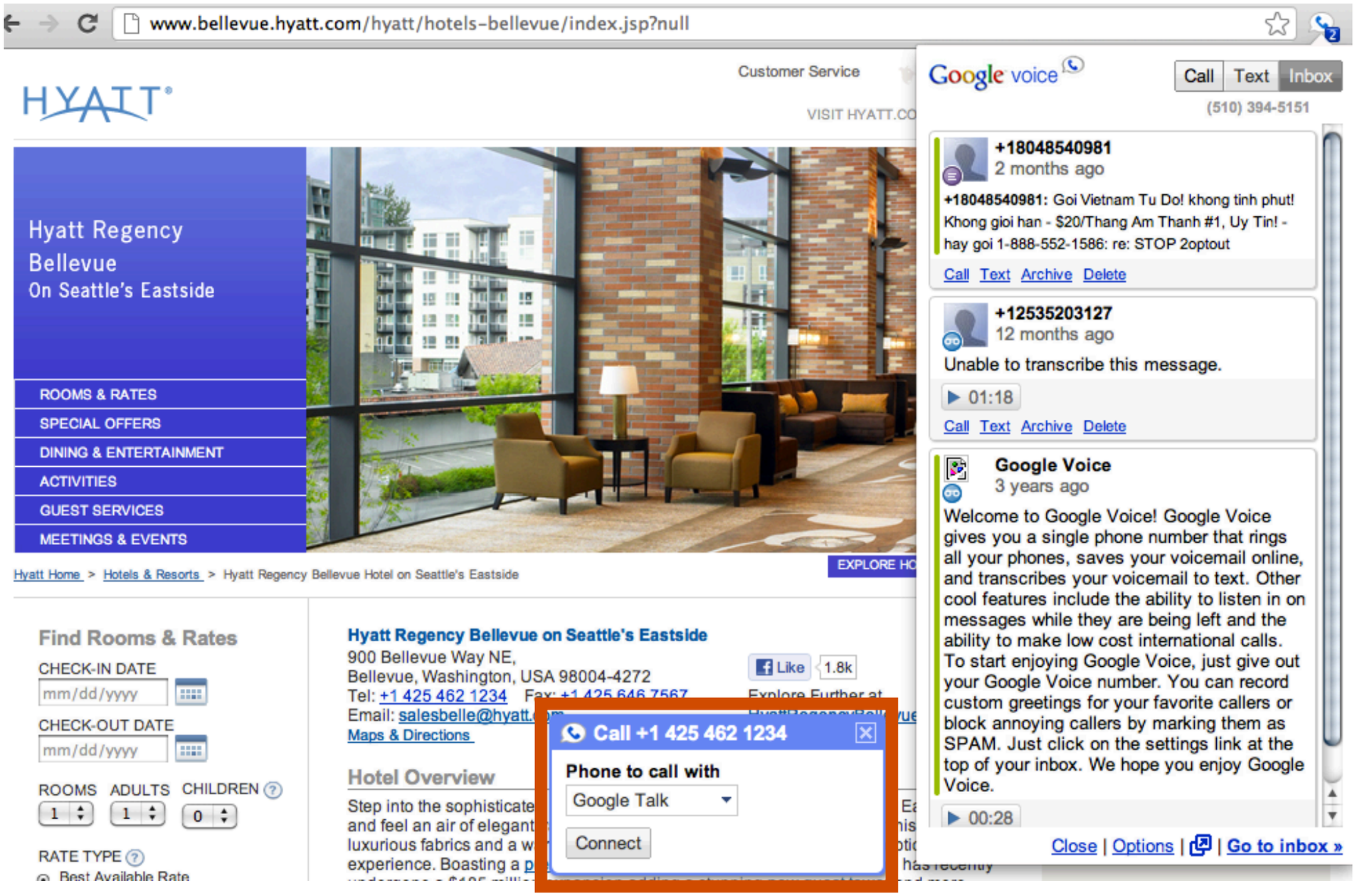
AN EVALUATION OF THE GOOGLE CHROME EXTENSION SECURITY ARCHITECTURE

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



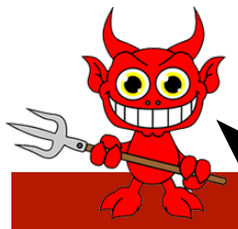
CHROME EXTENSIONS



CHROME EXTENSIONS

servers

servers



client-side website

extension

client-side website

browser API

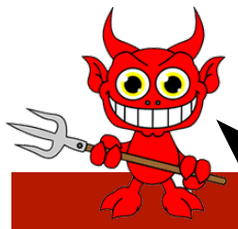
history

bookmarks

WEB ATTACKER

servers

servers



client-side website

extension

client-side website

browser API

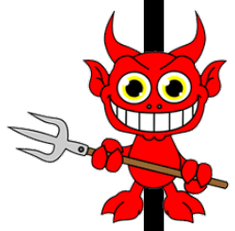
history

bookmarks

WEB ATTACKER

servers

servers



client-side website

client-side website

extension

browser API

history

bookmarks

NETWORK ATTACKER

servers

servers

client-side website

client-side website

extension

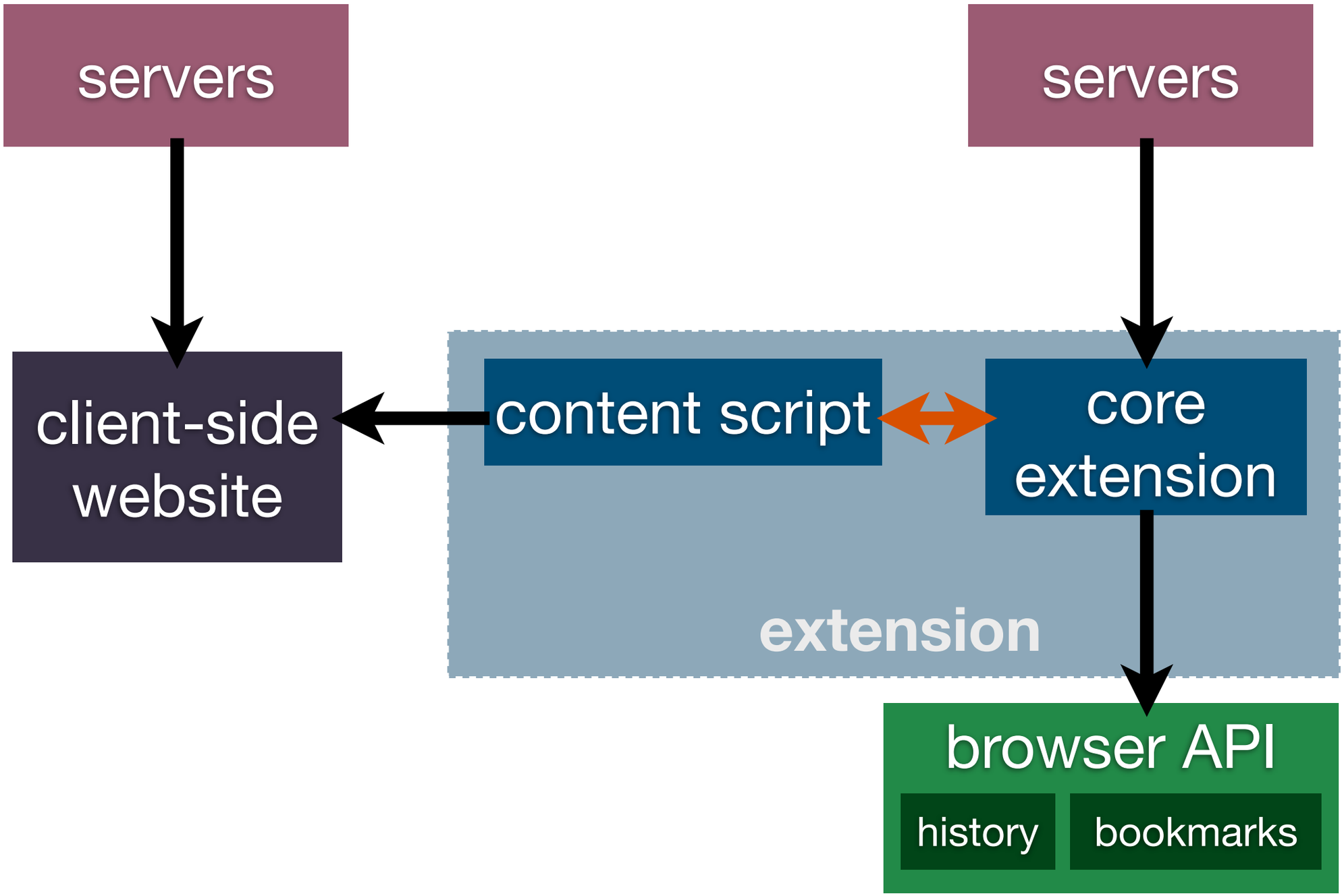
browser API

history

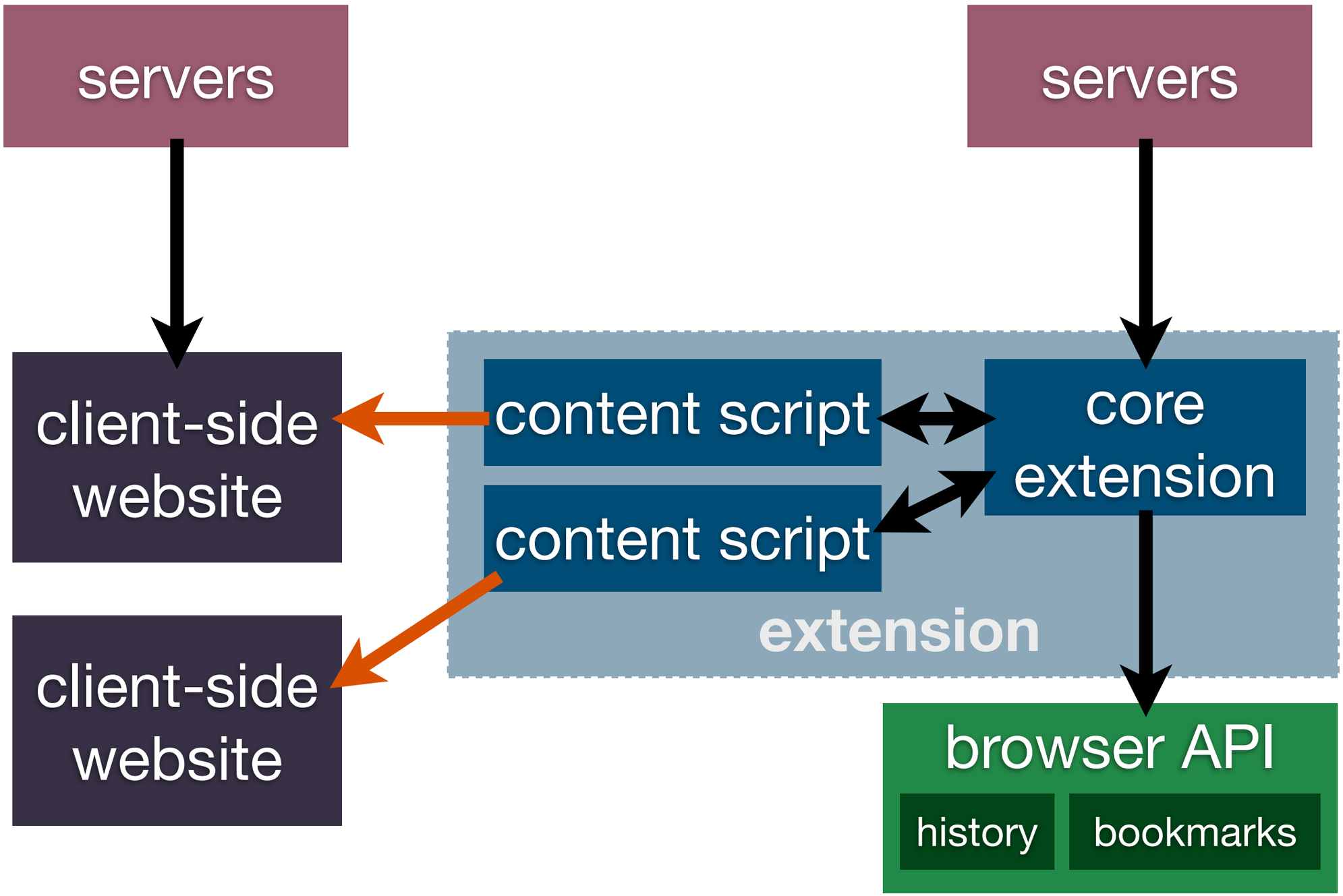
bookmarks

NETWORK ATTACKER

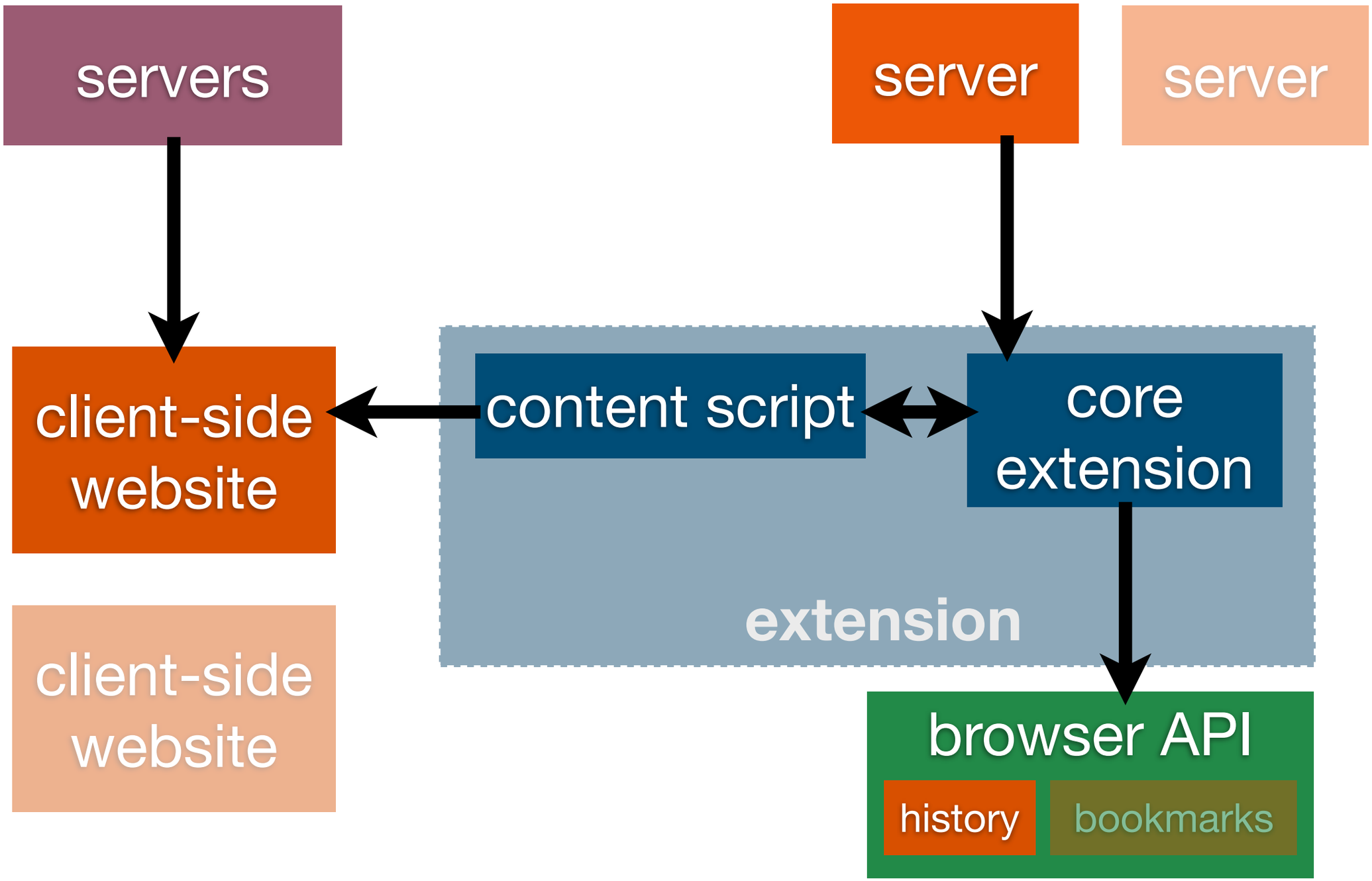
CHROME'S SECURITY MECHANISMS



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

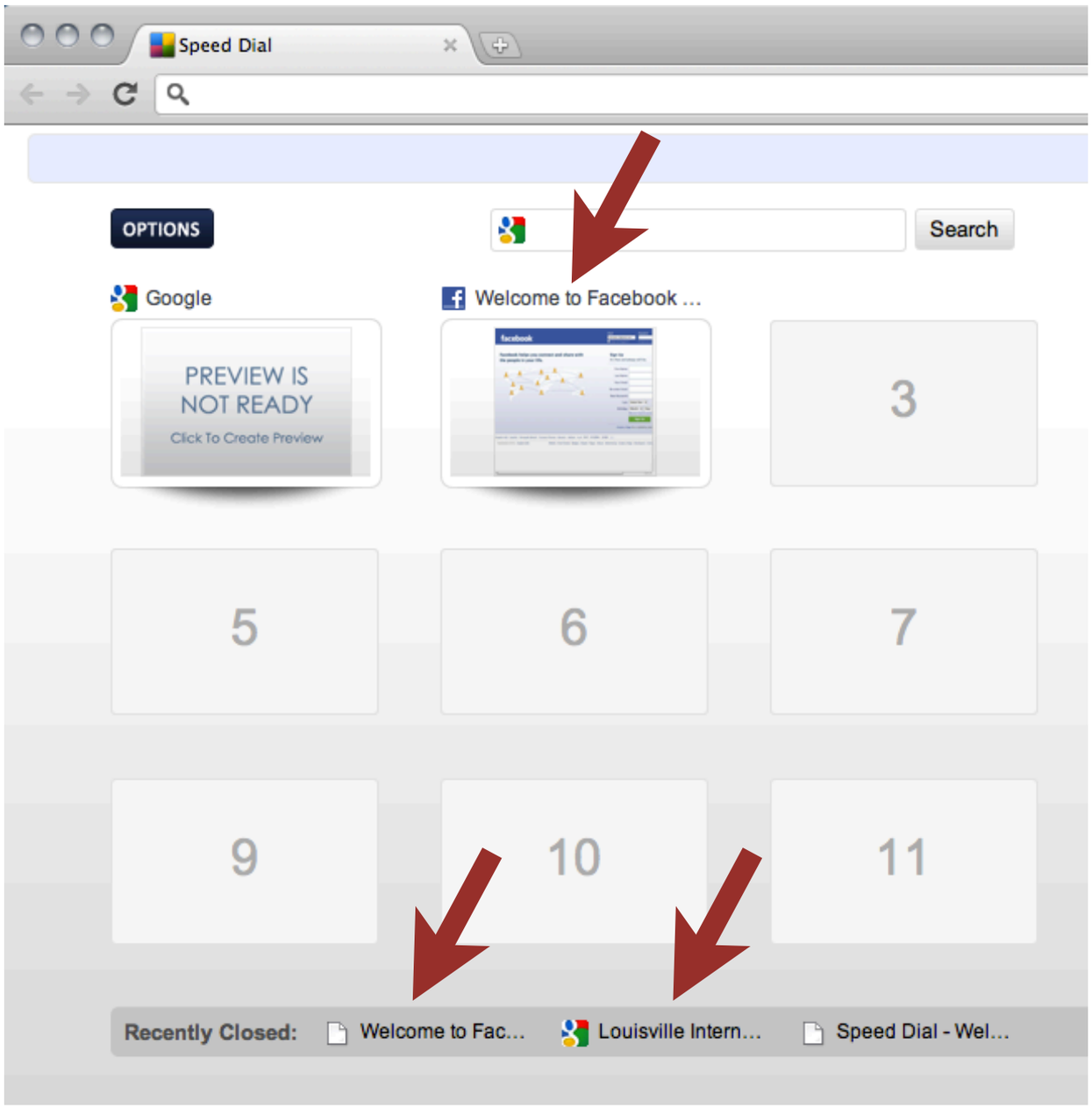
Vulnerability Location	Web Attacker	Network Attacker
Core	5	50
Content Script	3	1
Website	6	14

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

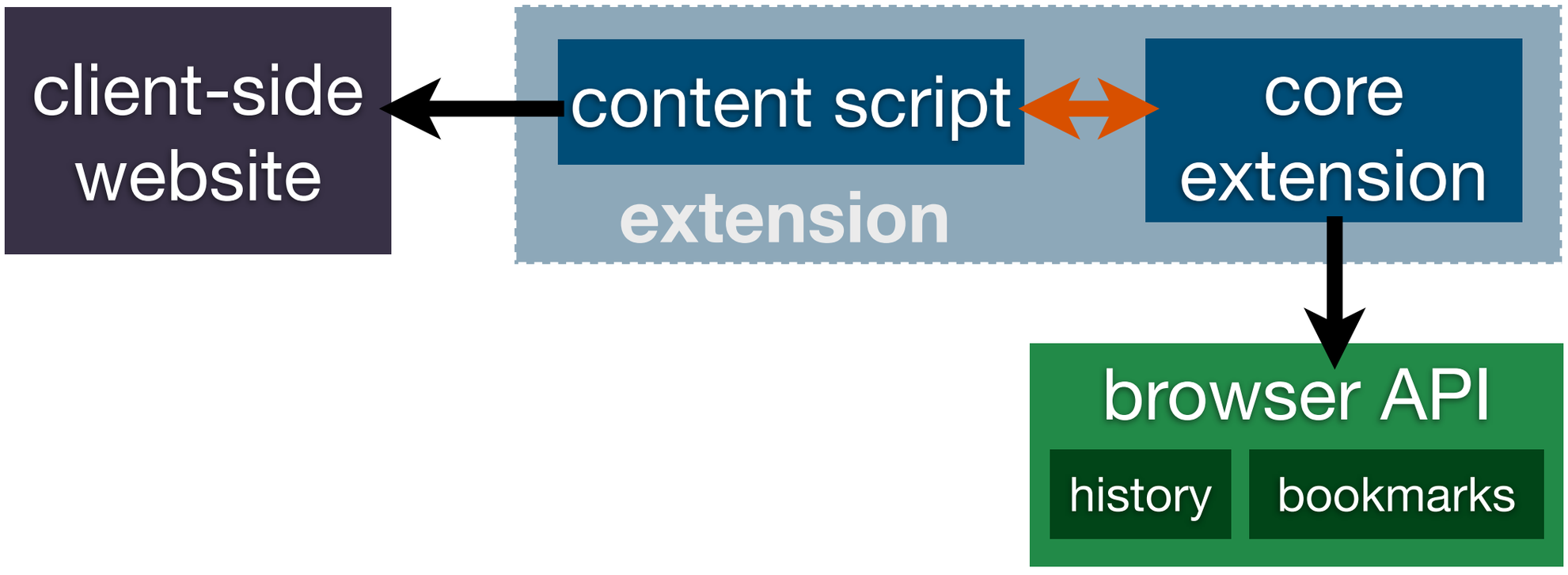
1 vulnerability due to this mistake

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%

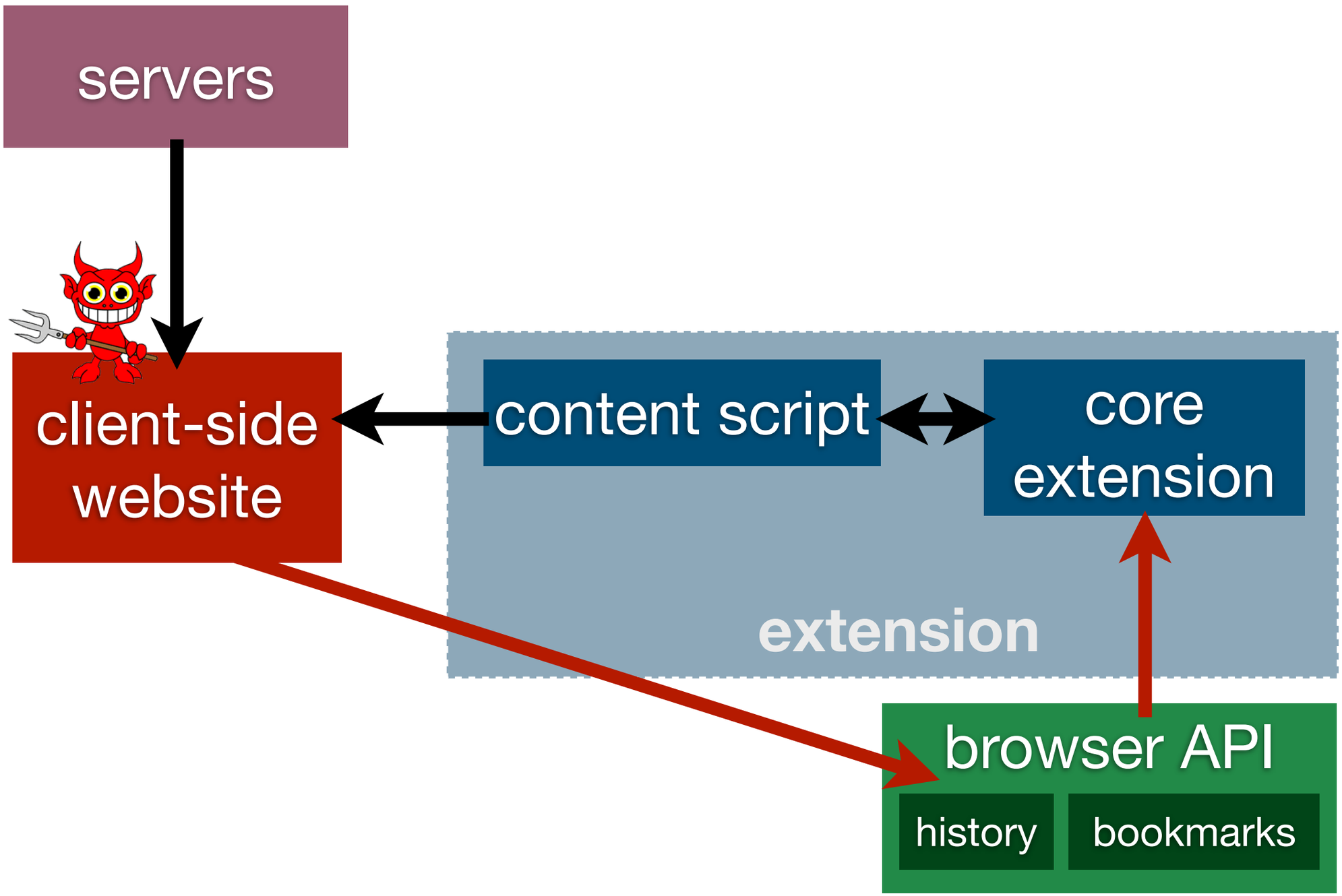
(Of the 61 extensions with content scripts)

PRIVILEGE “LEAKAGE”

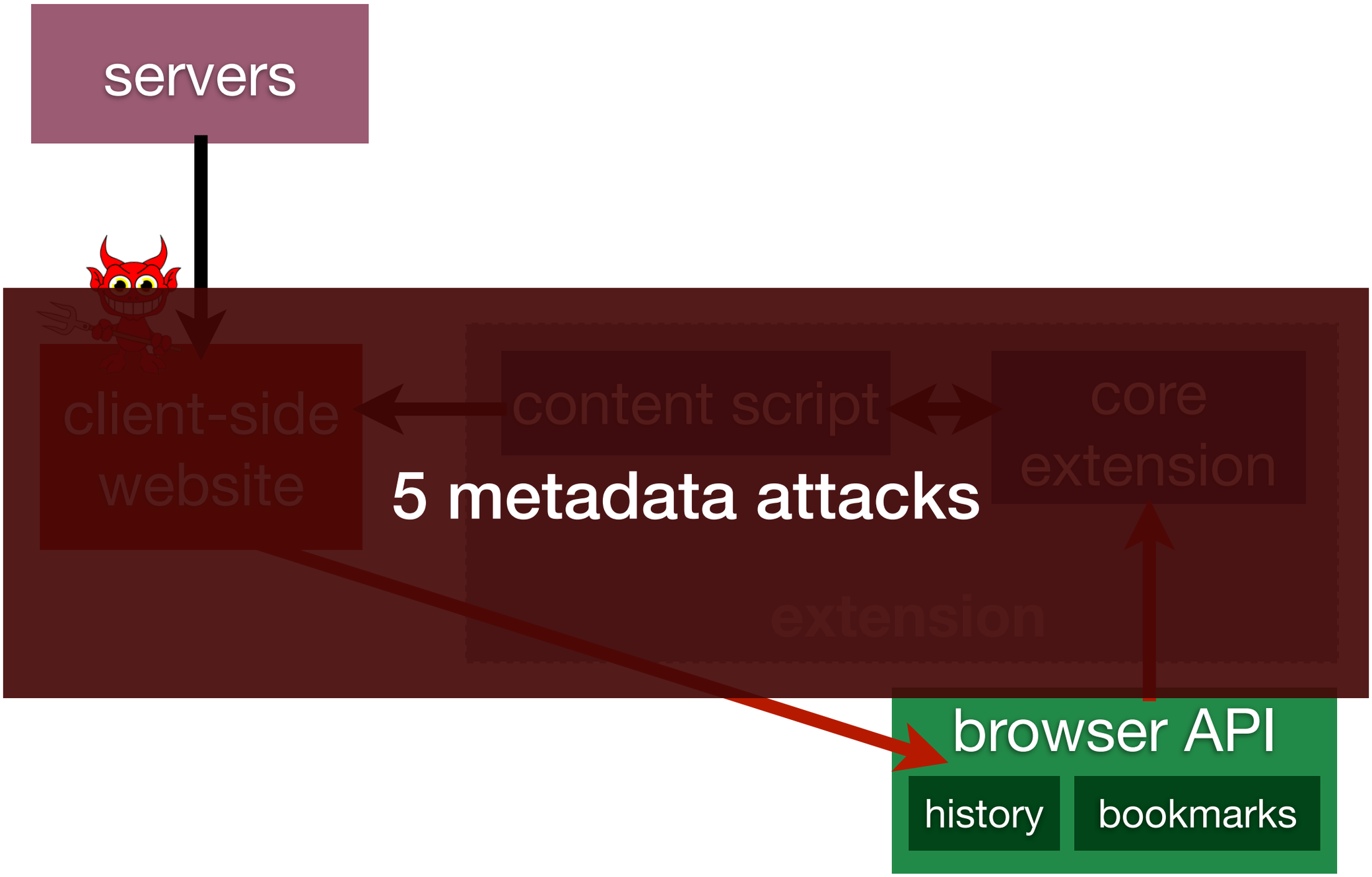
Privilege separation would fully protect most core extensions, but a third of developers circumvent it

Vulnerability count:

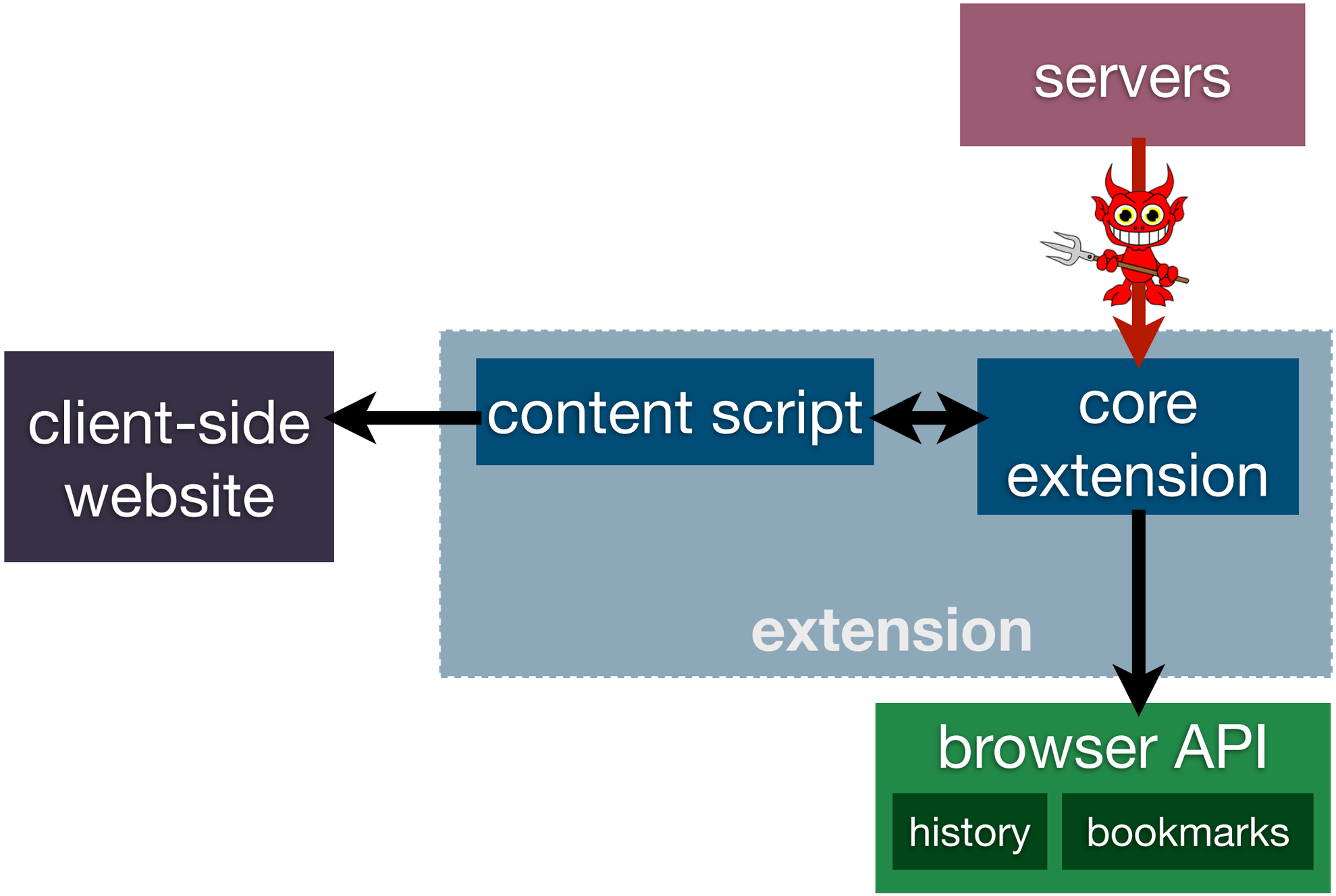
50 core extension vulns



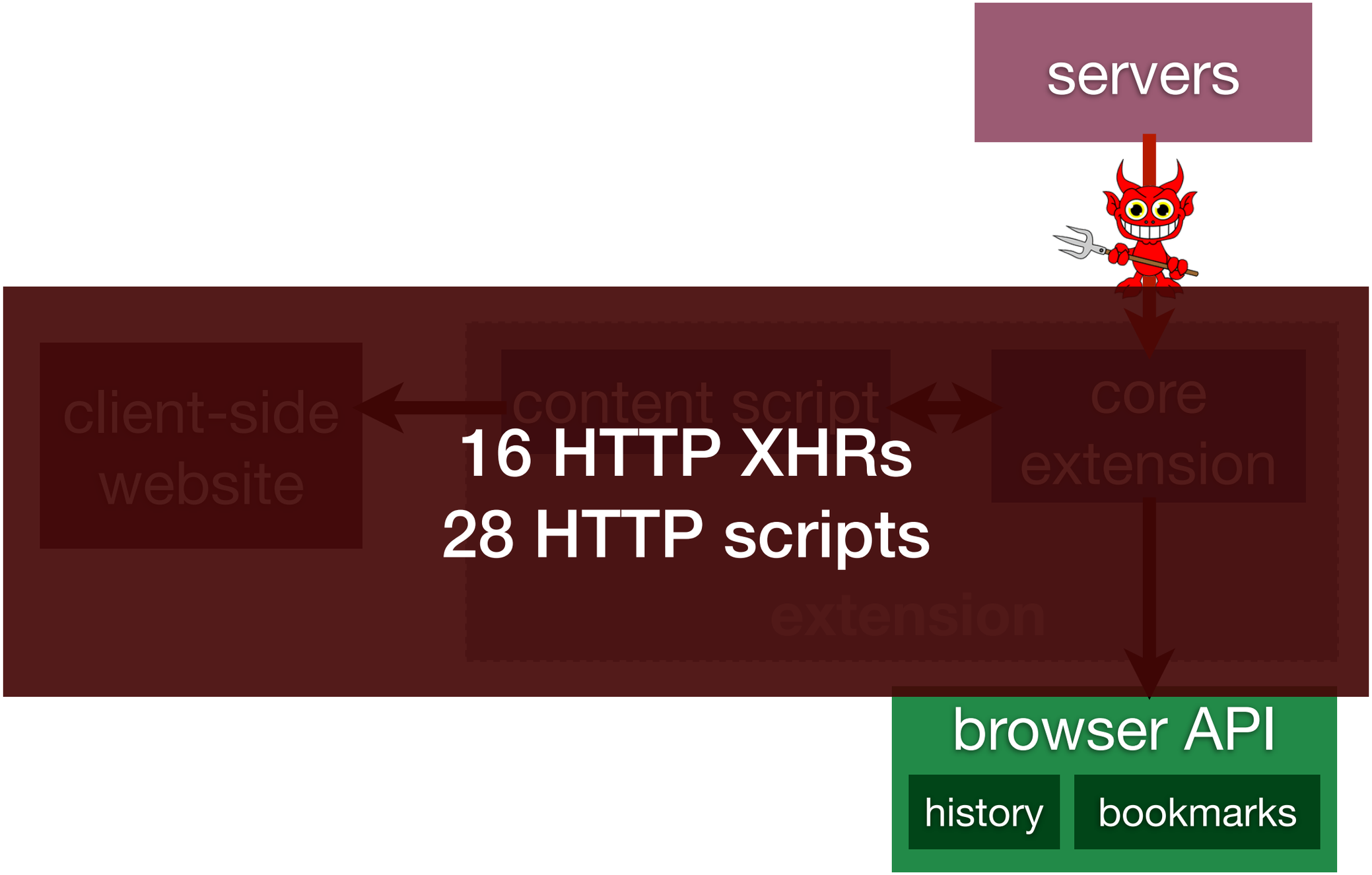
METADATA ATTACK



METADATA ATTACK



HTTP SCRIPTS/XHRS



HTTP SCRIPTS/XHRS

Privilege separation can be powerful,

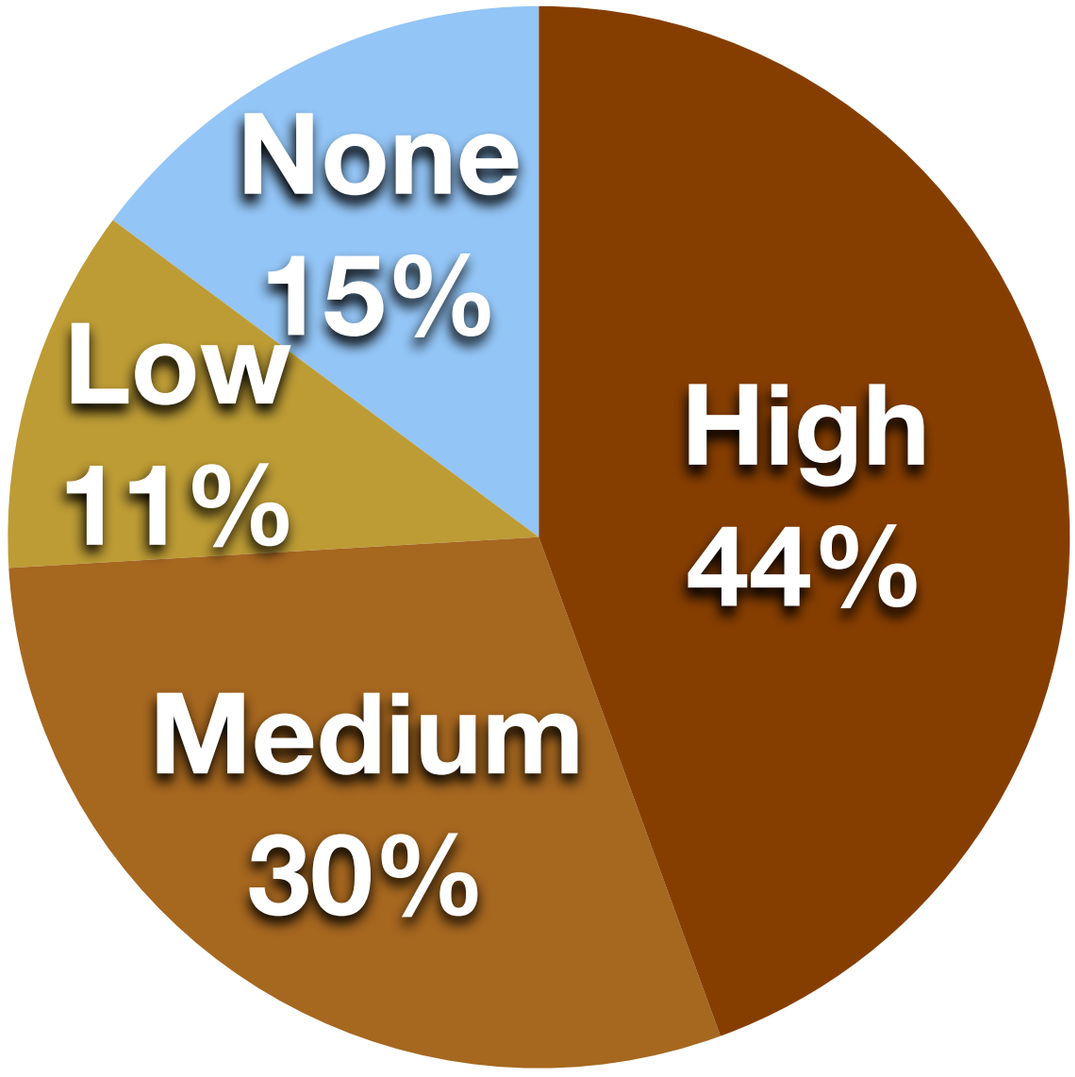
but its placement in the system matters

Something else is needed to protect core extensions

PERMISSIONS

Permissions:

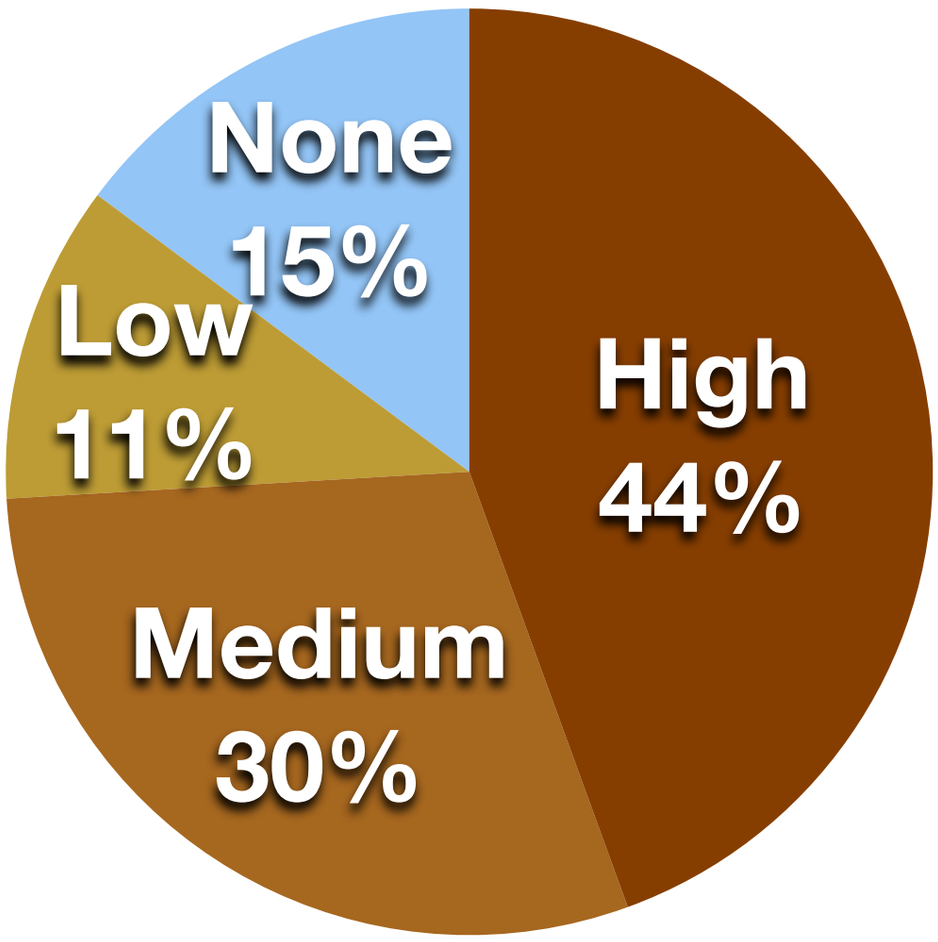
limit the scope of core vulnerabilities



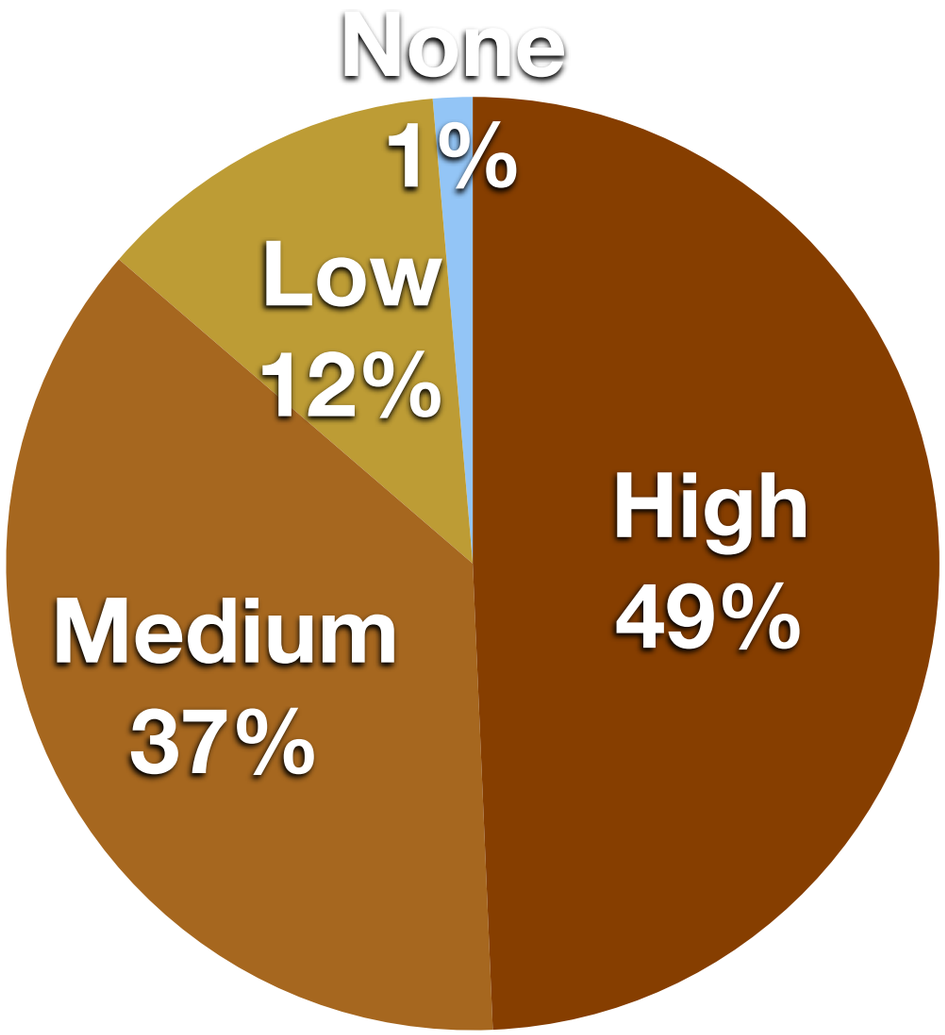
27 buggy extensions

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?

adriennefelt@gmail.com

www.adrienneporterfelt.com