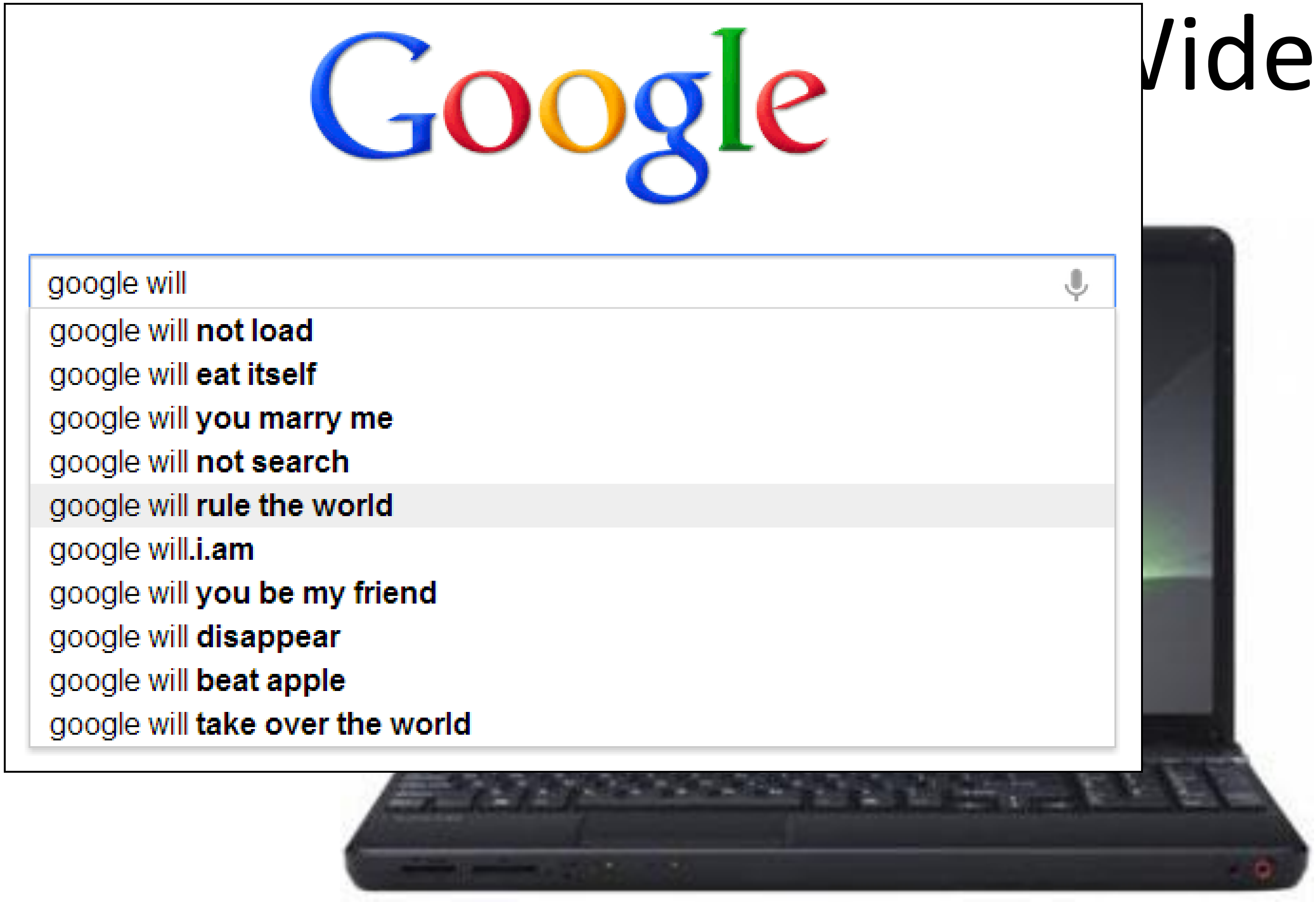
Rethinking Web Platform Extensibility

Mohan Dhawan

Rutgers University

Gateway to the World Wide Web

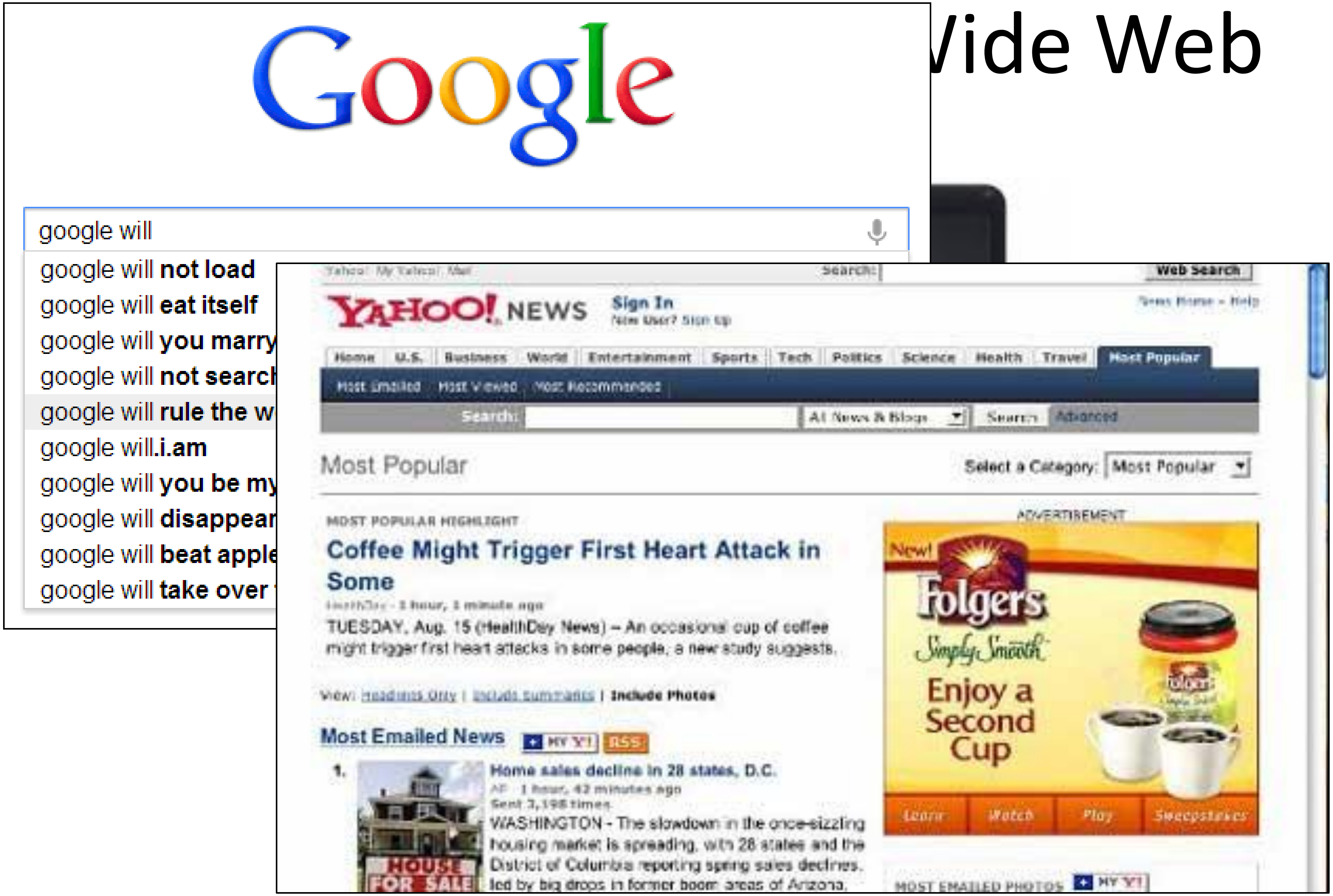
Vide Web



google will

google will **not load**
google will **eat itself**
google will **you marry me**
google will **not search**
google will **rule the world**
google will**.i.am**
google will **you be my friend**
google will **disappear**
google will **beat apple**
google will **take over the world**

Vide Web



google will

- google will **not load**
- google will **eat itself**
- google will **you marry**
- google will **not search**
- google will **rule the w**
- google will**.i.am**
- google will **you be my**
- google will **disappear**
- google will **beat apple**
- google will **take over**

Most Popular

Select a Category: Most Popular

MOST POPULAR HIGHLIGHT

Coffee Might Trigger First Heart Attack in Some

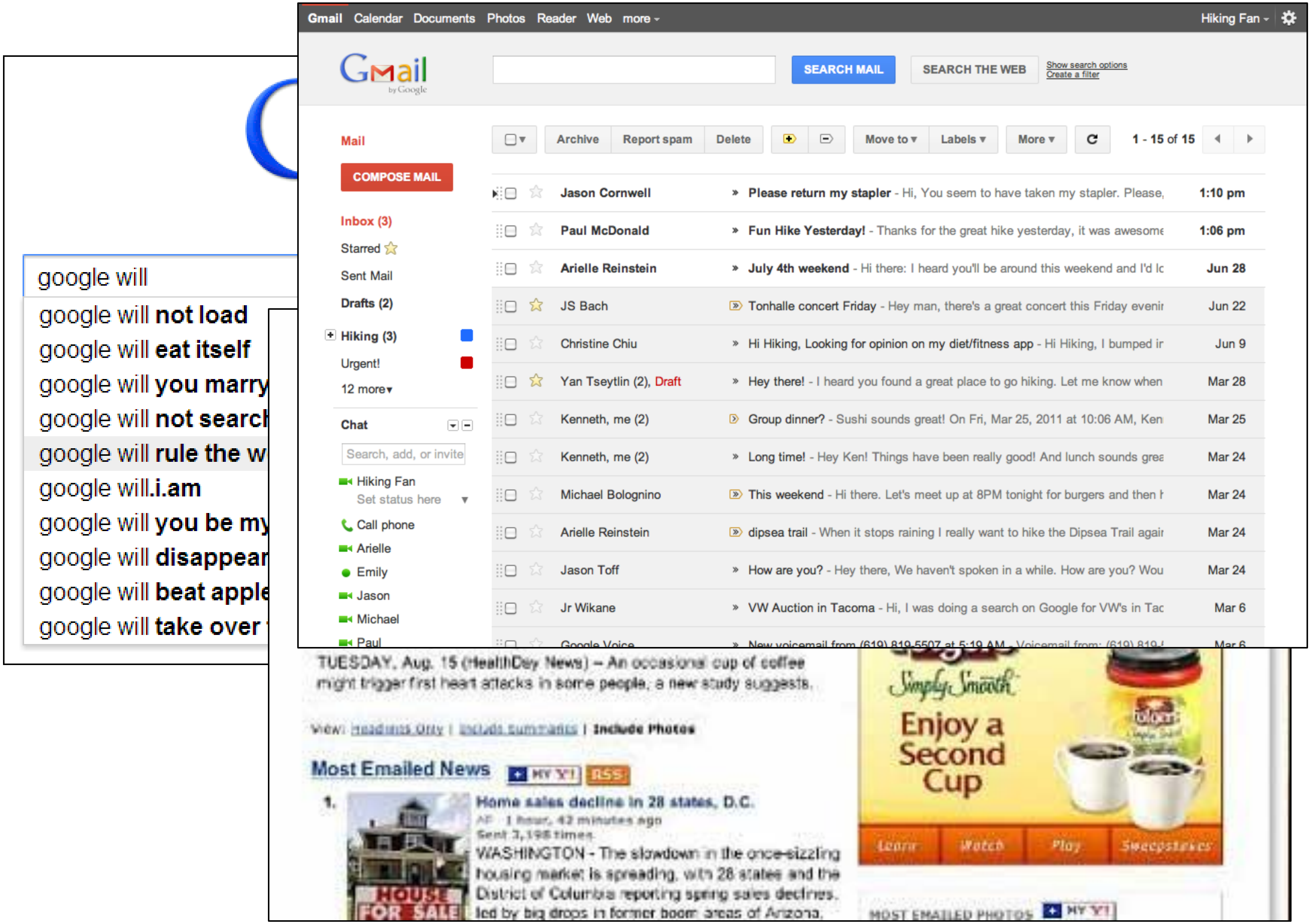
HealthDay - 1 hour, 1 minute ago

TUESDAY, Aug. 15 (HealthDay News) – An occasional cup of coffee might trigger first heart attacks in some people, a new study suggests.

View: Headlines Only | Include Summaries | **Include Photos**

Most Emailed News

1. **Home sales decline in 28 states, D.C.**
   AP - 1 hour, 42 minutes ago
   Sent 3,198 times
   WASHINGTON - The slowdown in the once-sizzling housing market is spreading, with 28 states and the District of Columbia reporting spring sales declines, led by big drops in former boom areas of Arizona,



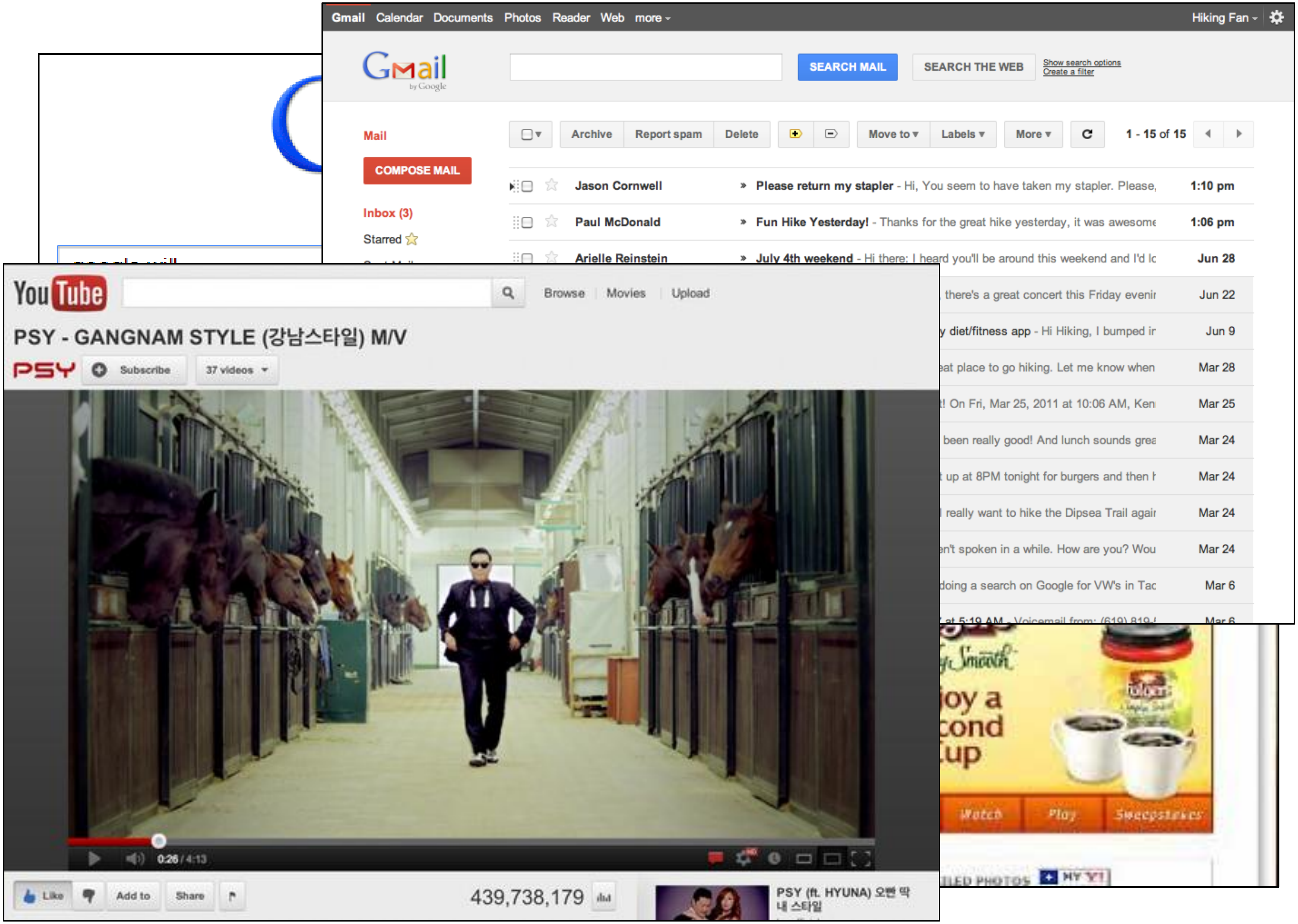
google will

google will not load
google will eat itself
google will you marry
google will not search
google will rule the w
google will.i.am
google will you be my
google will disappear
google will beat apple
google will take over

Jason Cornwell	**Please return my stapler** - Hi, You seem to have taken my stapler. Please,	1:10 pm
Paul McDonald	**Fun Hike Yesterday!** - Thanks for the great hike yesterday, it was awesome	1:06 pm
Arielle Reinstein	**July 4th weekend** - Hi there: I heard you'll be around this weekend and I'd lc	Jun 28
JS Bach	Tonhalle concert Friday - Hey man, there's a great concert this Friday evenir	Jun 22
Christine Chiu	Hi Hiking, Looking for opinion on my diet/fitness app - Hi Hiking, I bumped ir	Jun 9
Yan Tseytlin (2), Draft	Hey there! - I heard you found a great place to go hiking. Let me know when	Mar 28
Kenneth, me (2)	Group dinner? - Sushi sounds great! On Fri, Mar 25, 2011 at 10:06 AM, Ken	Mar 25
Kenneth, me (2)	Long time! - Hey Ken! Things have been really good! And lunch sounds grea	Mar 24
Michael Bolognino	This weekend - Hi there. Let's meet up at 8PM tonight for burgers and then I	Mar 24
Arielle Reinstein	dipsea trail - When it stops raining I really want to hike the Dipsea Trail agair	Mar 24
Jason Toff	How are you? - Hey there, We haven't spoken in a while. How are you? Wou	Mar 24
Jr Wikane	VW Auction in Tacoma - Hi, I was doing a search on Google for VW's in Tac	Mar 6
Google Voice	New voicemail from (619) 819-5507 at 5:19 AM - Voicemail from: (619) 819-!	Mar 6

TUESDAY, Aug. 15 (HealthDay News) -- An occasional cup of coffee might trigger first heart attacks in some people, a new study suggests.

1. Home sales decline in 28 states, D.C.
AP - 1 hour, 42 minutes ago
Sent 3,198 times
WASHINGTON - The slowdown in the once-sizzling housing market is spreading, with 28 states and the District of Columbia reporting spring sales declines, led by big drops in former boom areas of Arizona,



Jason Cornwell » **Please return my stapler** - Hi, You seem to have taken my stapler. Please, 1:10 pm

Paul McDonald » **Fun Hike Yesterday!** - Thanks for the great hike yesterday, it was awesome 1:06 pm

Arielle Reinstein » **July 4th weekend** - Hi there: I heard you'll be around this weekend and I'd lc Jun 28

there's a great concert this Friday evenir Jun 22

y diet/fitness app - Hi Hiking, I bumped ir Jun 9

eat place to go hiking. Let me know when Mar 28

! On Fri, Mar 25, 2011 at 10:06 AM, Ken Mar 25

been really good! And lunch sounds grea Mar 24

t up at 8PM tonight for burgers and then I Mar 24

I really want to hike the Dipsea Trail agair Mar 24

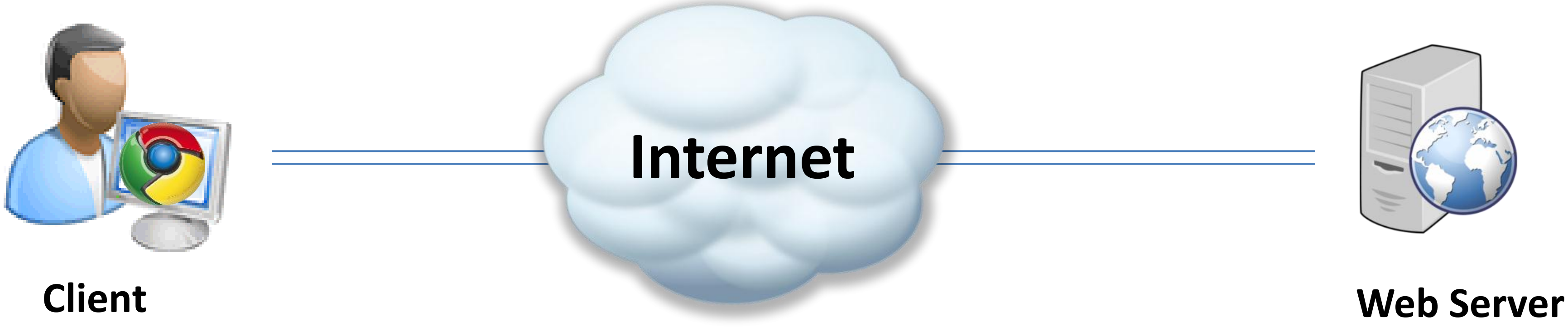
en't spoken in a while. How are you? Wou Mar 24

doing a search on Google for VW's in Tac Mar 6

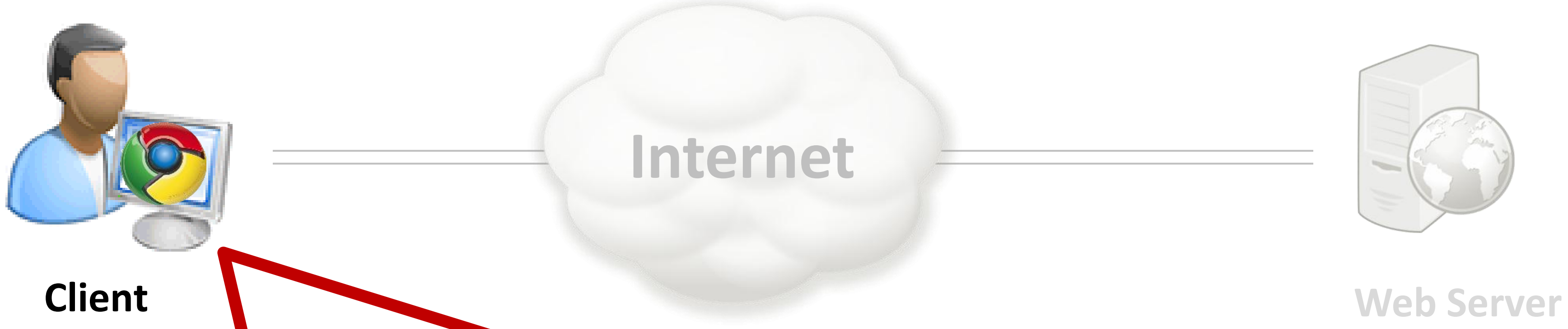
PSY - GANGNAM STYLE (강남스타일) M/V

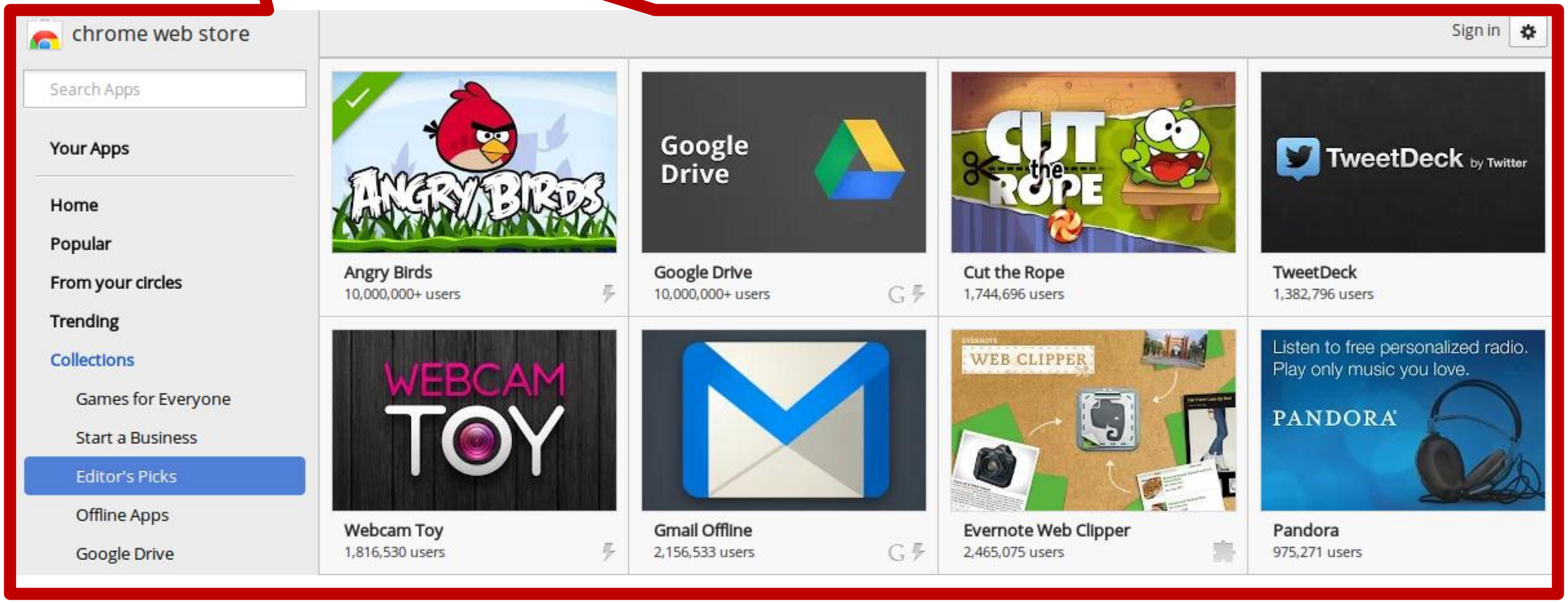
Gmail
Calendar
Documents
Photos
Reader
Web
more
Hiking Fan
Gmail by Google
SEARCH MAIL
SEARCH THE WEB
Show search options
Create a filter
Mail
Archive
Report spam
Delete
Move to
Labels
More
1 - 15 of 15
1:10 pm
1:06 pm
Jun 28
Jun 22
Jun 9
Mar 28
Mar 25
Mar 24
Mar 24
Mar 24
Mar 24
Mar 6
ANGRY BIRDS
BETA
PLAY
YouTube
PSY - GANGNAM ST
PSY
Subscribe
0:26 / 4:13
Like
Add to
Share
439,738,179
PSY (ft. HYUNA) 오빤 딱 내 스타일

Web platform extensibility



Web platform extensibility




chrome web store

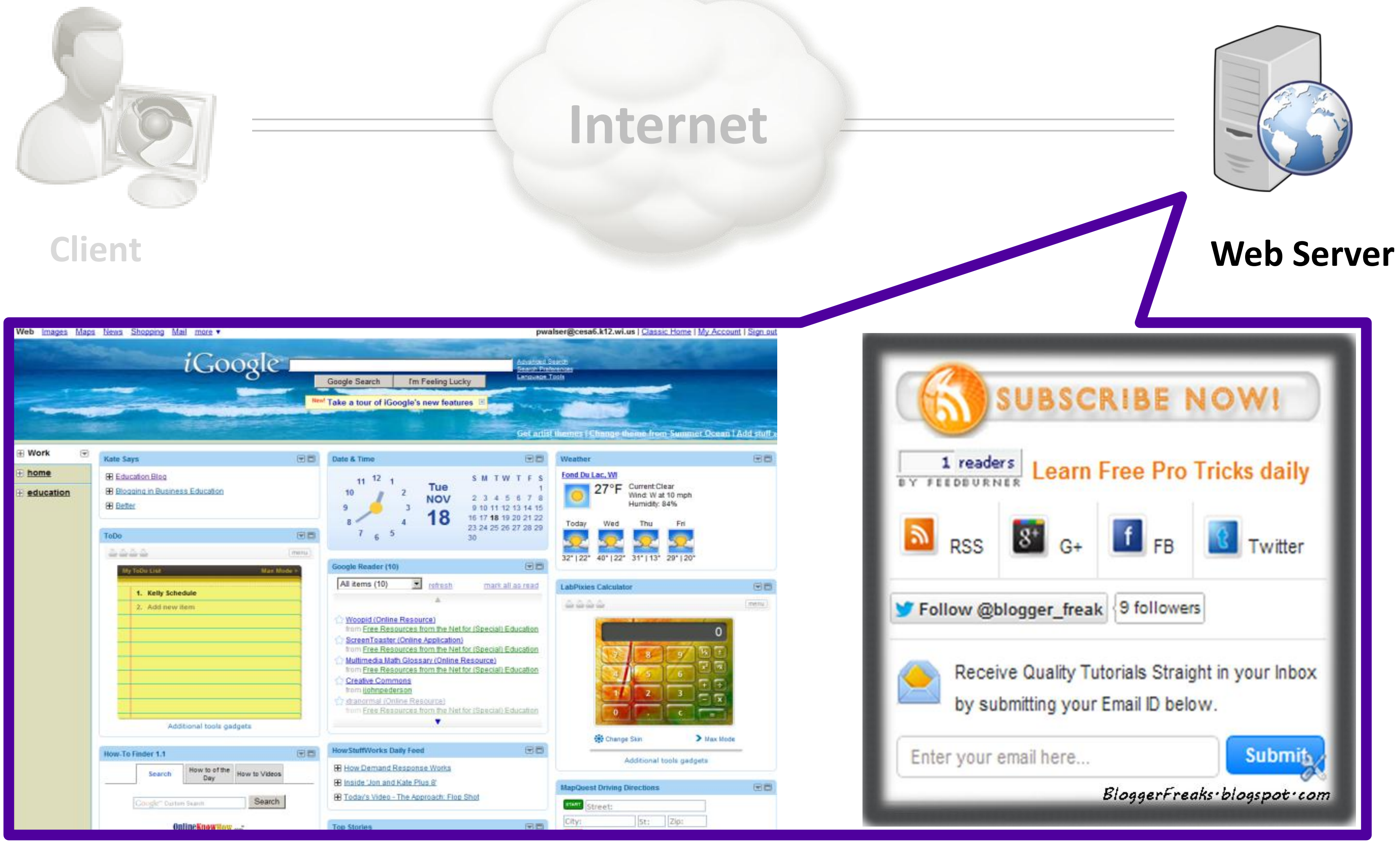
Search Apps

Sign in

- Your Apps
- Home
- Popular
- From your circles
- Trending
- Collections
  - Games for Everyone
  - Start a Business
  - Editor's Picks
  - Offline Apps
  - Google Drive

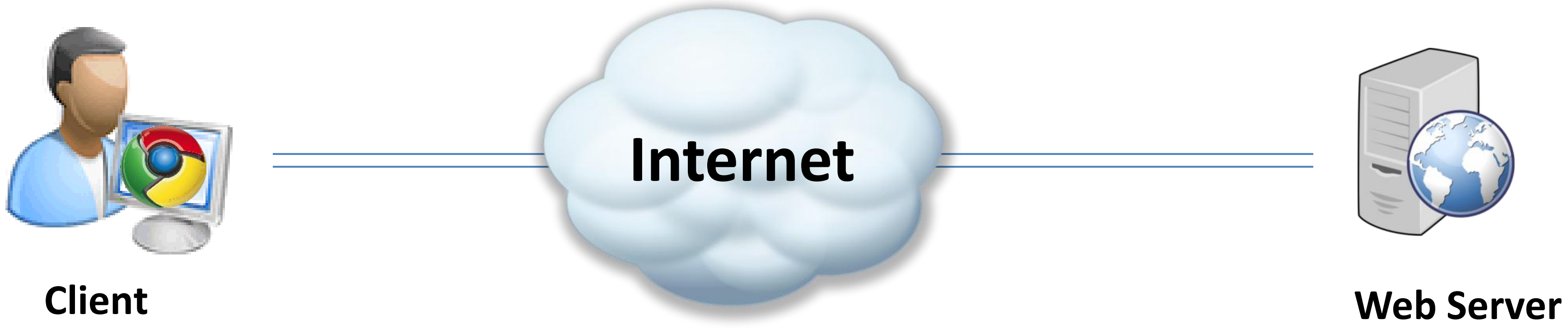
Angry Birds 10,000,000+ users	Google Drive 10,000,000+ users	Cut the Rope 1,744,696 users	TweetDeck 1,382,796 users
Webcam Toy 1,816,530 users	Gmail Offline 2,156,533 users	Evernote Web Clipper 2,465,075 users	Pandora 975,271 users

Web platform extensibility



Receive Quality Tutorials Straight in your Inbox by submitting your Email ID below.

Web platform extensibility

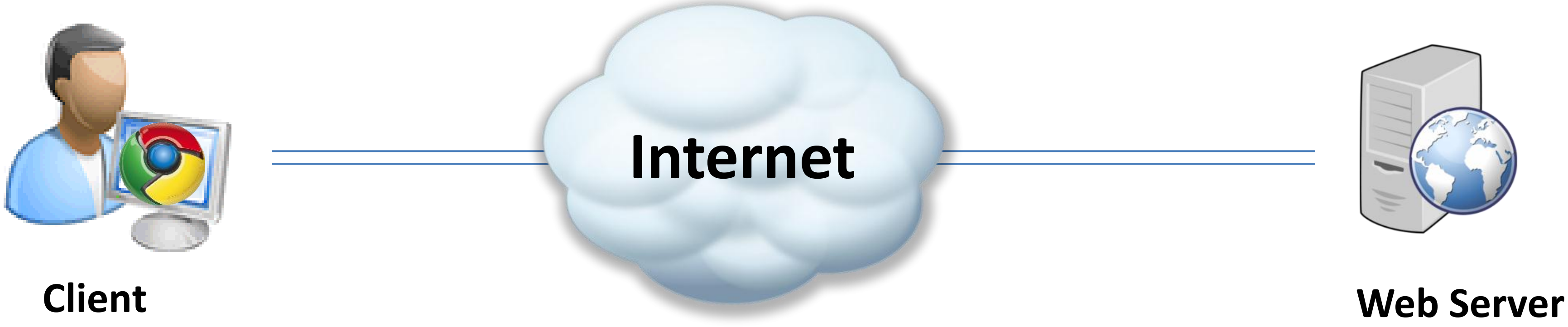


Client

Internet

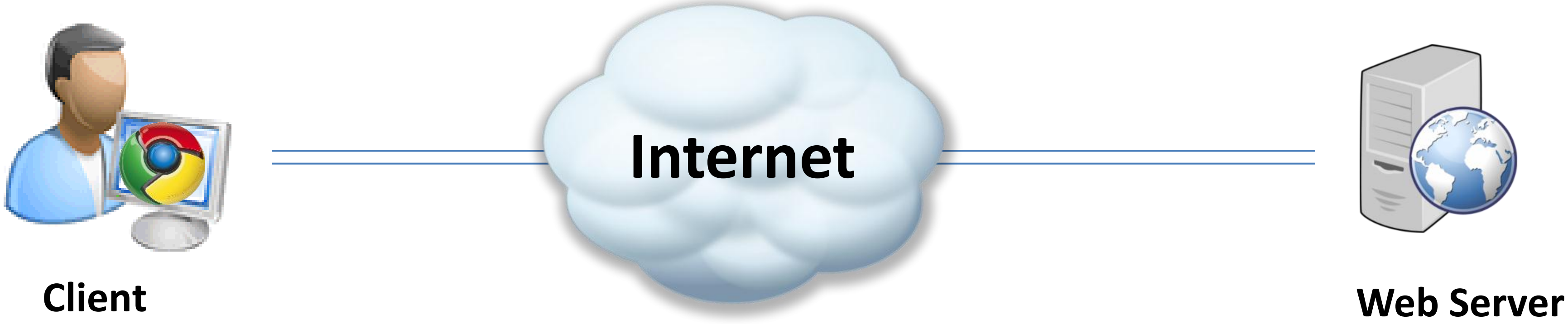
Web Server

Web platform extensibility



Web browser and Web application extensibility are complementary

Web platform extensibility

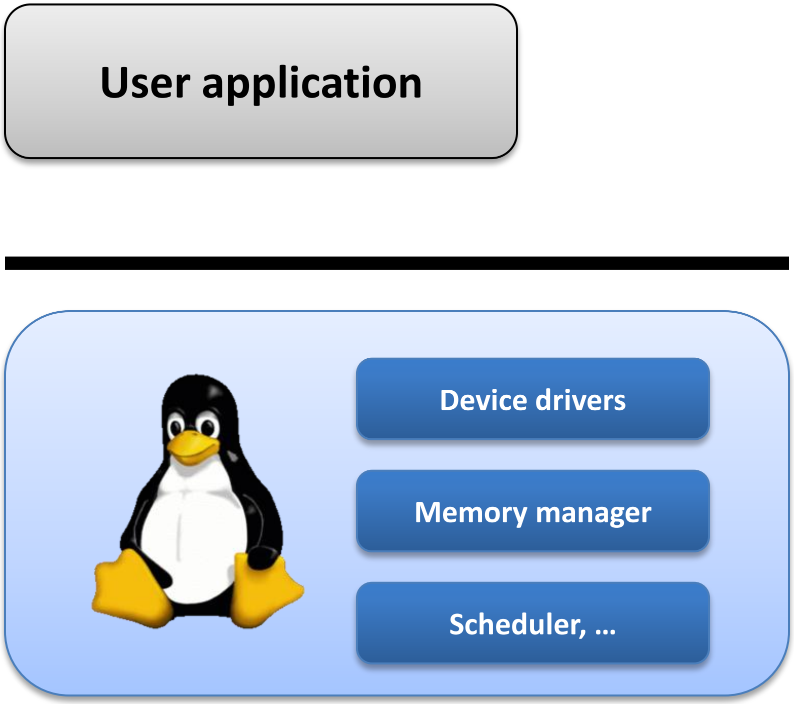


Web browser and Web application extensibility are complementary

Client-hosted Web applications can enhance Web browser functionality

Browser extensions can enhance Web application functionality

An operating systems analogy



User application

Device drivers

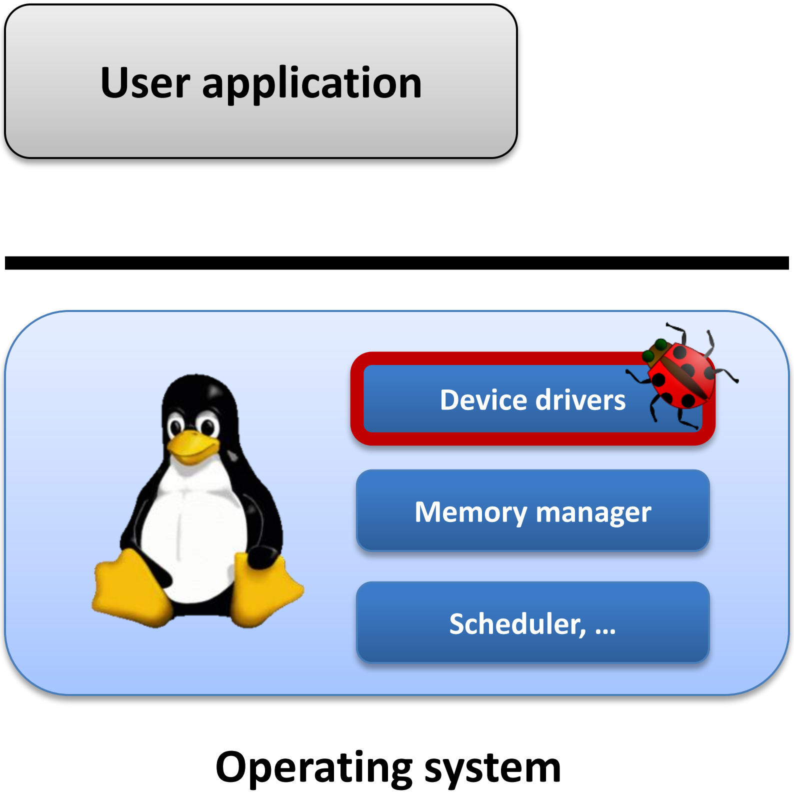
Memory manager

Scheduler, …

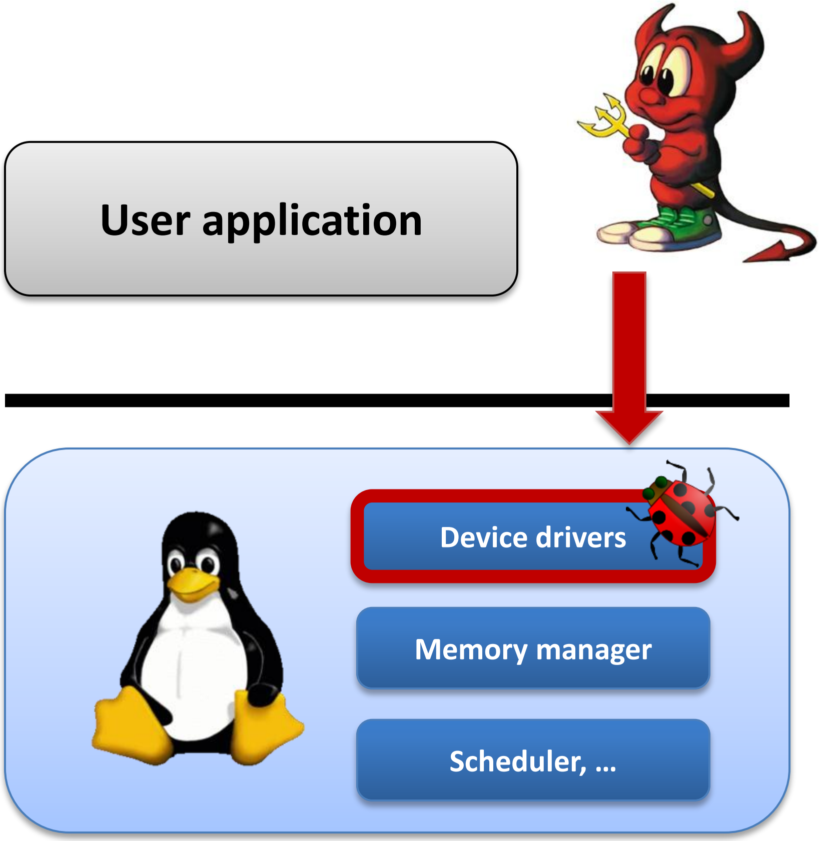
Operating system

Problems with OS extensibility (I)

Problem: Buggy & vulnerable drivers



Problems with OS extensibility (I)



User application

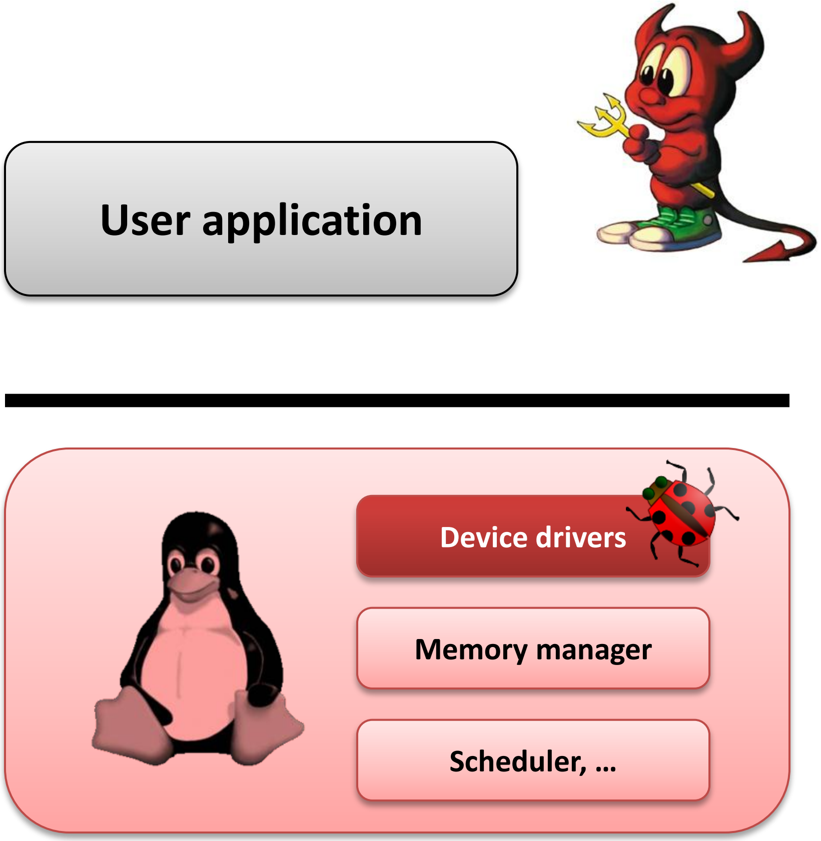
Device drivers

Memory manager

Scheduler, …

Operating system

Problems with OS extensibility (I)



User application

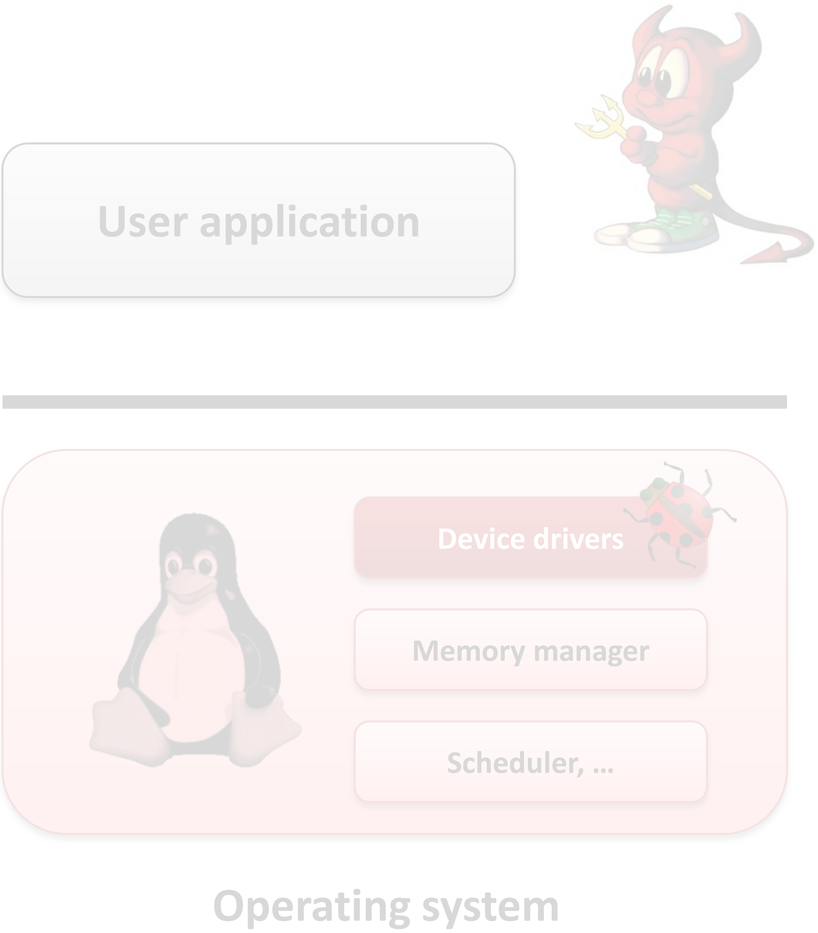
Device drivers

Memory manager

Scheduler, …

Operating system

Problems with OS extensibility (I)



Some solutions

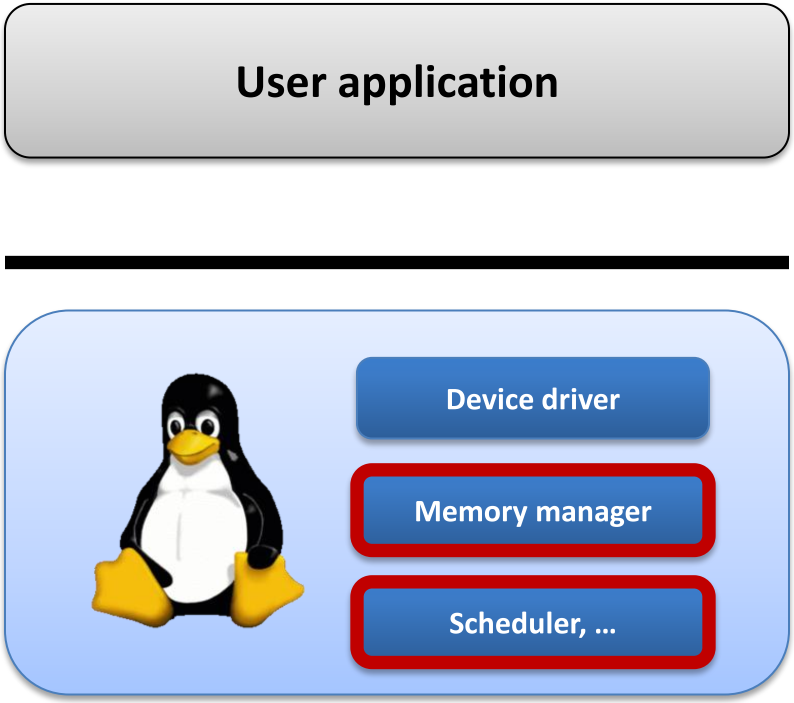
1) SPIN [SOSP'95]
Key idea: Language-based safety

2) VINO [OSDI'96]
Key idea: SFI + Lightweight transactions

3) Nooks [SOSP'03]
Key idea: Lightweight protection domains

Problems with OS extensibility (II)

Problem: OS bloat, rigid interfaces

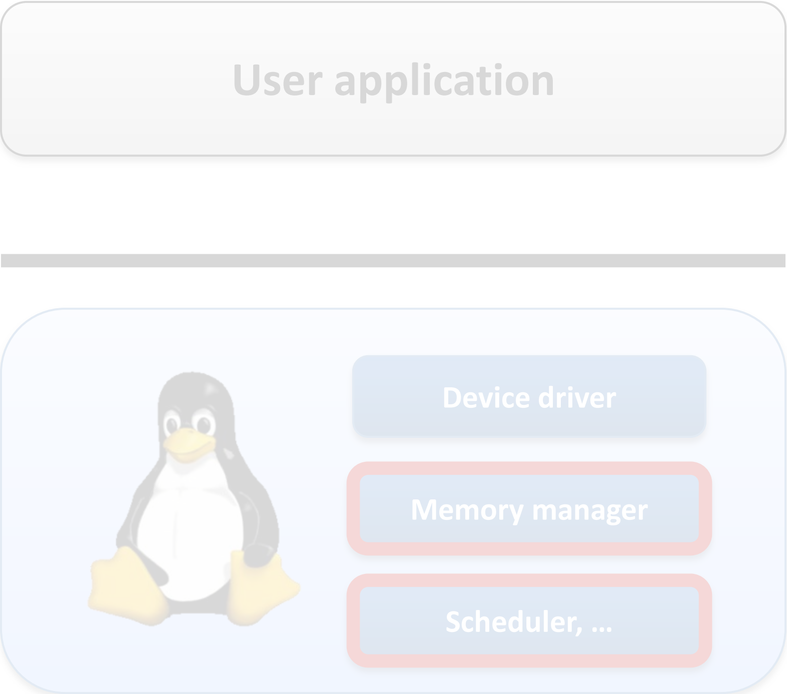

User application

Device driver

Memory manager

Scheduler, …

Problems with OS extensibility (II)

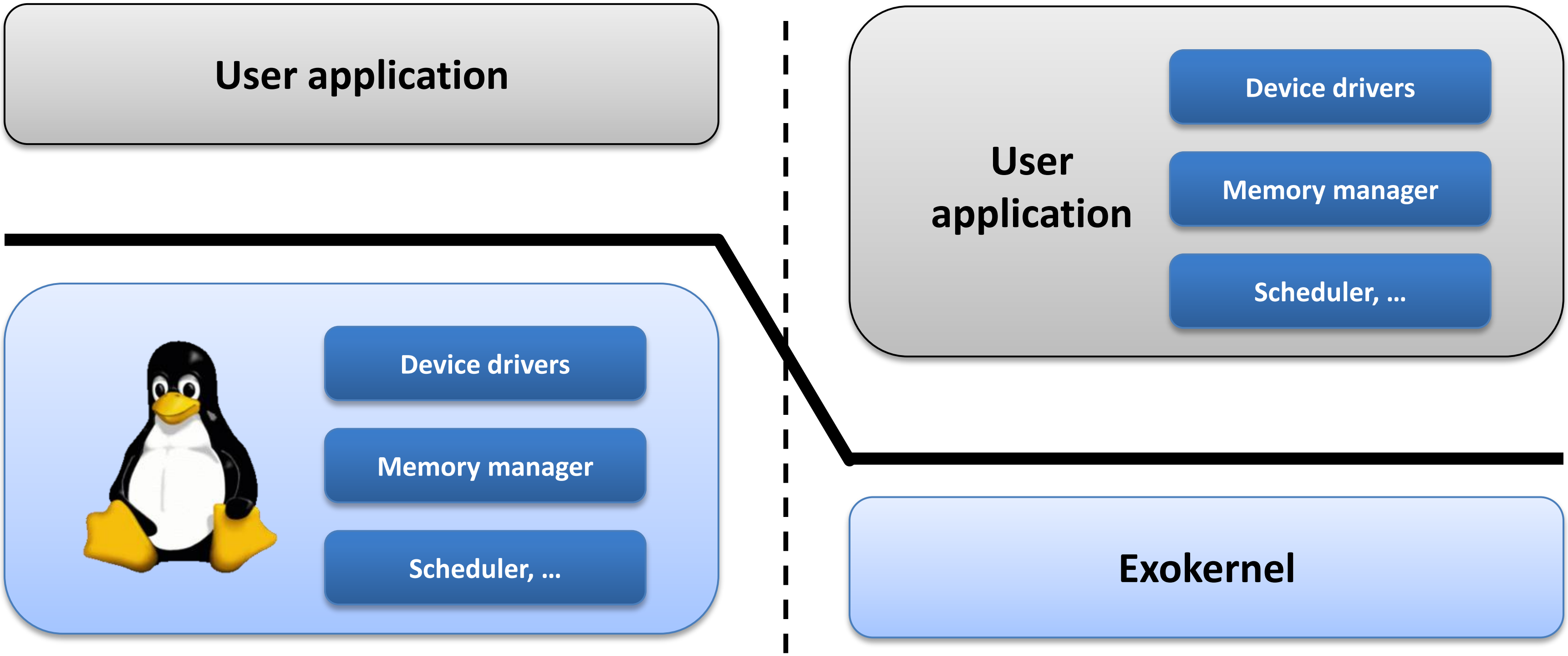


Solution

Exokernel **[SOSP’95]**

Key idea: **Applications manage complexity**

Exokernel operating system



User application

Device drivers

Memory manager

Scheduler, …

User application

Device drivers

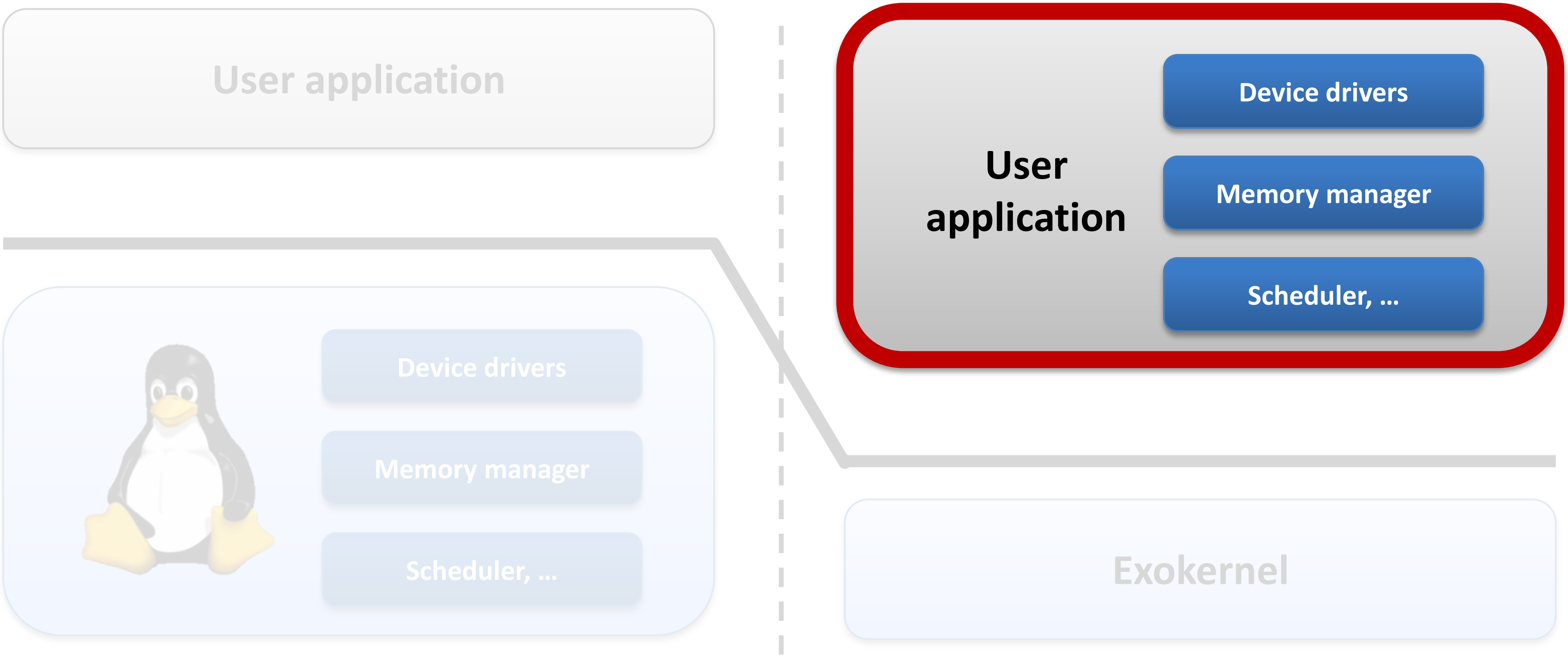
Memory manager

Scheduler, …

Exokernel

Exokernel operating system

User application manages complexity



My thesis

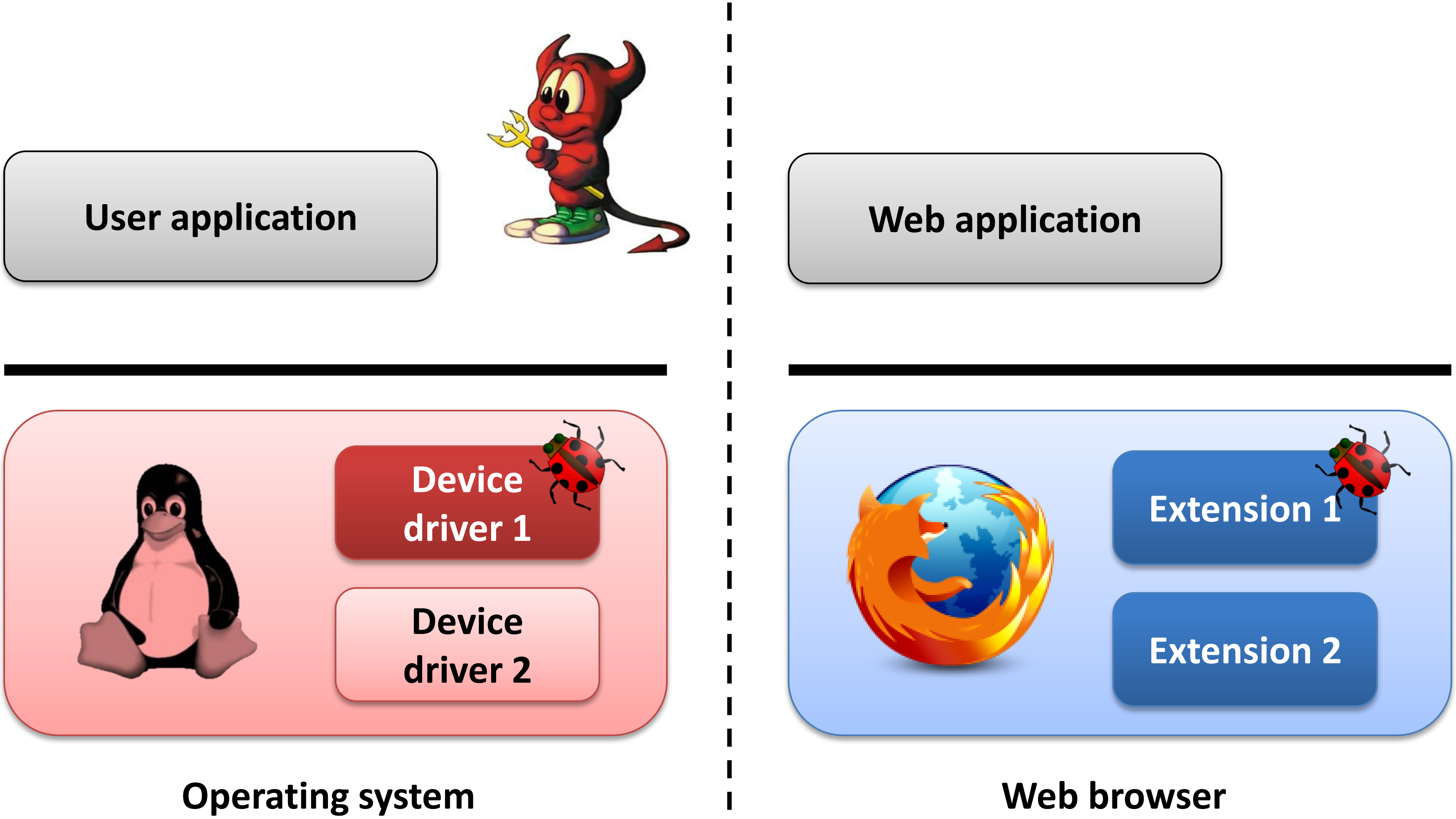
We can leverage operating system principles to secure and enhance the extensibility of the Web platform

Contributions

- **Characterizing extensibility issues in web browsers**
  - Analyzed the nature of information flow in JavaScript-based web browser extensions **[ACSAC’09** , **ECOOP’12a]**
- **Extensibility as a *language* and *system* primitive**
  - Designed and implemented a language runtime system to secure web application extensibility **[PLAS’10**, **ECOOP’12b]**
  - Built a novel browser architecture that enables applications to leverage extensibility for security and robustness **[SOSP’11]**

Part I: Securing Web platform extensions with Sabre and Transcript

Analogy: OS extensions



User application

Web application

Device driver 1

Device driver 2

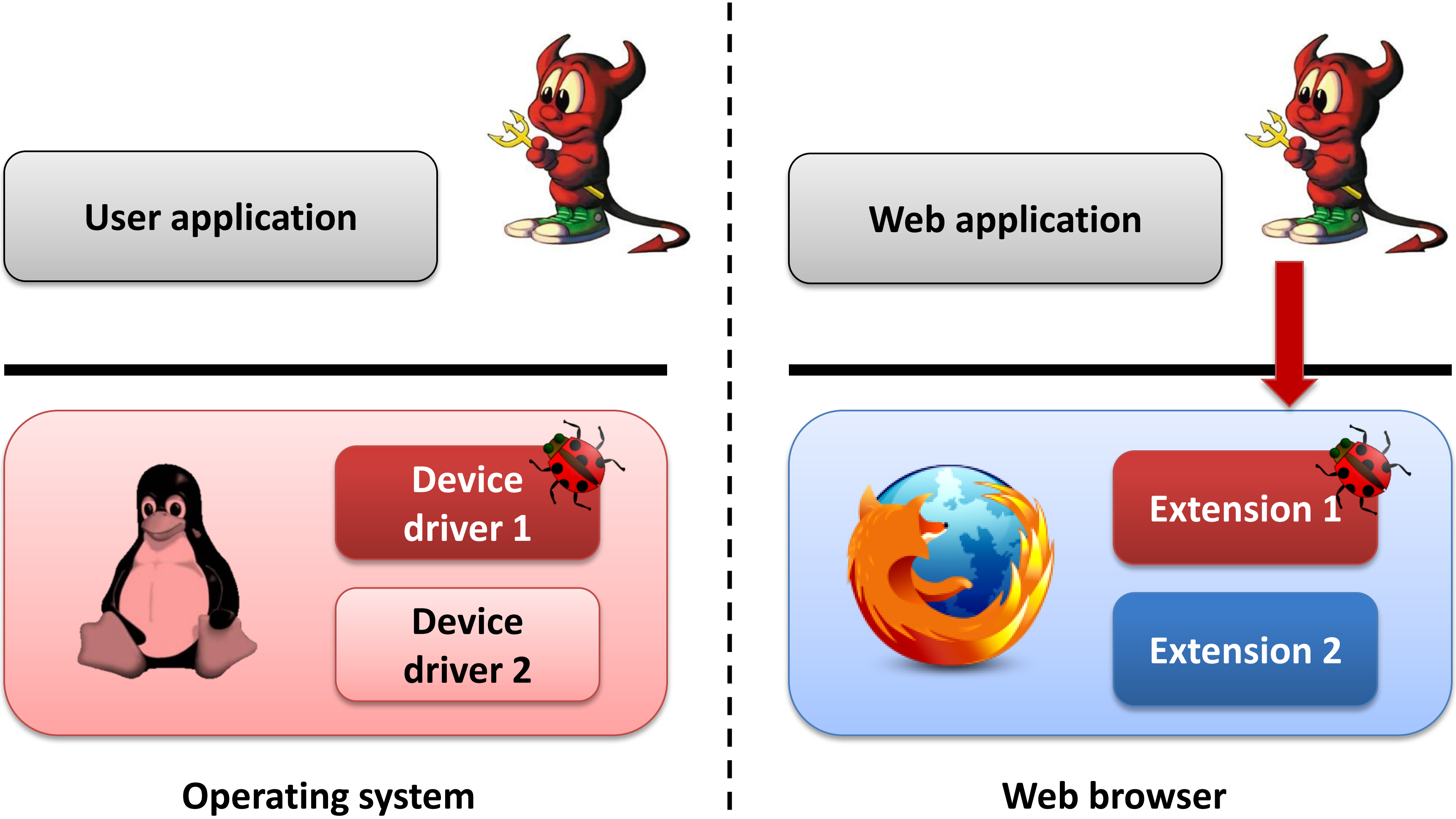
Extension 1

Extension 2

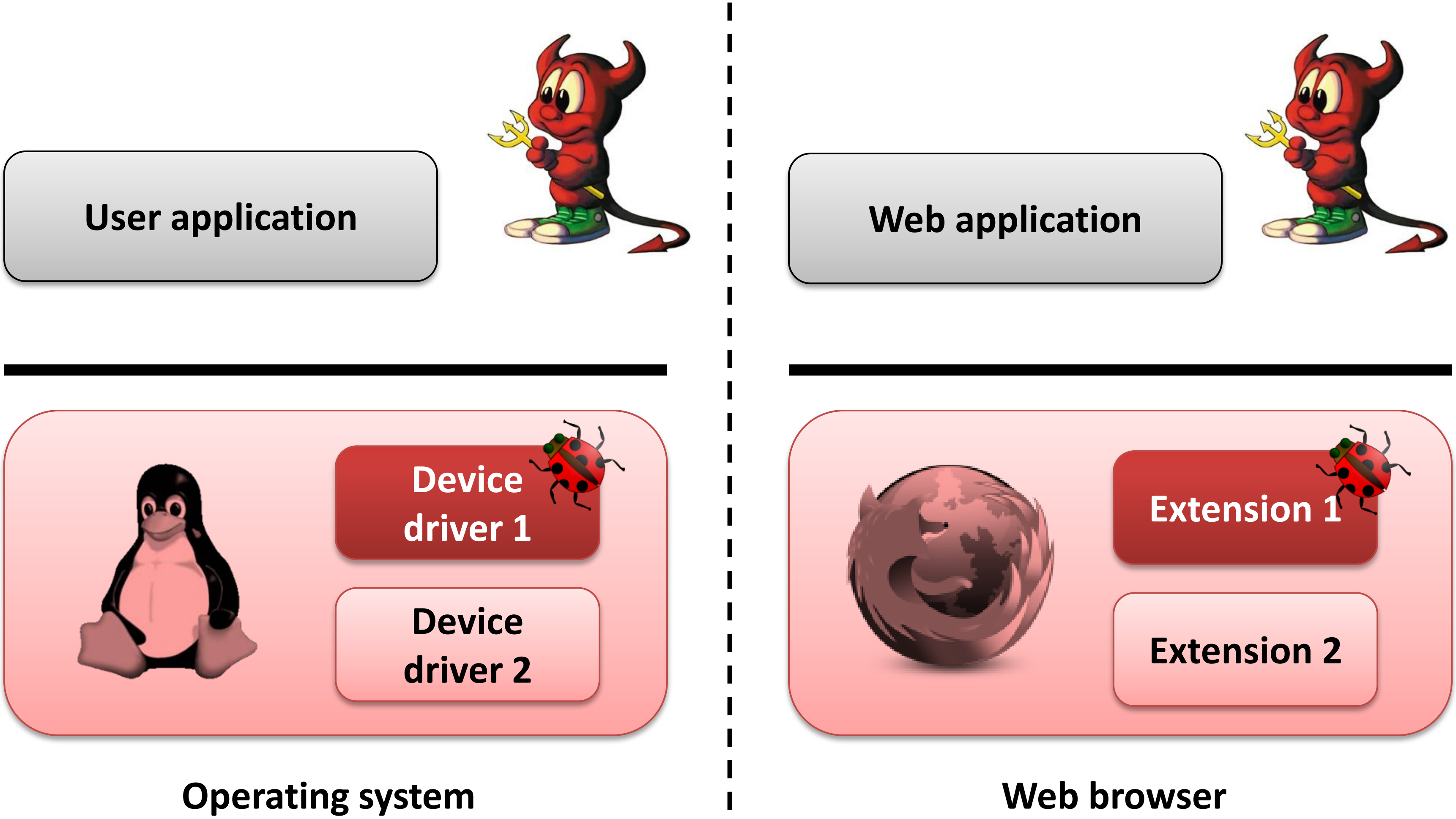
Operating system

Web browser

Analogy: OS extensions



Analogy: OS extensions



User application

Web application

Device driver 1

Device driver 2

Extension 1

Extension 2

Operating system

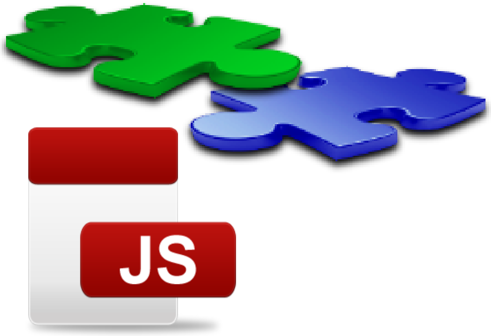
Web browser

Extensibility with vulnerability ?

CVE-2013-0422,
CVE-2011-0873,
CVE-2011-0871,
CVE-2011-0862,
CVE-2011-0815,
CVE-2011-0814,
…

CVE-2011-2425,
CVE-2011-2424,
CVE-2011-2417,
CVE-2011-2416,
CVE-2011-2415,
CVE-2011-2414,
…

CVE-2012-2990,
CVE-2010-4597,
CVE-2010-4588,
CVE-2010-3973,
CVE-2010-2888,
CVE-2009-3737,
…



CVE-2012-2877,
CVE-2012-0958,
CVE-2011-3647,
CVE-2011-3001,
CVE-2011-1812,
CVE-2011-2785,
…

Extensibility with vulnerability ?

CVE-2013-0422,
CVE-2011-0873,
CVE-2011-0871,

CVE-2012-2990,
CVE-2010-4597,
CVE-2010-4588,
CVE-2010-3973,
CVE-2010-2888,
CVE-2009-3737,
…

CVE-2011-2425,
CVE-2011-2424,
CVE-2011-2417,

CVE-2012-2877,
CVE-2012-0958,
CVE-2011-3647,
CVE-2011-3001,
CVE-2011-1812,
CVE-2011-2785,
…

Arbitrary code execution, privilege escalation, denial of service, etc.

JavaScript-based extensions

Web browser extensions

Web application extensions

Extensions run with privileges of the hosting principal

JavaScript-based extensions

Web browser extensions

Web application extensions

Cookies

Browsing History

Preferences

Passwords

Network

File System

Operating System

JavaScript-based extensions

Web browser extensions

Web application extensions

Cookies

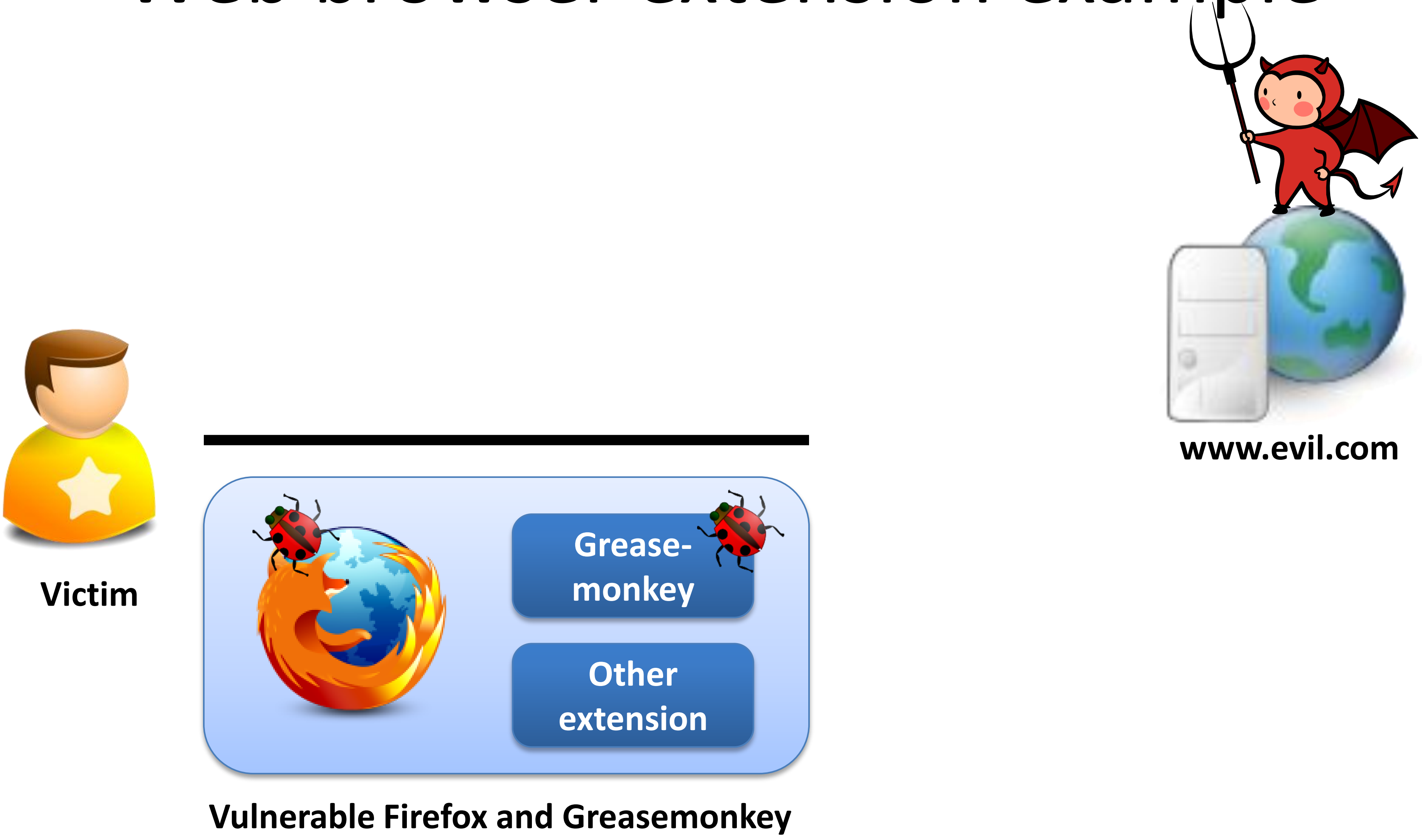
Local Storage

Application Data

Keyboard and
Mouse Events

AJAX

Web browser extension example



www.evil.com

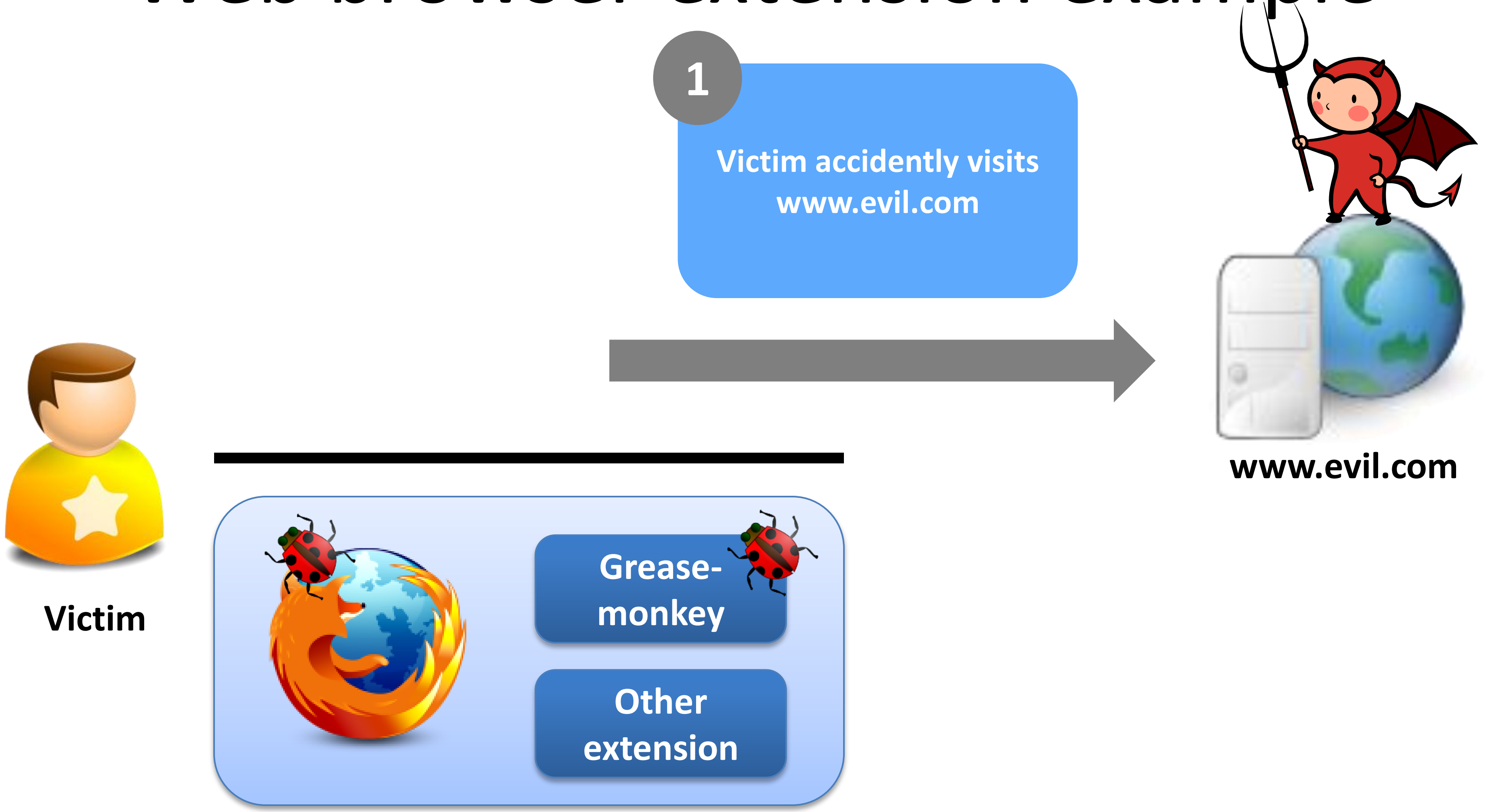
Victim

Grease-monkey

Other extension

Vulnerable Firefox and Greasemonkey

Web browser extension example



1

Victim accidently visits www.evil.com

www.evil.com

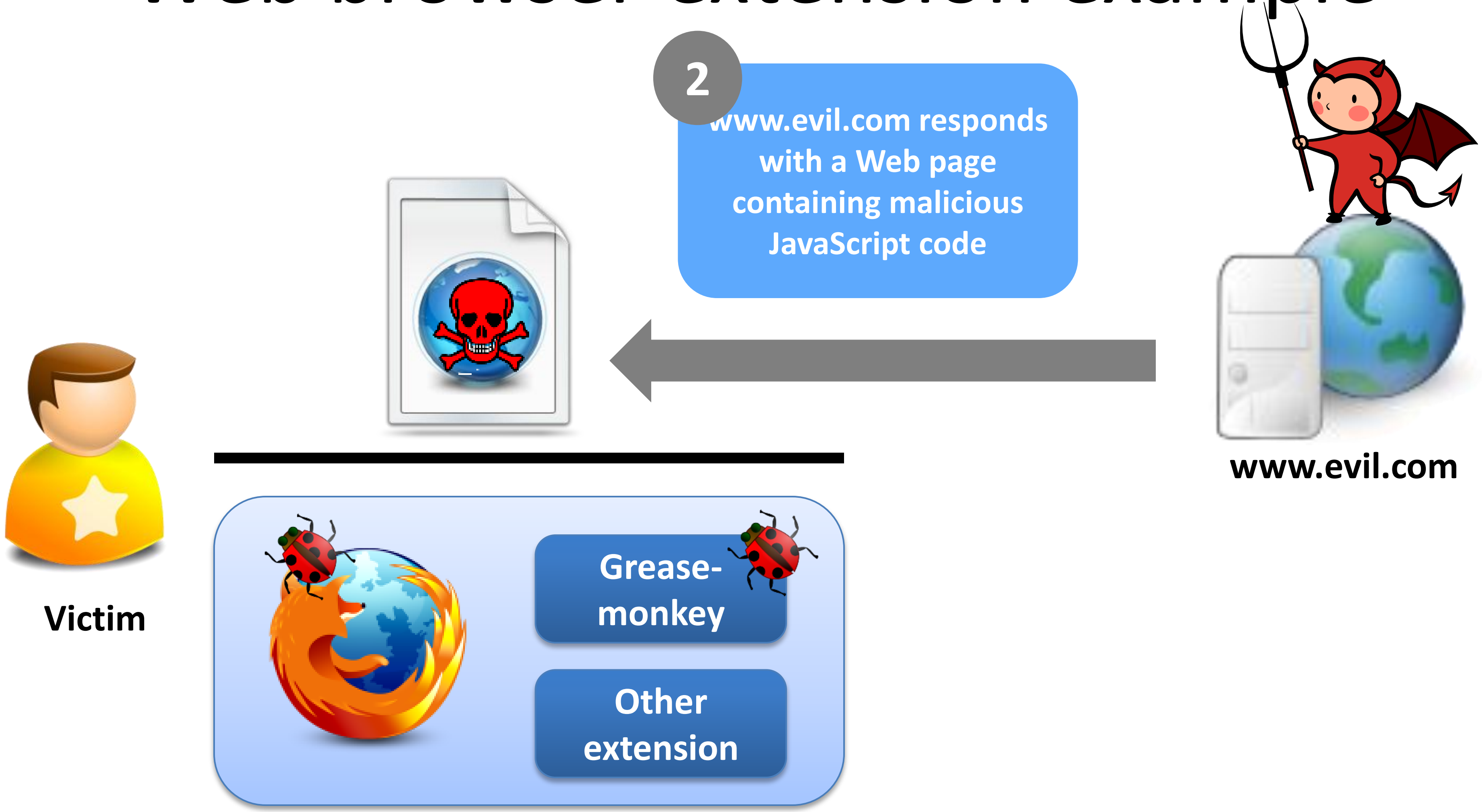
Victim

Grease-monkey

Other extension

Vulnerable Firefox and Greasemonkey

Web browser extension example



2

www.evil.com responds with a Web page containing malicious JavaScript code

www.evil.com

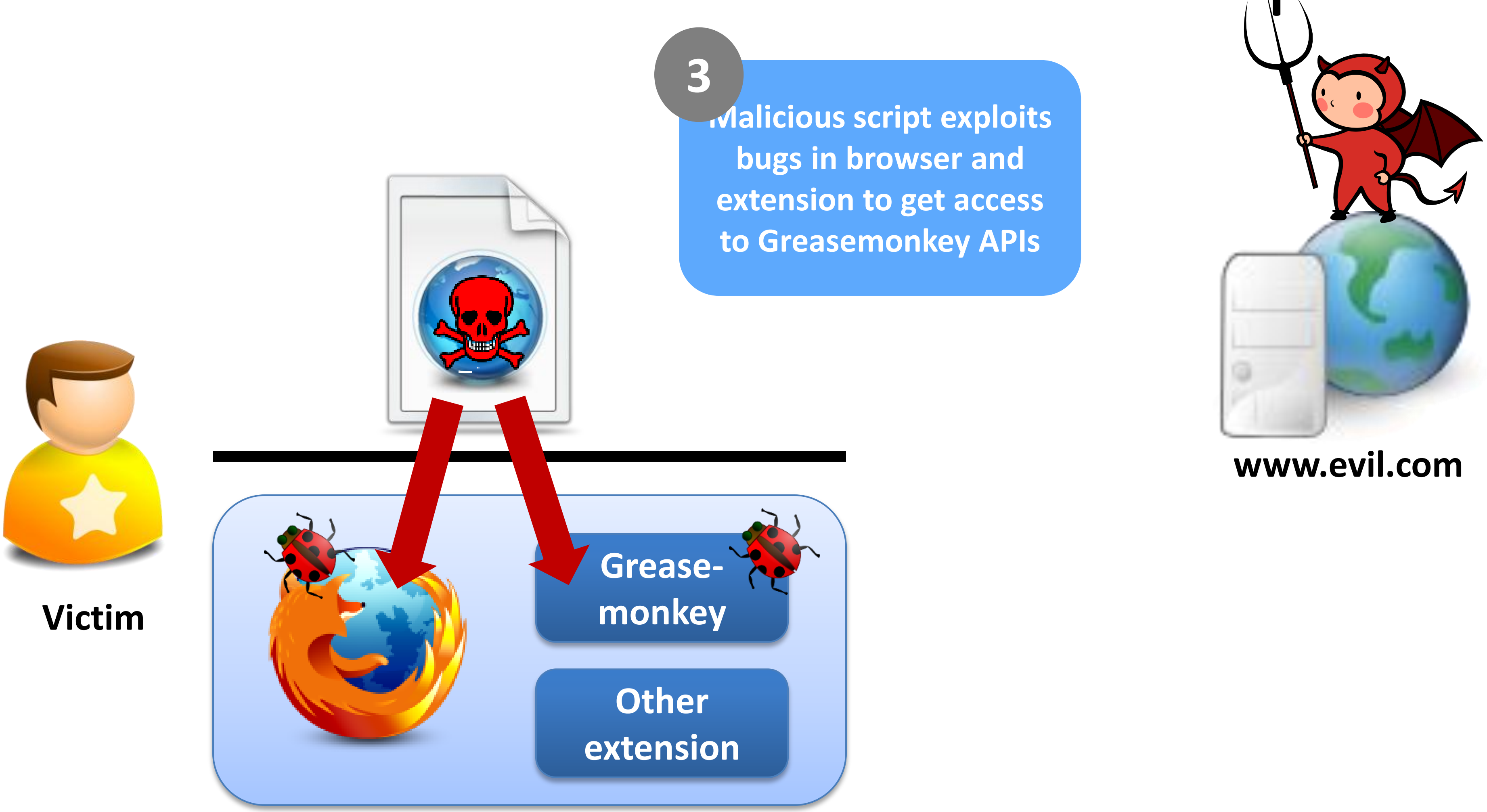
Victim

Grease-monkey

Other extension

Vulnerable Firefox and Greasemonkey

Web browser extension example



3

Malicious script exploits bugs in browser and extension to get access to Greasemonkey APIs

Victim

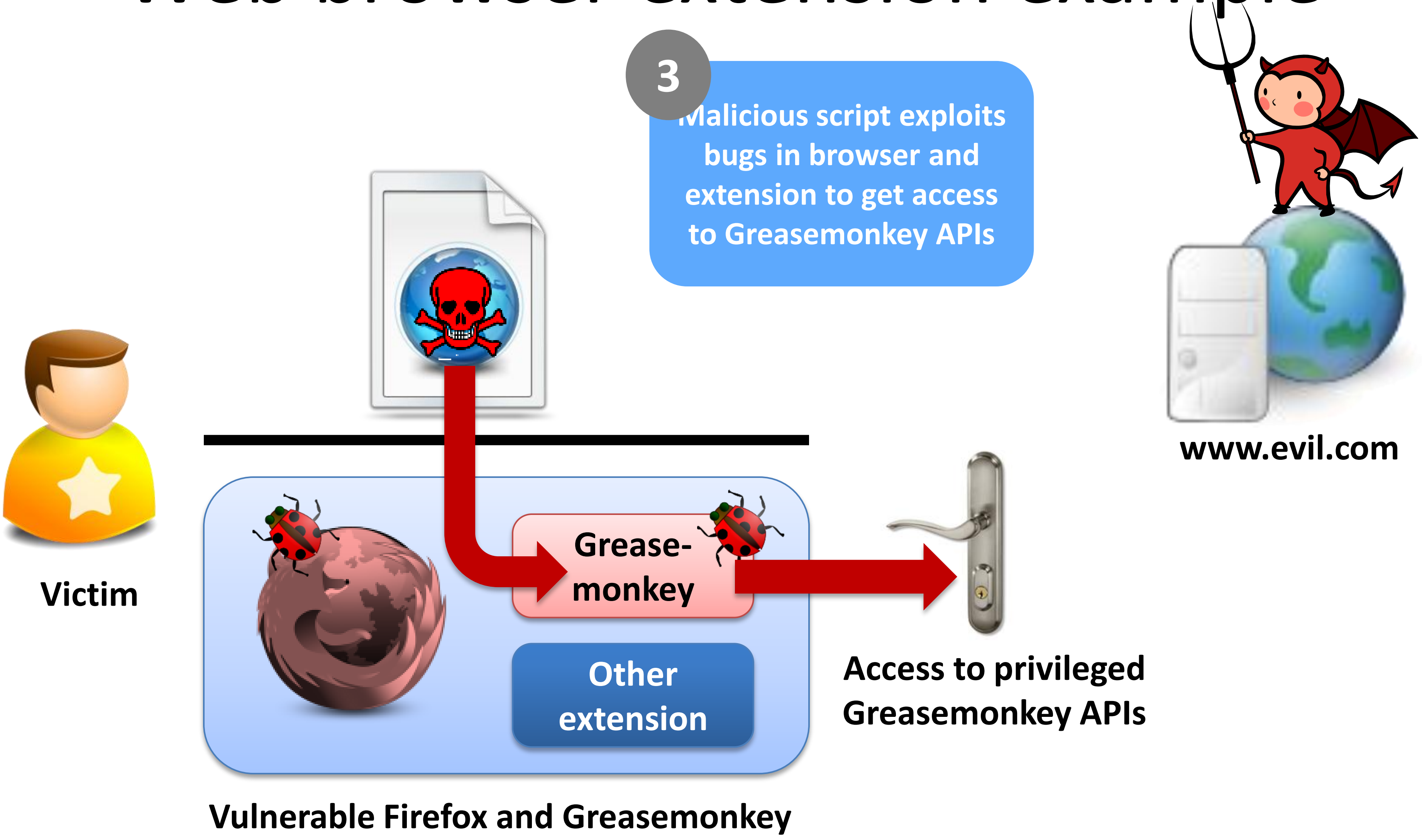
Grease-monkey

Other extension

www.evil.com

Vulnerable Firefox and Greasemonkey

Web browser extension example



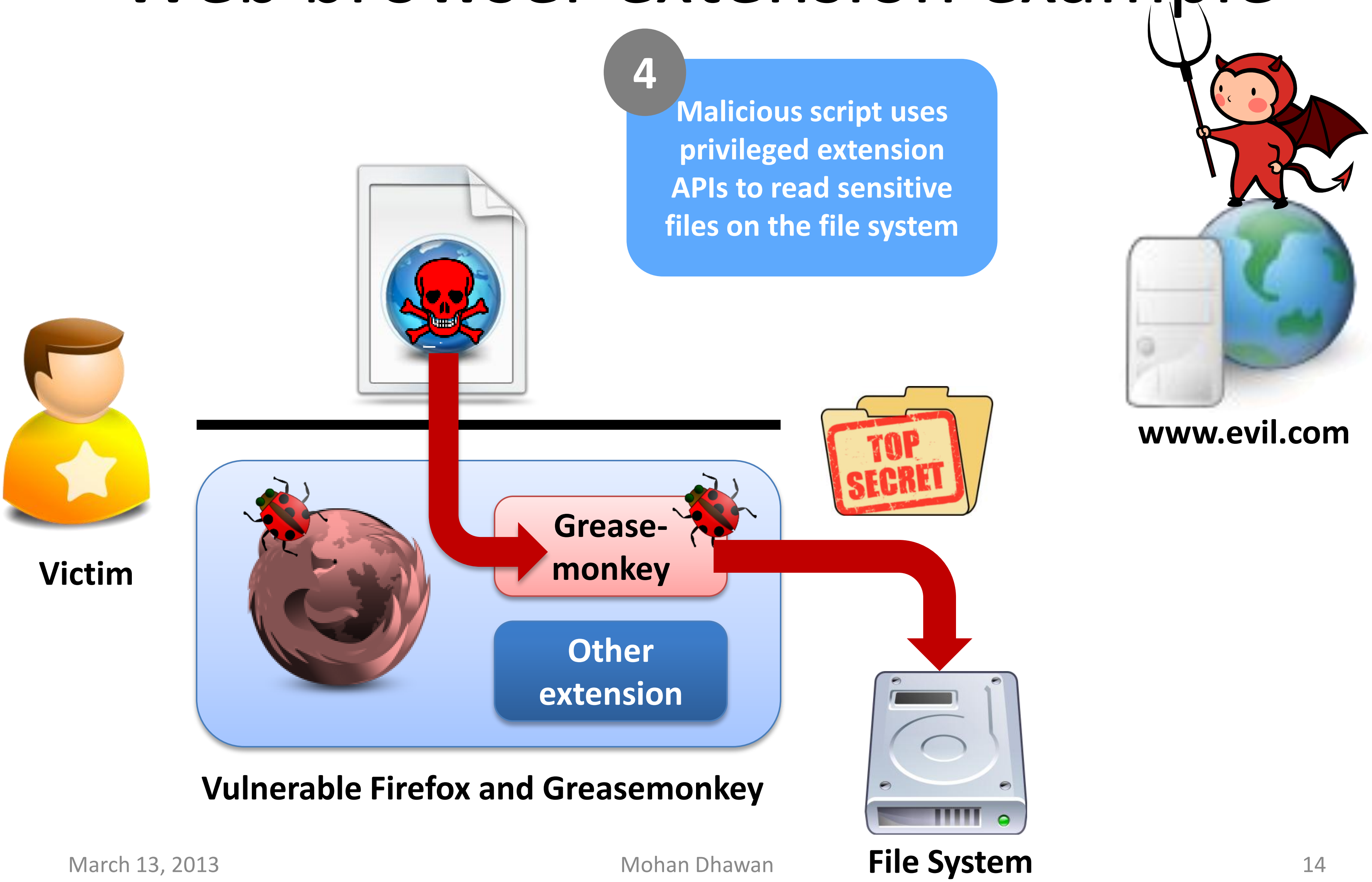
3

Malicious script exploits bugs in browser and extension to get access to Greasemonkey APIs

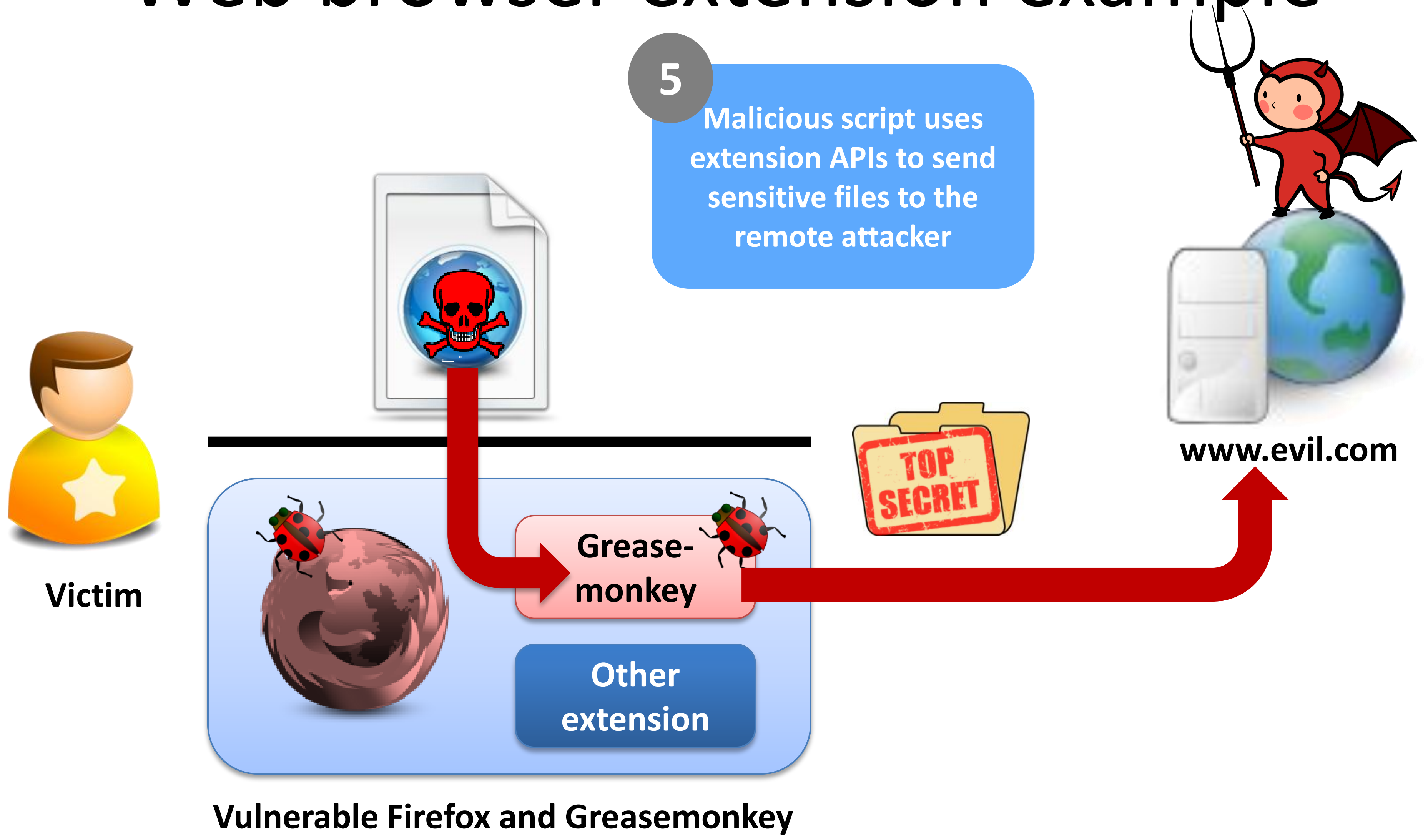
Access to privileged Greasemonkey APIs

Vulnerable Firefox and Greasemonkey

Web browser extension example


4
Malicious script uses privileged extension APIs to read sensitive files on the file system
www.evil.com
TOP SECRET
Victim
Grease-monkey
Other extension
Vulnerable Firefox and Greasemonkey
File System

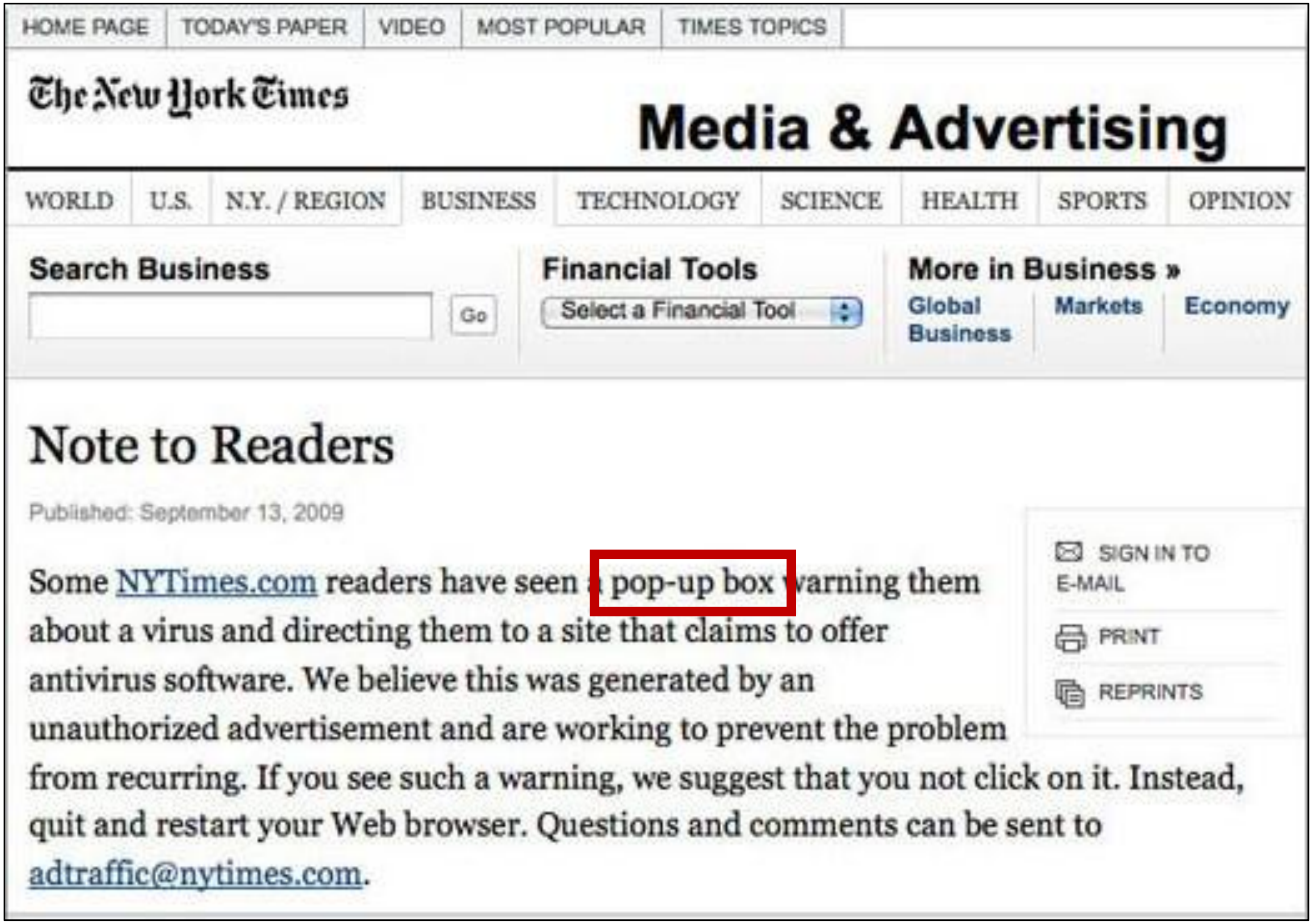
Web browser extension example



5 Malicious script uses extension APIs to send sensitive files to the remote attacker

Vulnerable Firefox and Greasemonkey

Web application extension example



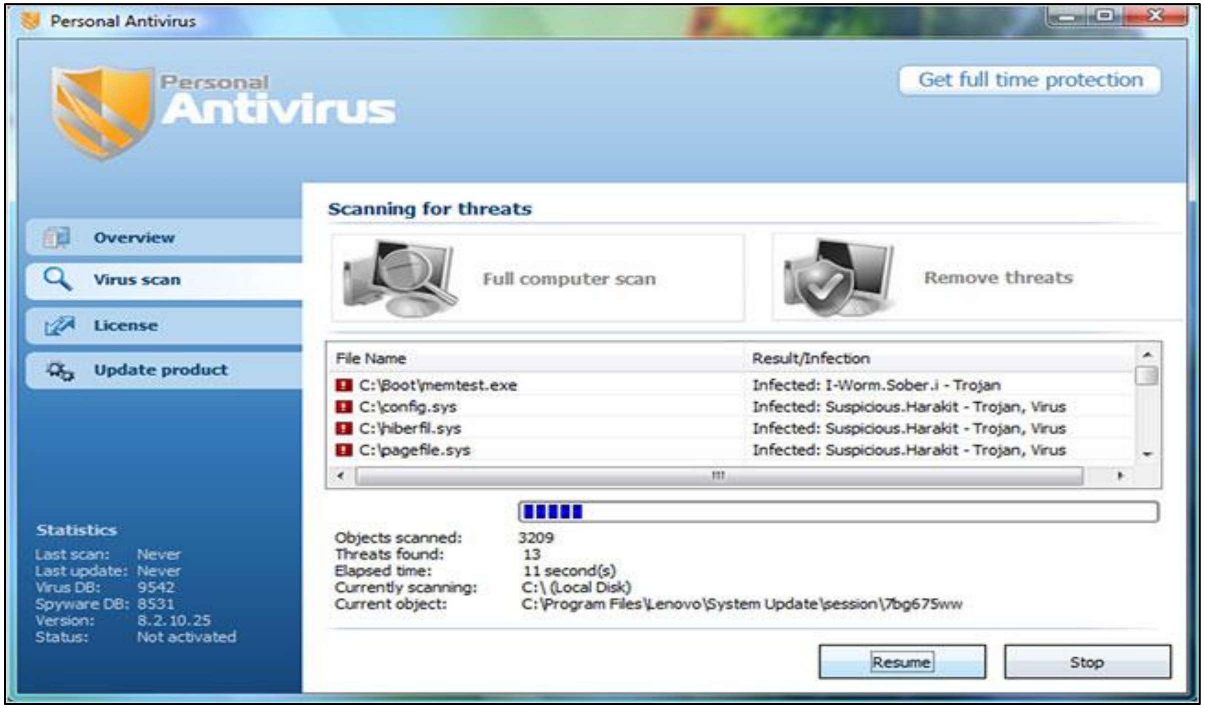
Note to Readers

Published: September 13, 2009

Some NYTimes.com readers have seen a pop-up box warning them about a virus and directing them to a site that claims to offer antivirus software. We believe this was generated by an unauthorized advertisement and are working to prevent the problem from recurring. If you see such a warning, we suggest that you not click on it. Instead, quit and restart your Web browser. Questions and comments can be sent to adtraffic@nytimes.com.

Web application extension example

- Rogue third party advertisement
  - Displayed image of fake virus scan



Scanning for threats

File Name	Result/Infection
C:\Boot\memtest.exe	Infected: I-Worm.Sober.i - Trojan
C:\config.sys	Infected: Suspicious.Harakit - Trojan, Virus
C:\hiberfil.sys	Infected: Suspicious.Harakit - Trojan, Virus
C:\pagefile.sys	Infected: Suspicious.Harakit - Trojan, Virus

Objects scanned: 3209
Threats found: 13
Elapsed time: 11 second(s)
Currently scanning: C:\ (Local Disk)
Current object: C:\Program Files\Lenovo\System Update\session\7bg675ww

Statistics
Last scan: Never
Last update: Never
Virus DB: 9542
Spyware DB: 8531
Version: 8.2.10.25
Status: Not activated

Problems with extensions

Web browser extensions

Web application extensions

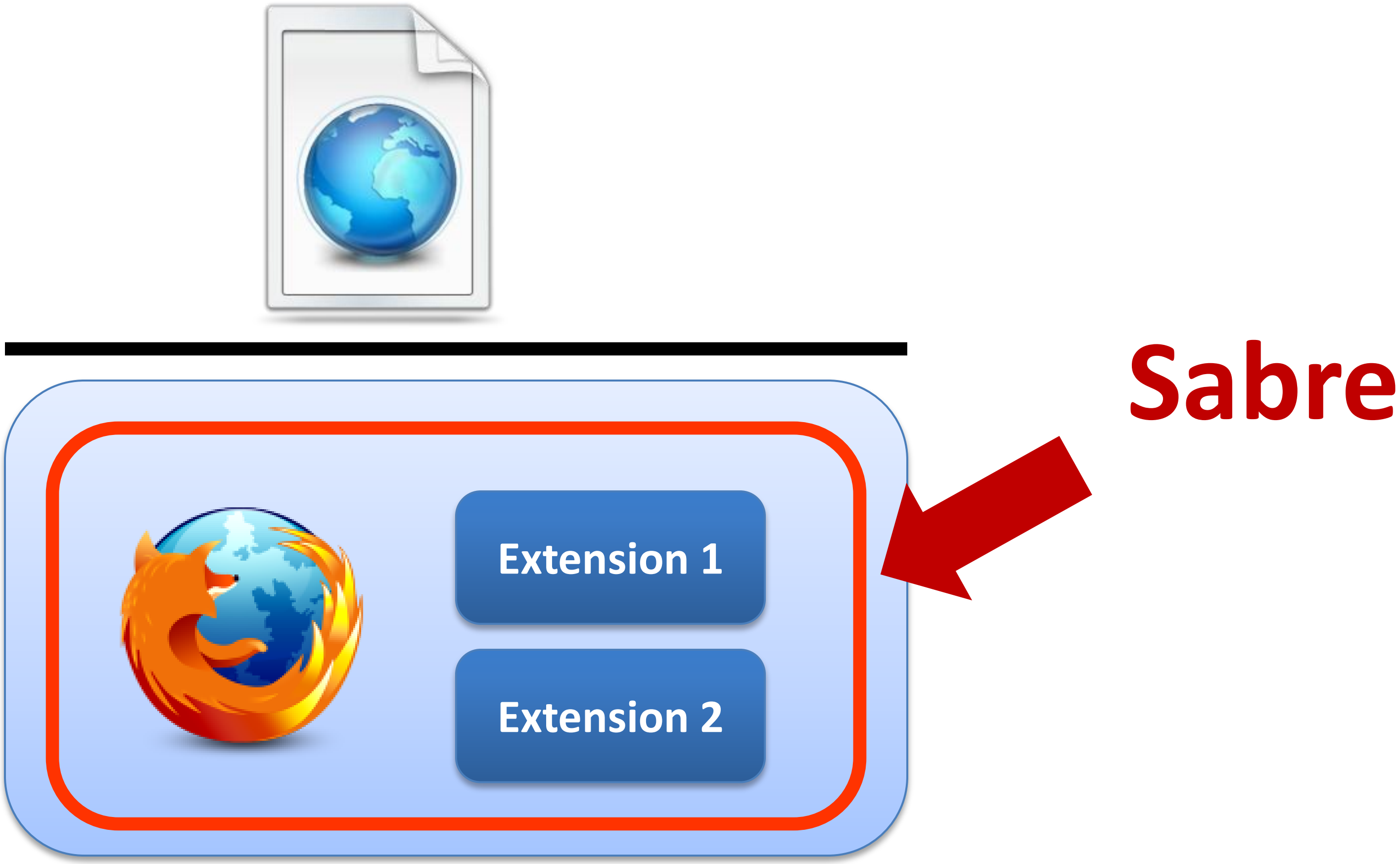
Untrusted extensions put client security and privacy at risk

Security for extensions

- **Sabre [ACSAC’09] (Best Student Paper Award) secure Web browser extensions**
  - Analyze information flow in JavaScript-based extensions
  - Sabre found several information flow violations in legacy extensions
- **Transcript [PLAS’10, ECOOP’12b] secures Web application and Web browser extensions**
  - Implements ***isolation*** as a first class primitive for JavaScript

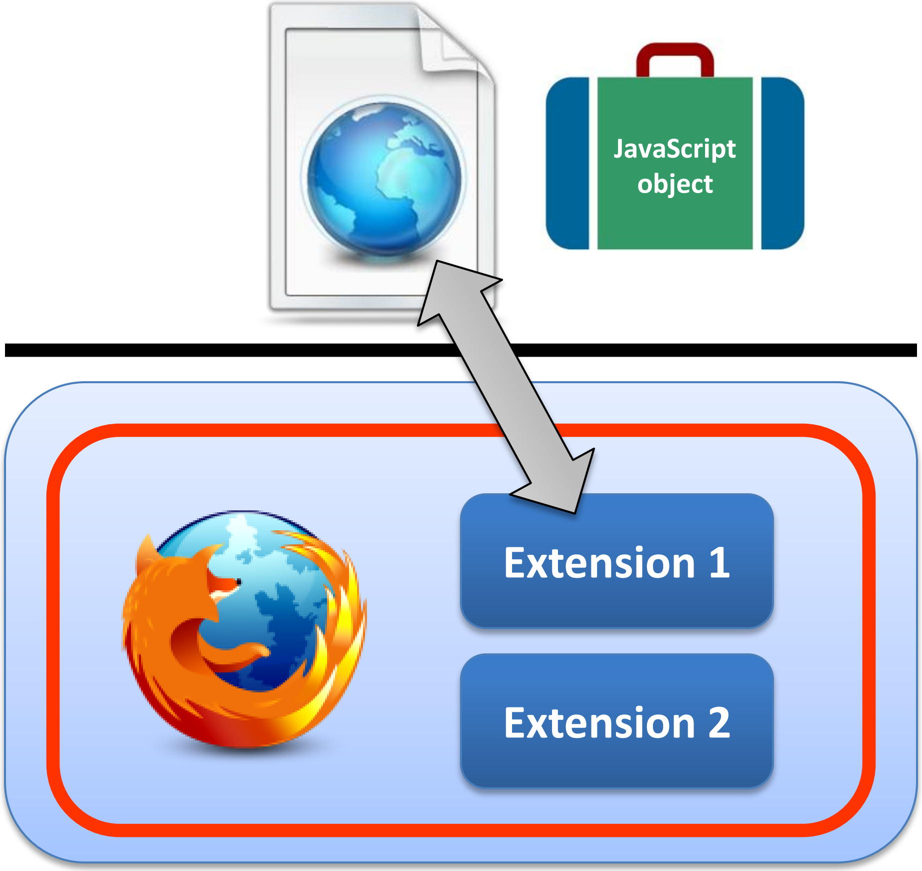
Sabre: Analyzing information flow in JavaScript-based extensions

Sabre: Key idea



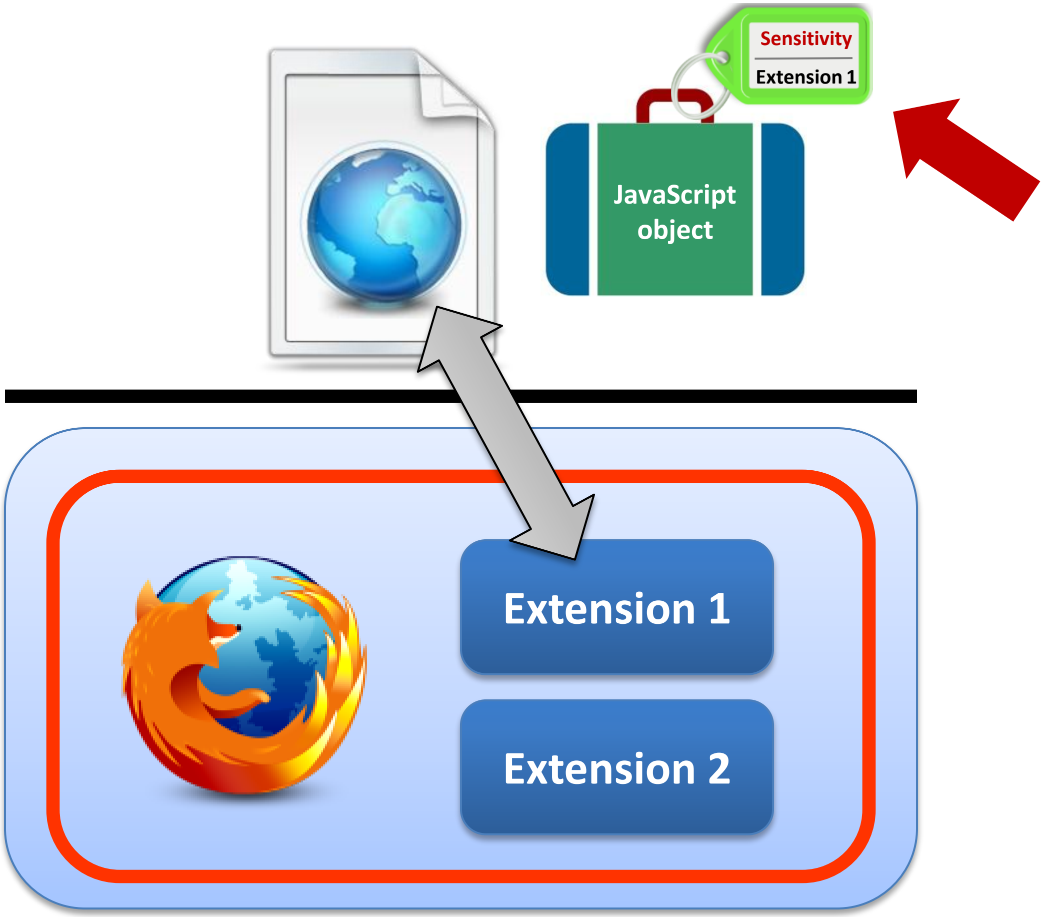
Sabre enhanced Firefox with extensions

Sabre: Key idea



Sabre enhanced Firefox with extensions

Sabre: Key idea



Sensitivity

Extension 1

JavaScript object

Security label

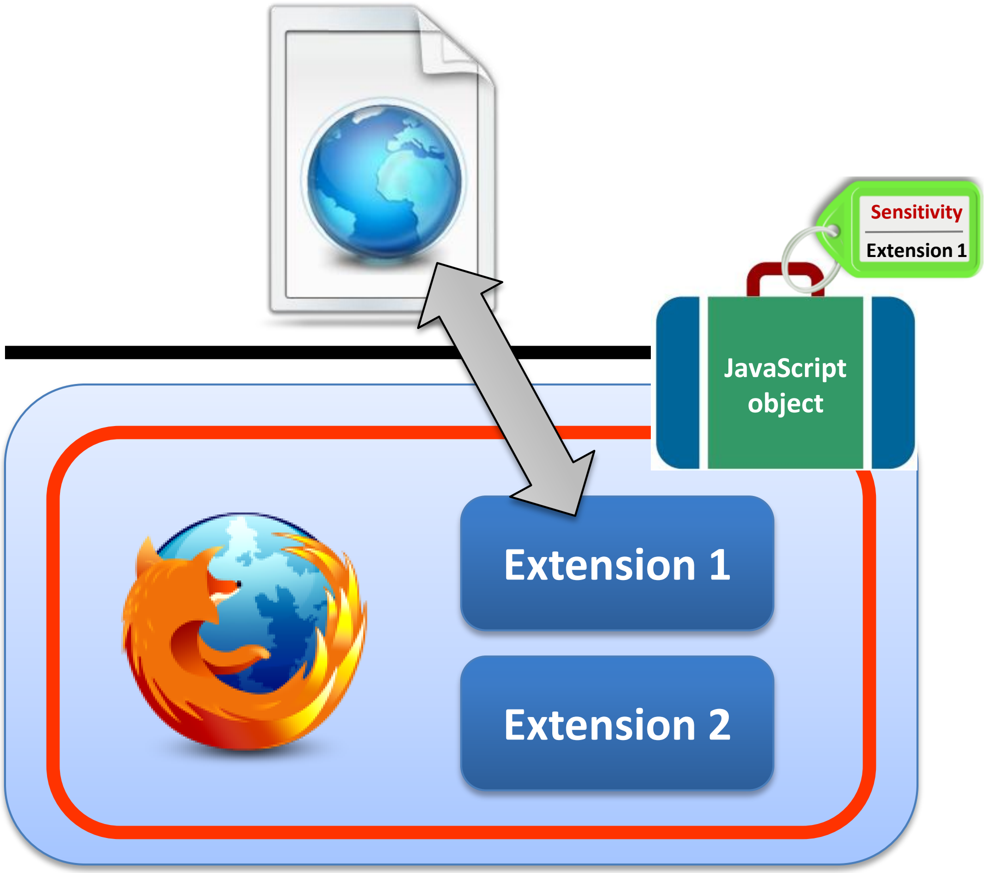
Extension 1

Extension 2

Sabre enhanced Firefox with extensions

1 Appropriately mark data as sensitive

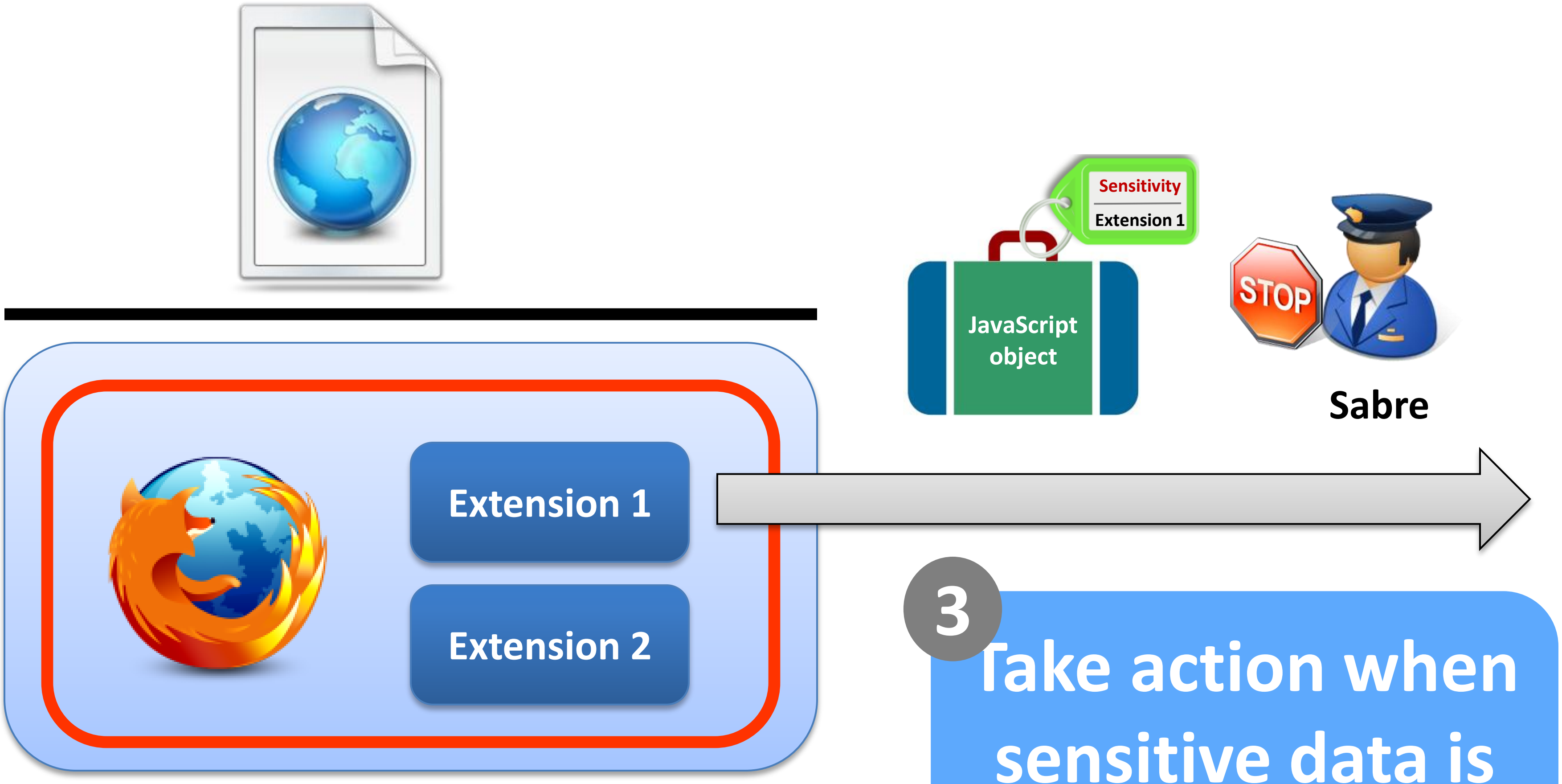
Sabre: Key idea



Sabre enhanced Firefox with extensions

2 Track the propagation of security label in the browser

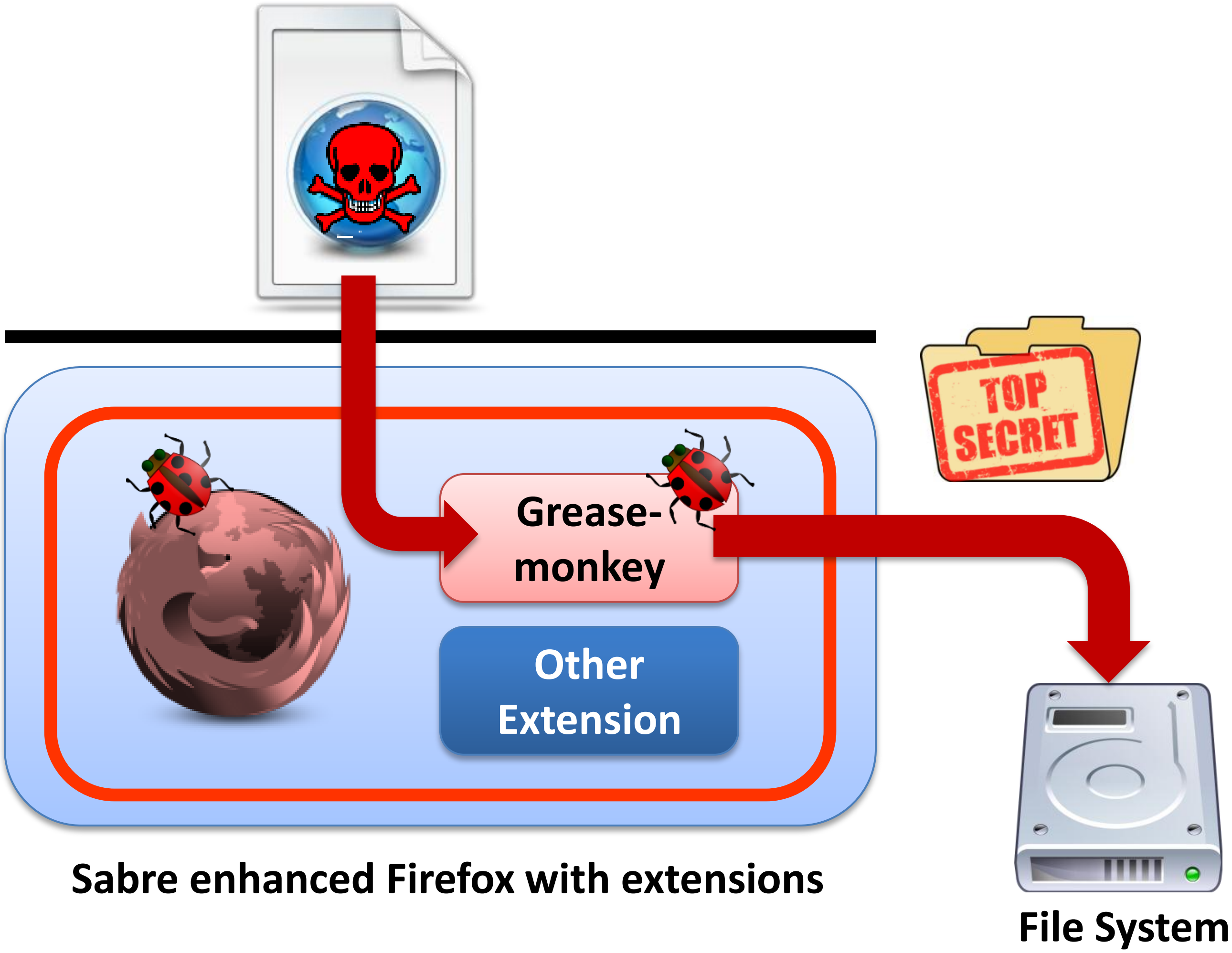
Sabre: Key idea



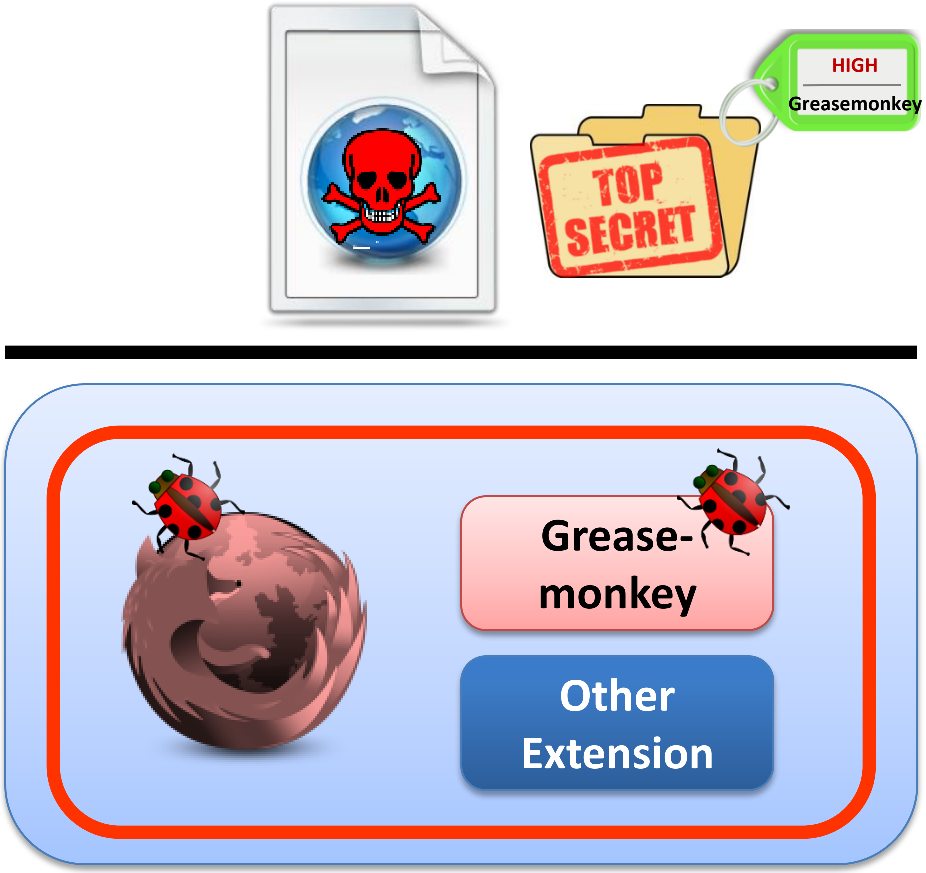
Sabre enhanced Firefox with extensions

3 Take action when sensitive data is externalized

Sabre: Greasemonkey attack



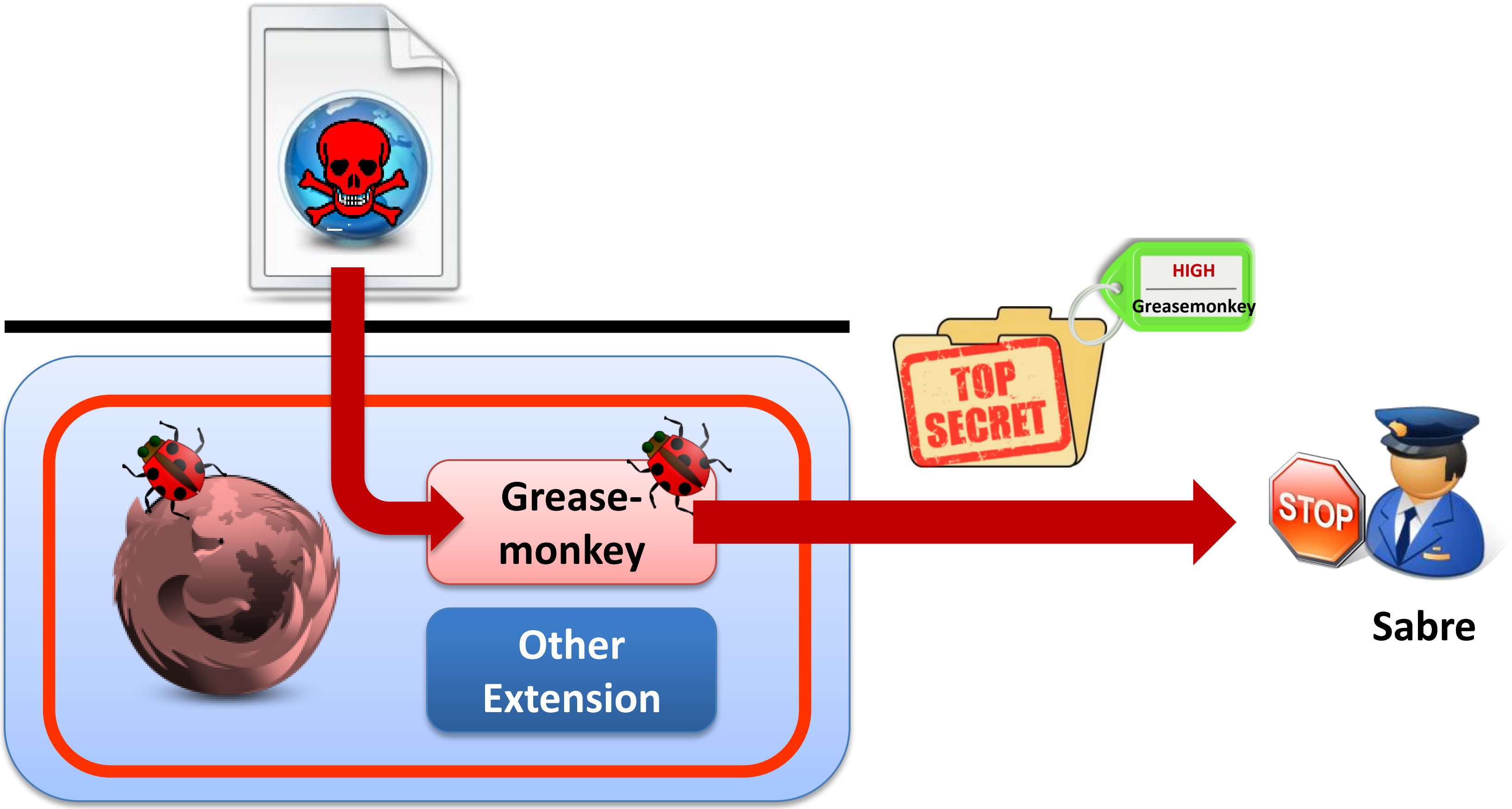
Sabre: Greasemonkey attack



Security label

Sabre enhanced Firefox with extensions

Sabre: Greasemonkey attack



Sabre enhanced Firefox with extensions

Results: Categorizing benign extensions

	Extension	HTML forms	HTTP channel	File system	Load URLs	JS events
1	Ad Block		✓	✓		
2	All-in-one Sidebar			✓		
3	Cool Previews		✓	✓		
4	Download Statusbar			✓		
5	Fast Video Download				✓	
6	Forecastfox		✓	✓	✓	
7	Foxmarks Synchronizer		✓	✓		
8	Ghostery			✓		
9	Google Previews		✓	✓		
10	Greasemonkey (v0.8.1)		✓	✓		
11	NoScript		✓	✓		
12	PDF Download		✓	✓	✓	
13	PwdHash	✓				
14	SpeedDial			✓	✓	
15	StumbleUpon		✓	✓	✓	
16	Stylish		✓	✓	✓	✓
17	Tab Mix Plus			✓	✓	
18	User Agent Switcher			✓		
19	Video DownloadHelper		✓	✓		
20	Web-of-Trust		✓	✓	✓	

Results: Categorizing benign extensions

	Extension	HTML forms	HTTP channel	File system	Load URLs	JS events
1	Ad Block		✓	✓		
2	All-in-one Sidebar			✓		
3	Cool Previews		✓	✓		
4	Download Statusbar			✓		
5	Fast Video Download				✓	
13	Fwdflash	✓				
14	SpeedDial			✓	✓	
15	StumbleUpon		✓	✓	✓	
16	Stylish		✓	✓	✓	✓
17	Tab Mix Plus			✓	✓	
18	User Agent Switcher			✓		
19	Video DownloadHelper		✓	✓		
20	Web-of-Trust		✓	✓	✓	

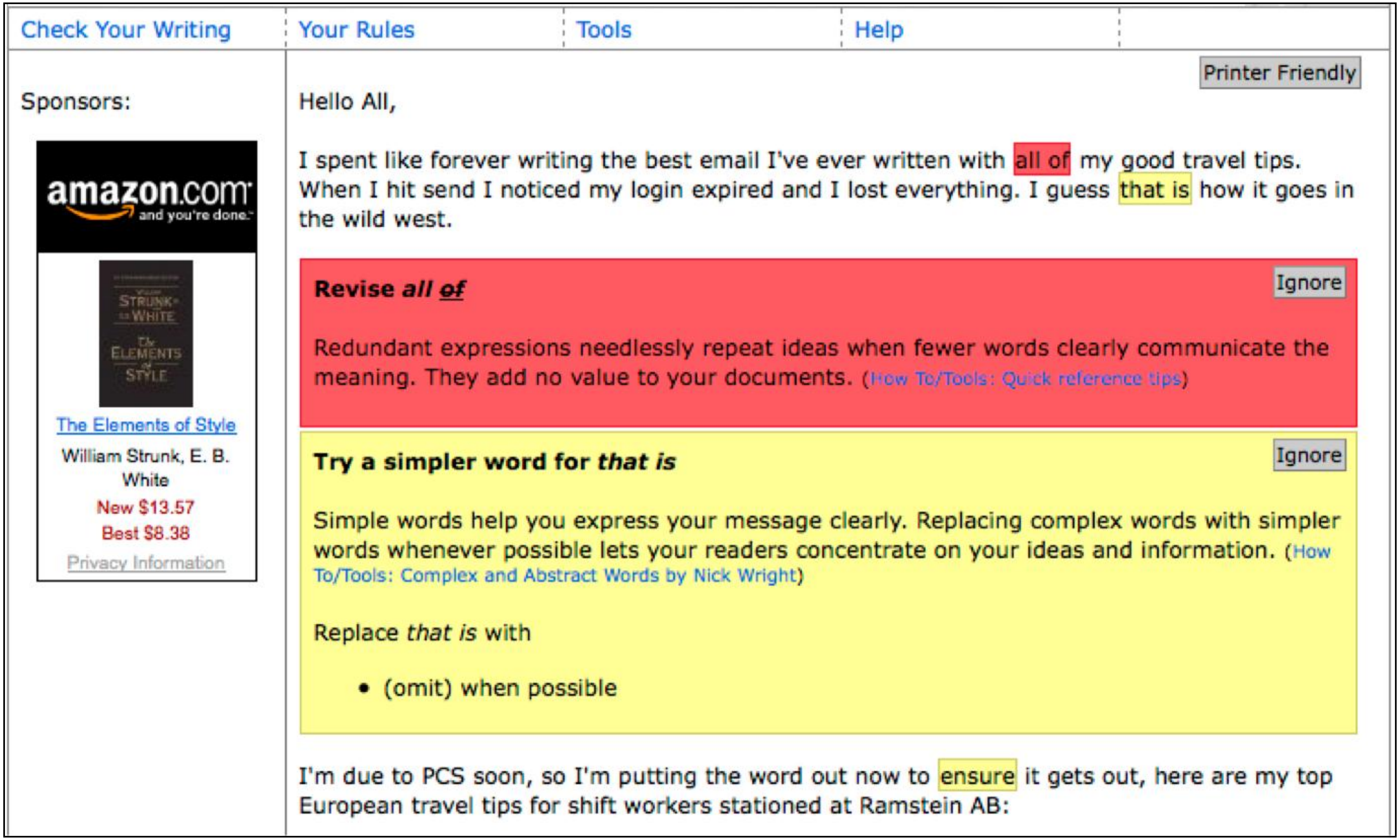
Whitelisting / declassification of trusted extensions is essential

Results: Accuracy

- **Vulnerable and malicious extensions**
  - GreaseMonkey v0.3.3
  - Firebug v1.01
  - FFsniFF
  - BrowserSPY
- **Result**
  - Precisely identified all flow violations
  - No false positives during normal web browsing

Transcript: Language-based security for Web platform extensions

Example: Online text editor



Hello All,

I spent like forever writing the best email I've ever written with all of my good travel tips. When I hit send I noticed my login expired and I lost everything. I guess that is how it goes in the wild west.

Revise *all ~~of~~*

Redundant expressions needlessly repeat ideas when fewer words clearly communicate the meaning. They add no value to your documents. (How To/Tools: Quick reference tips)

Try a simpler word for *that is*

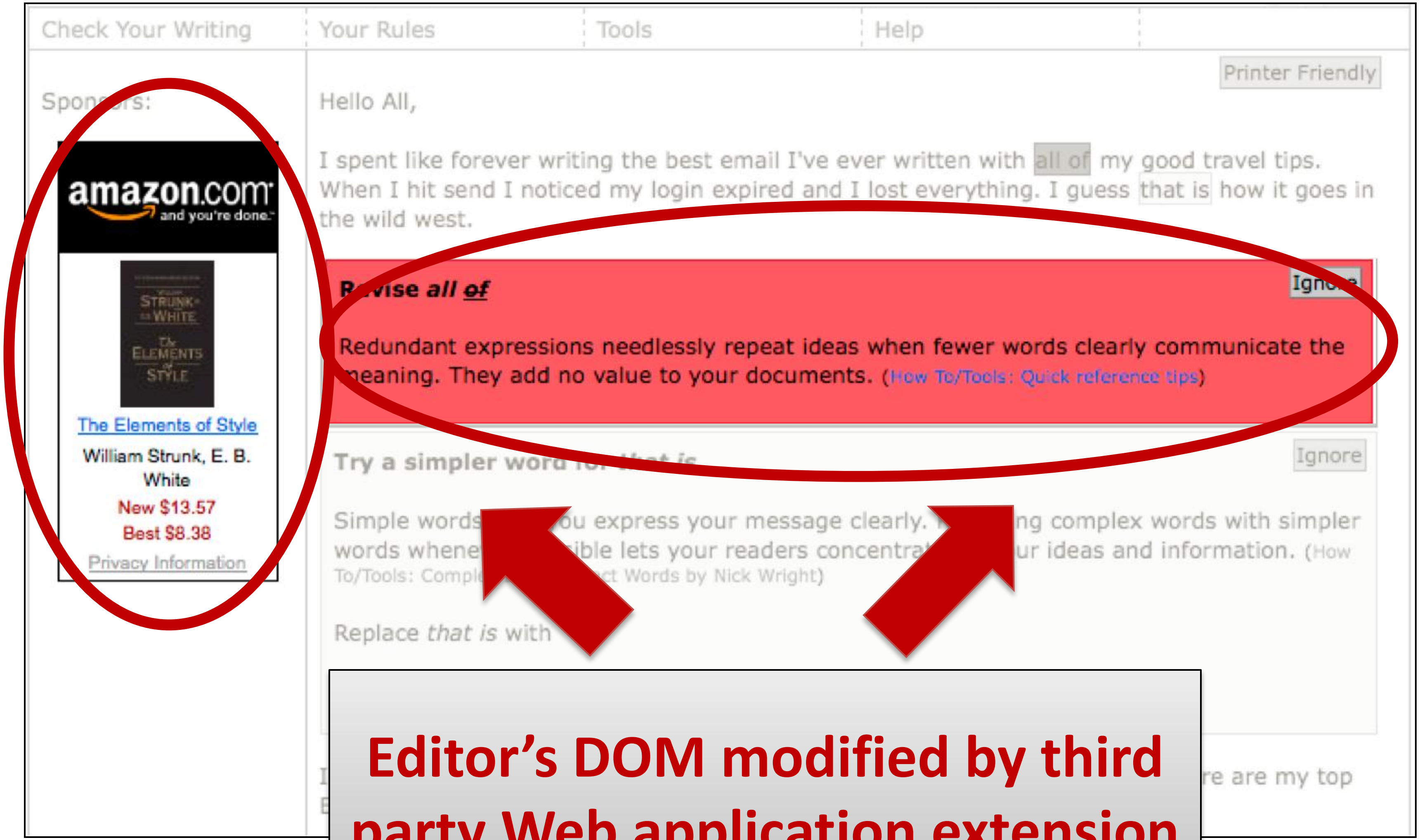
Simple words help you express your message clearly. Replacing complex words with simpler words whenever possible lets your readers concentrate on your ideas and information. (How To/Tools: Complex and Abstract Words by Nick Wright)

Replace *that is* with

- (omit) when possible

I'm due to PCS soon, so I'm putting the word out now to ensure it gets out, here are my top European travel tips for shift workers stationed at Ramstein AB:

Example: Online text editor



The Elements of Style

William Strunk, E. B. White

New $13.57

Best $8.38

Privacy Information

Hello All,

I spent like forever writing the best email I've ever written with all of my good travel tips. When I hit send I noticed my login expired and I lost everything. I guess that is how it goes in the wild west.

Revise *all of*

Redundant expressions needlessly repeat ideas when fewer words clearly communicate the meaning. They add no value to your documents. (How To/Tools: Quick reference tips)

Try a simpler word for *that is*

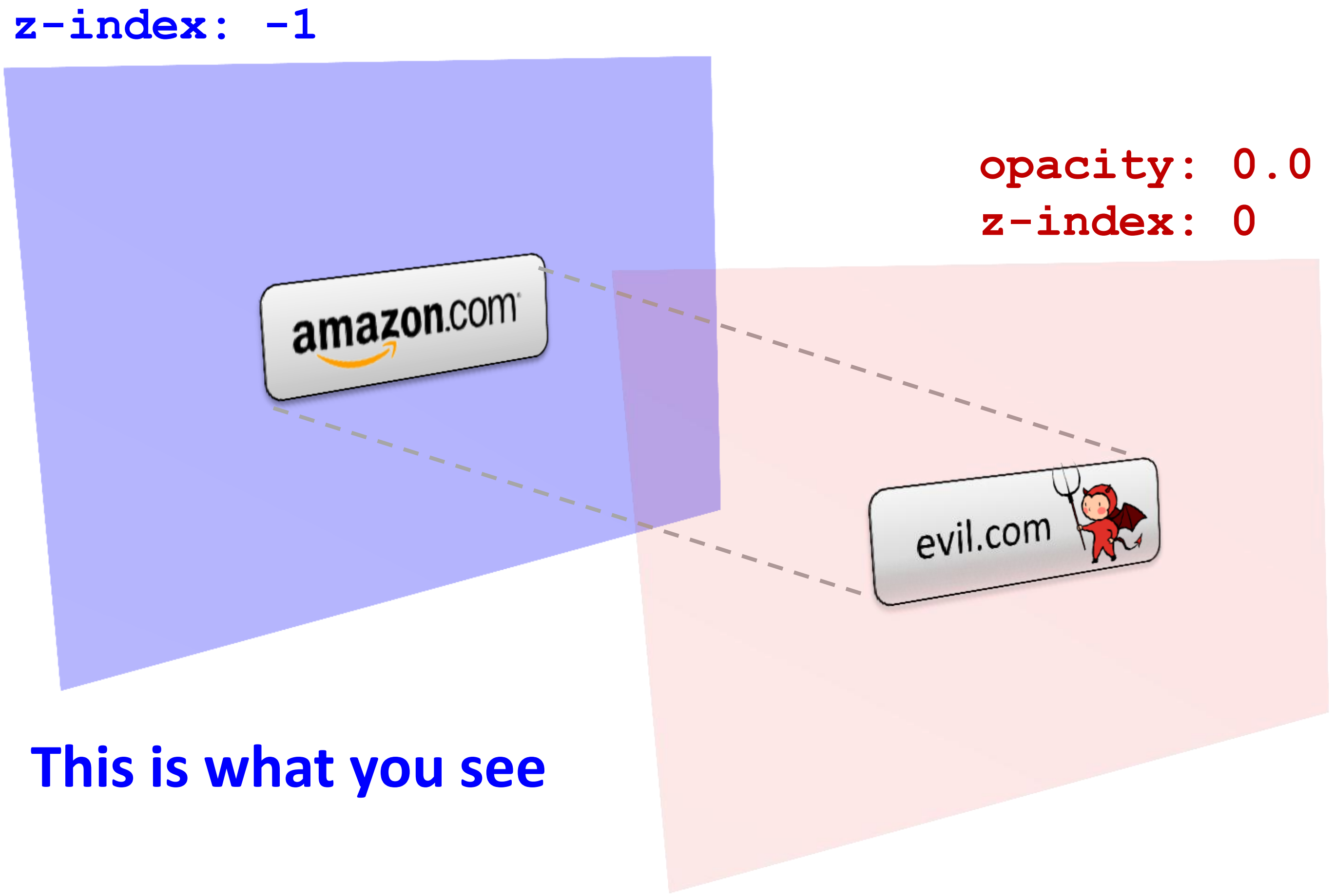
Simple words ou express your message clearly. ng complex words with simpler words whene ible lets your readers concentra ur ideas and information. (How To/Tools: Compl ct Words by Nick Wright)

Replace *that is* with

re are my top

Editor's DOM modified by third party Web application extension

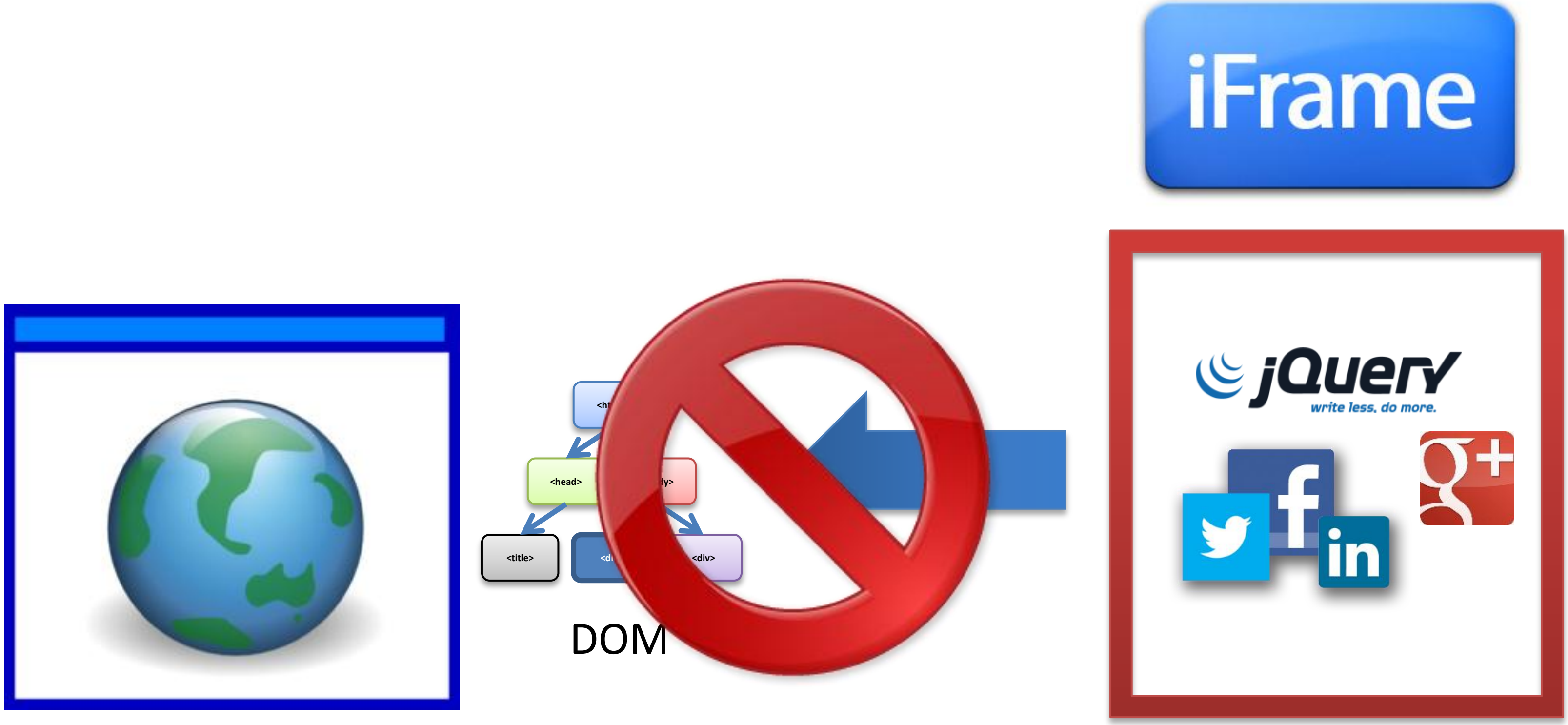
UI redressing attack



This is what you see

This is what you click on

State of the art: Access control

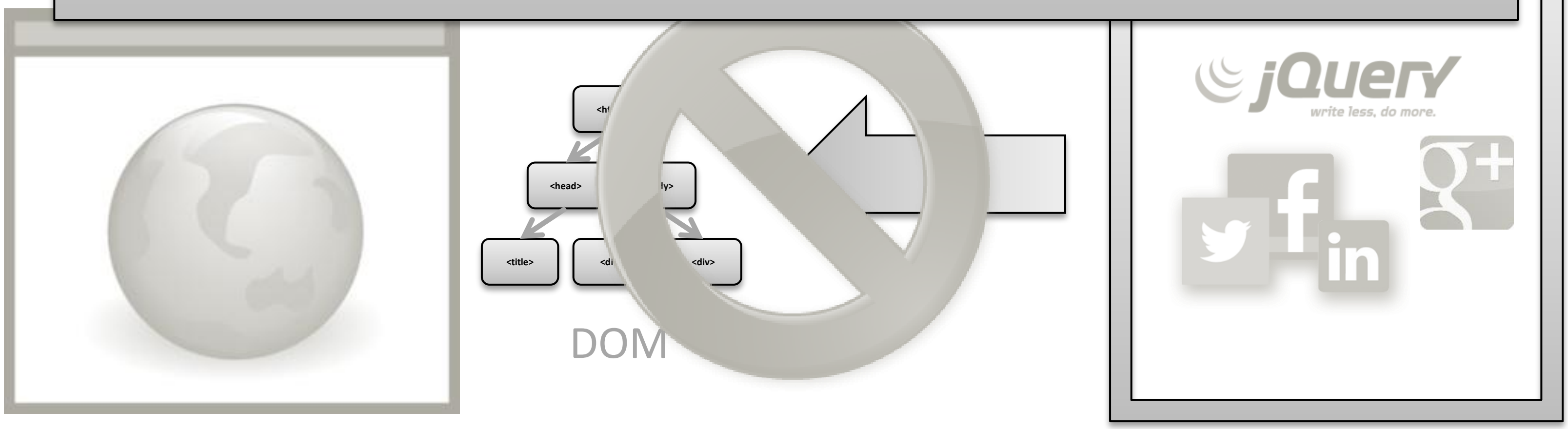


Web Application

`<iframe>` sandboxed third party content

State of the art: Access control

<iframe> is rigid and hampers functionality

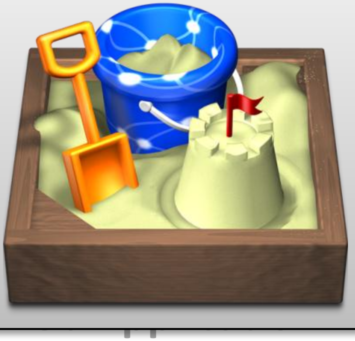


Web Application

<iframe> sandboxed third party content

State of the art: Access control

`<iframe>` is rigid and hampers functionality



Need a fine-grained JavaScript sandbox

<iframe> sandboxed third party content

Access control sufficient ?

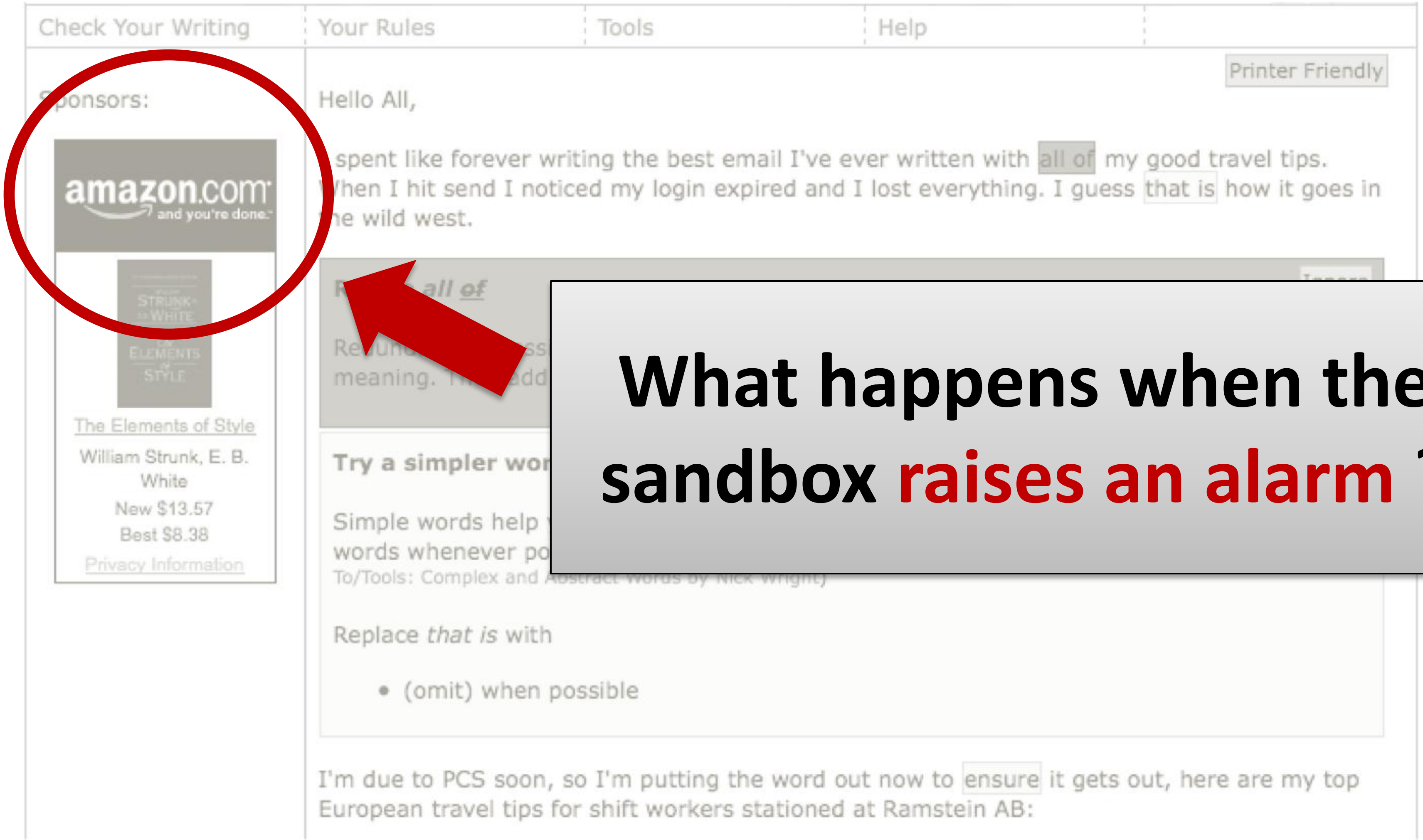
Reference monitors use access control policies to sandbox untrusted third party JavaScript content

Access control not sufficient

Reference monitors use access control policies to sandbox untrusted third party JavaScript content

Access control policies may allow seemingly innocuous, but undesirable JavaScript heap and DOM changes

Access control not sufficient



The Elements of Style

William Strunk, E. B. White

New $13.57

Best $8.38

Privacy Information

Hello All,

I spent like forever writing the best email I've ever written with all of my good travel tips. When I hit send I noticed my login expired and I lost everything. I guess that is how it goes in the wild west.

R all of

Re ss meaning. Th add

Try a simpler wor

Simple words help words whenever po To/Tools: Complex and Abstract Words by Nick Wright)

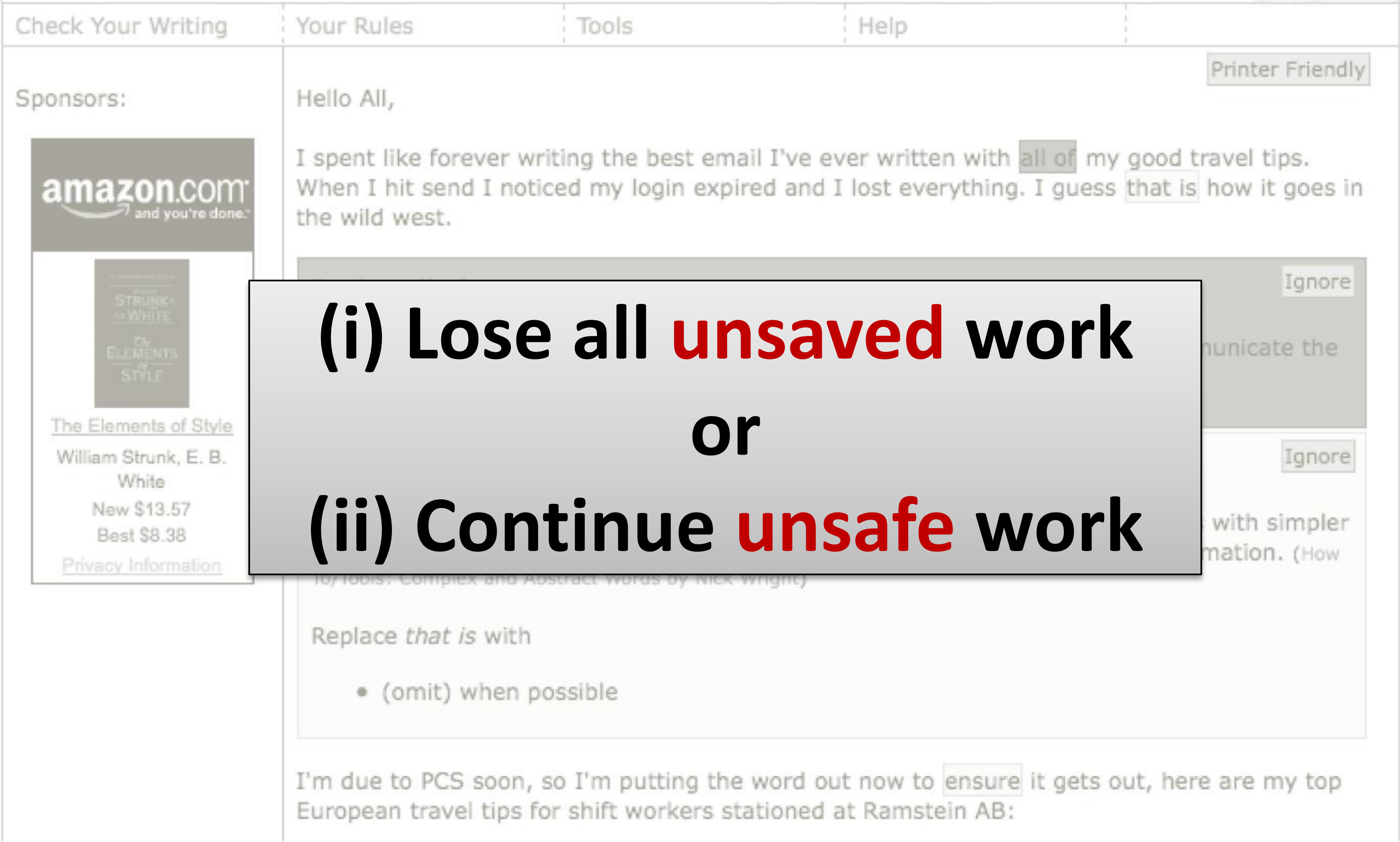
Replace *that is* with

- (omit) when possible

I'm due to PCS soon, so I'm putting the word out now to ensure it gets out, here are my top European travel tips for shift workers stationed at Ramstein AB:

What happens when the sandbox raises an alarm ?

Access control not sufficient



Hello All,

I spent like forever writing the best email I've ever written with all of my good travel tips. When I hit send I noticed my login expired and I lost everything. I guess that is how it goes in the wild west.

...unicate the

... with simpler ...mation. (How To) Tools: Complex and Abstract Words by Nick Wright)

Replace *that is* with

- (omit) when possible

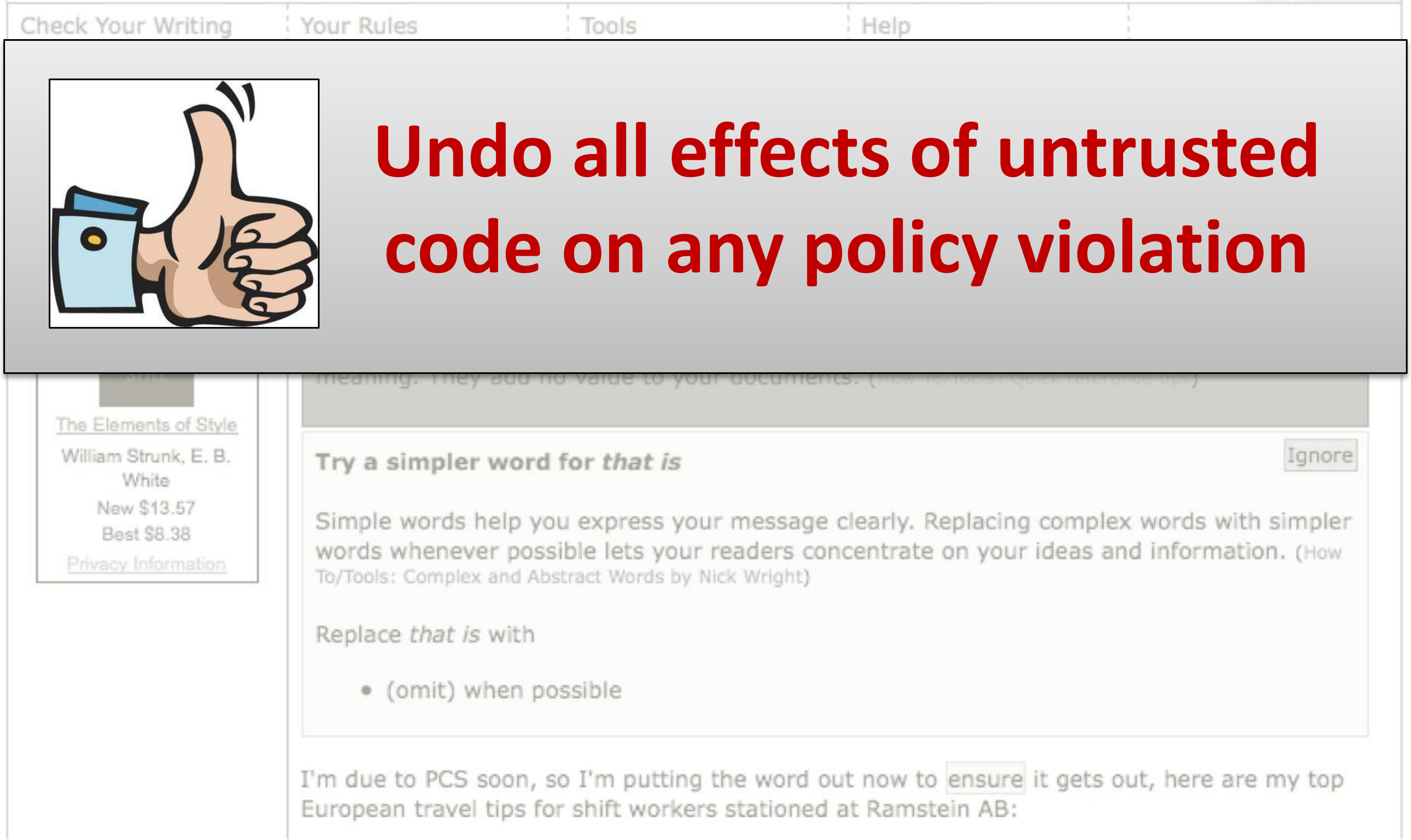
I'm due to PCS soon, so I'm putting the word out now to ensure it gets out, here are my top European travel tips for shift workers stationed at Ramstein AB:

(i) Lose all unsaved work

or

(ii) Continue unsafe work

Access control not sufficient



Undo all effects of untrusted code on any policy violation

meaning. They add no value to your documents.

The Elements of Style
William Strunk, E. B. White
New $13.57
Best $8.38
Privacy Information

Try a simpler word for *that is*

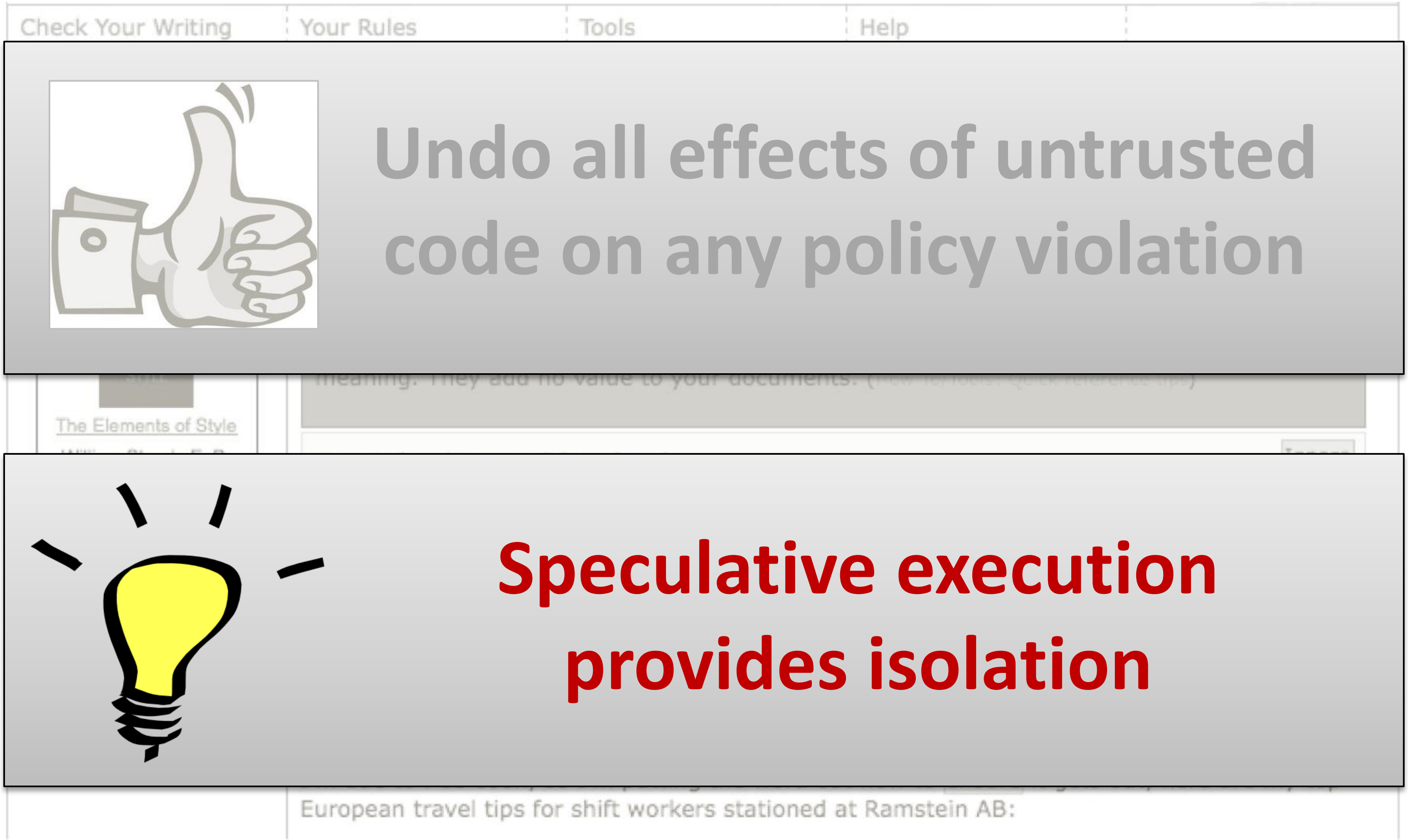
Simple words help you express your message clearly. Replacing complex words with simpler words whenever possible lets your readers concentrate on your ideas and information. (How To/Tools: Complex and Abstract Words by Nick Wright)

Replace *that is* with

- (omit) when possible

I'm due to PCS soon, so I'm putting the word out now to ensure it gets out, here are my top European travel tips for shift workers stationed at Ramstein AB:

Access control not sufficient


Check Your Writing
Your Rules
Tools
Help
meaning. They add no value to your documents.
The Elements of Style
European travel tips for shift workers stationed at Ramstein AB:

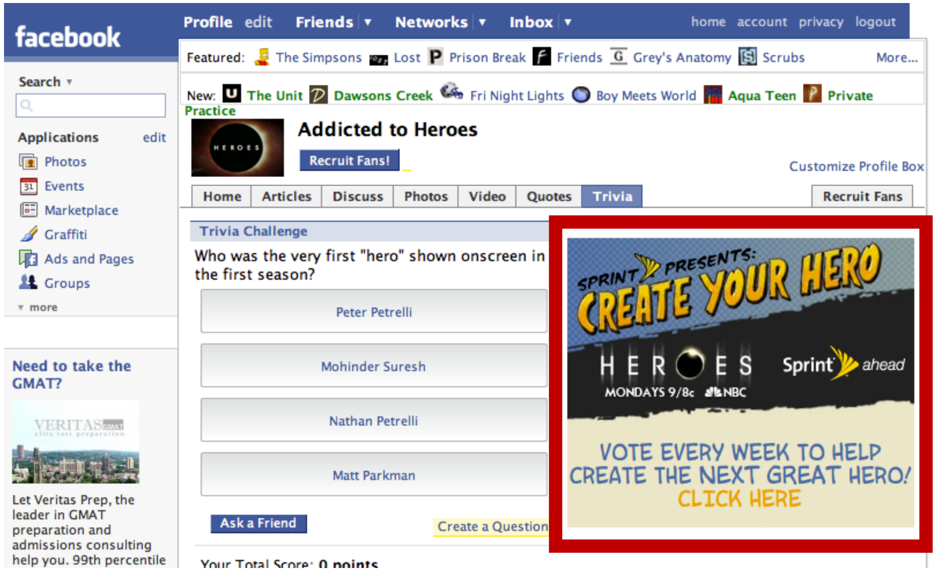
Undo all effects of untrusted code on any policy violation

Speculative execution provides isolation

Transcript

- Enhance JavaScript language with **speculation**
  - Execute untrusted content speculatively

Web Application



Who was the very first "hero" shown onscreen in the first season?

Need to take the GMAT?

Let Veritas Prep, the leader in GMAT preparation and admissions consulting help you. 99th percentile

Your Total Score: 0 points

Speculative Execution

  - Commit changes after policy enforcement

Transcript goals (I)

JS

```
eval
this
with
```

Transcript goals (I)

eval
this
with

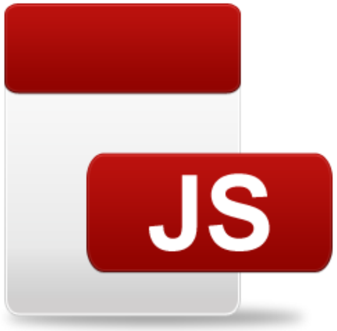
```
> eval(‘var foo = 42;’);
> foo
42
```

Transcript goals (I)

```
eval
this
with
```

```
> eval(<N/W or User Input>);
> ??
```

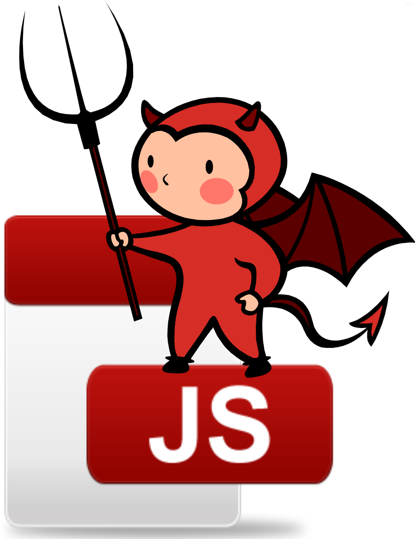
Transcript goals (I)



```
eval
this
with
```

Handle arbitrary third party code including dynamic constructs

Transcript goals (II)



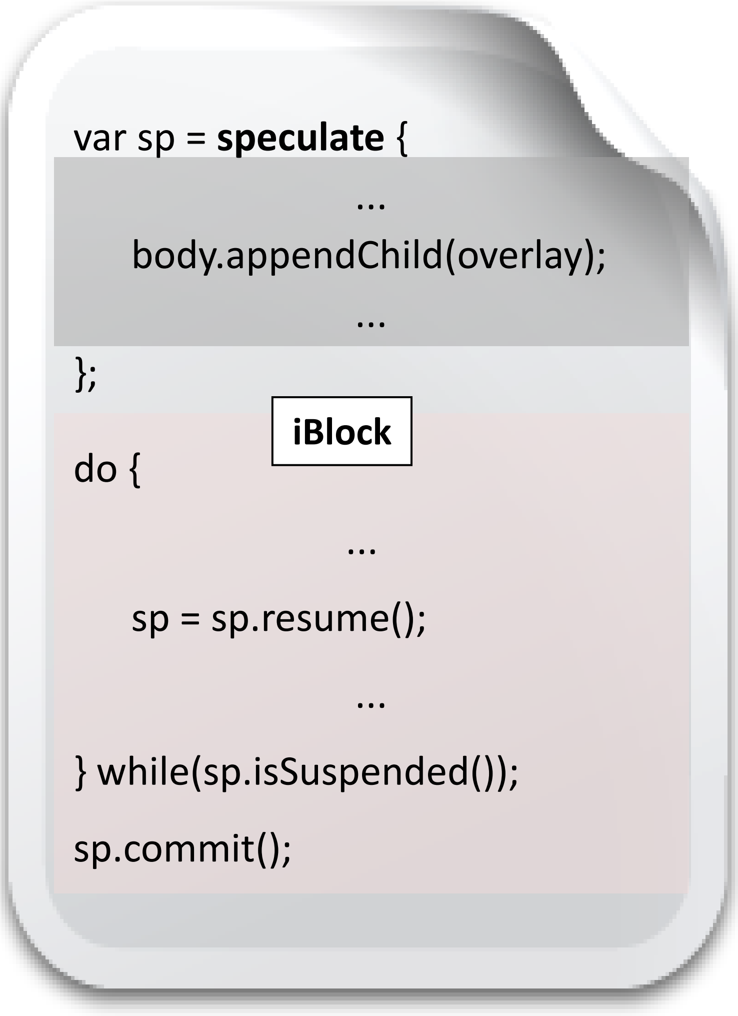
- Cookie stealing
- UI Redressing
- Drive-by downloads
- Annoying popups
- Undesired navigation
- X-domain communication

Enforce powerful security policies on 3rd party behavior

Features of Transcript

- **JavaScript speculation**
  – Speculative execution of **unmodified** third party JavaScript code
- **Suspend/resume speculative execution**
  – Web application can mediate external actions like DOM and AJAX operations (**akin to a system call**)
- **Speculative DOM updates**

Transcript in action

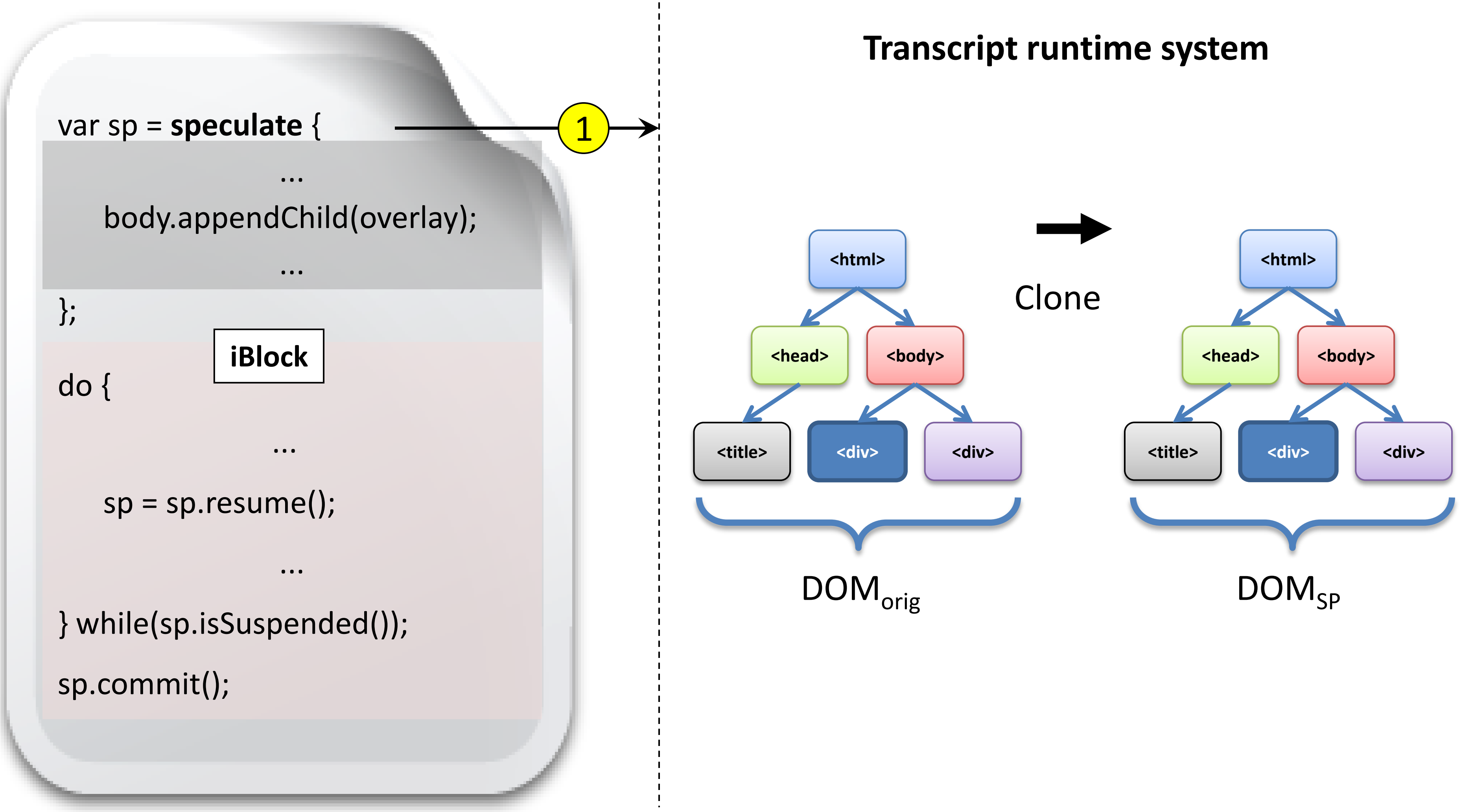


```
var sp = speculate {
                    ...
    body.appendChild(overlay);
                    ...
};
do {
                   ...
    sp = sp.resume();
                    ...
} while(sp.isSuspended());
sp.commit();
```

iBlock

Transcript runtime system

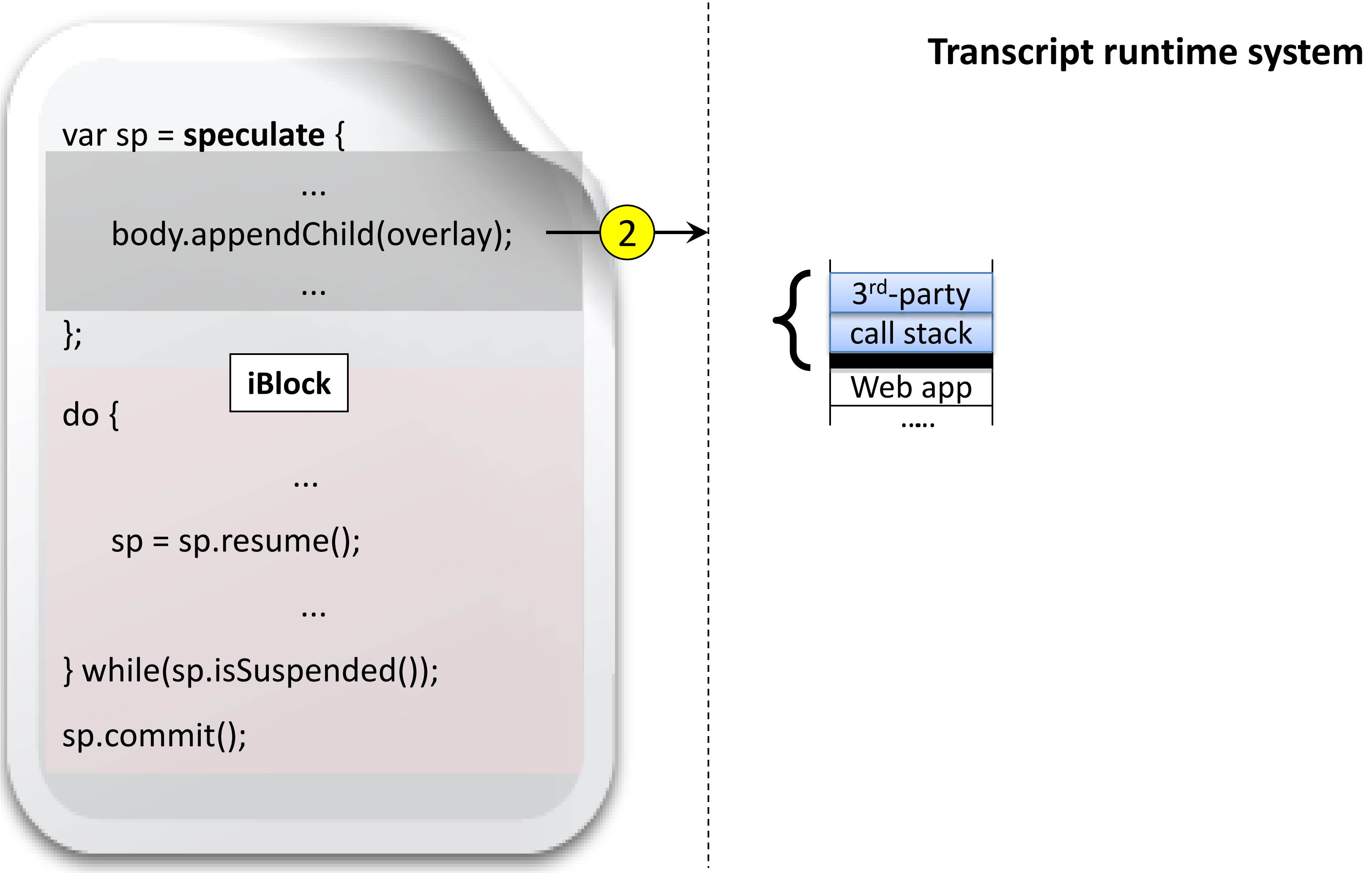
Transcript in action



```
var sp = speculate {
        ...
    body.appendChild(overlay);
        ...
};
do {
        ...
    sp = sp.resume();
        ...
} while(sp.isSuspended());
sp.commit();
```

Transcript runtime system

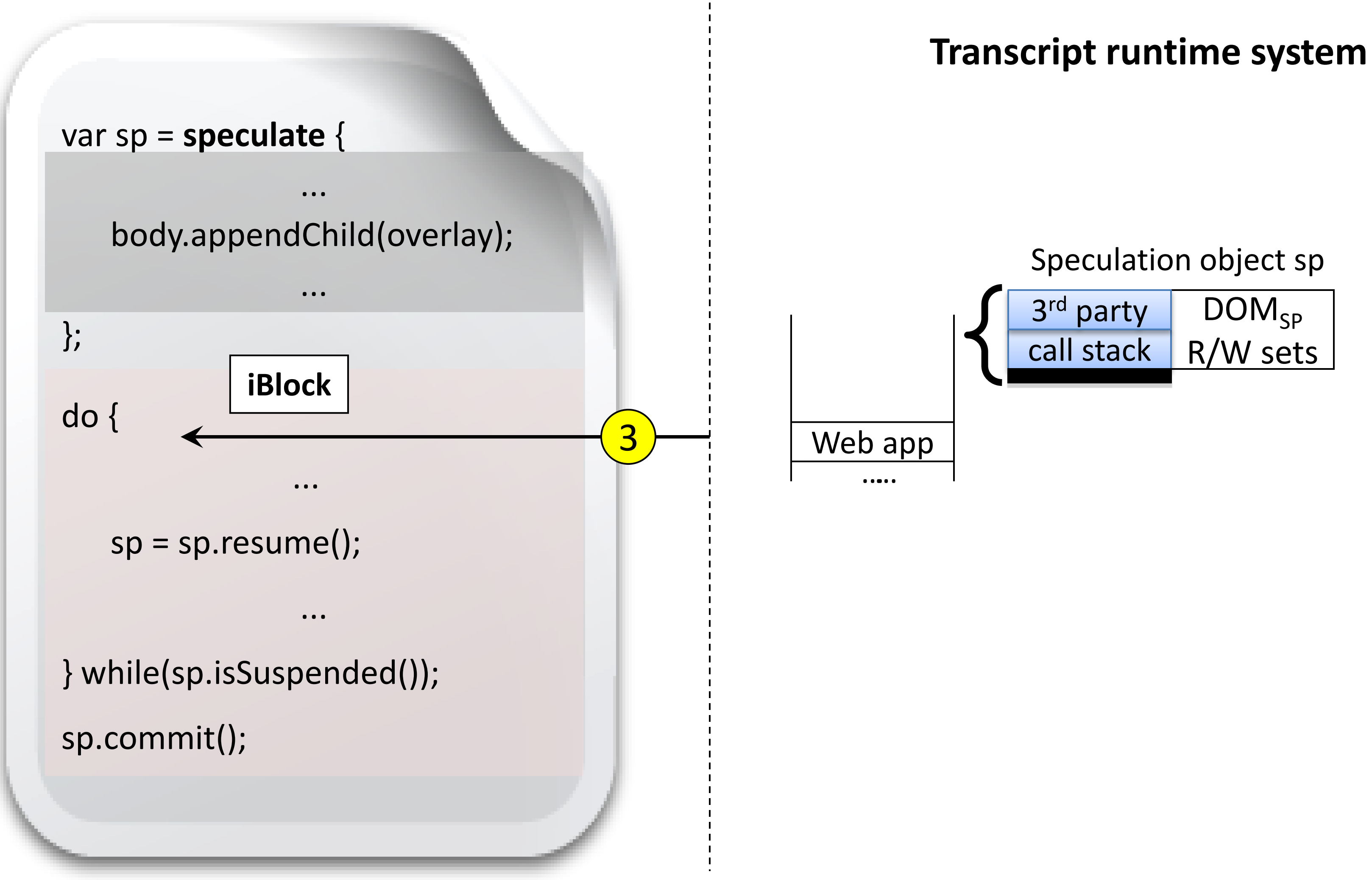
Transcript in action



```
var sp = speculate {
                    ...
    body.appendChild(overlay);
                    ...
};

do {
                   ...
    sp = sp.resume();
                    ...
} while(sp.isSuspended());
sp.commit();
```

Transcript in action

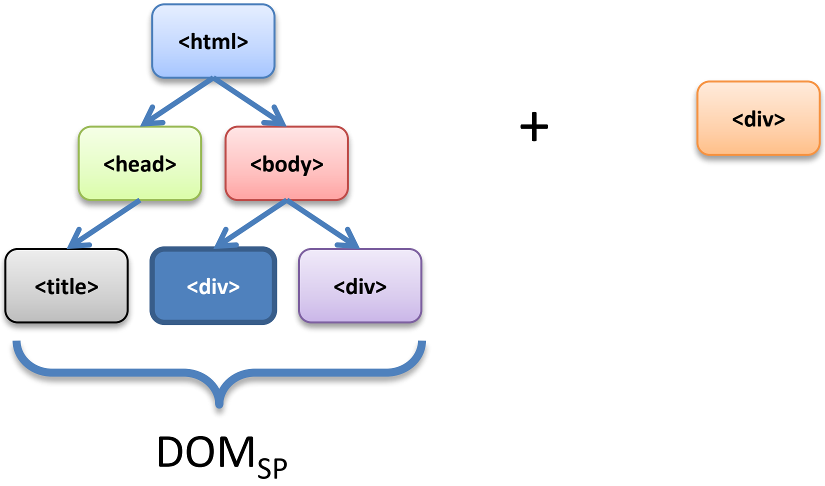


```
var sp = speculate {
            ...
    body.appendChild(overlay);
            ...
};
do {
            ...
    sp = sp.resume();
            ...
} while(sp.isSuspended());
sp.commit();
```

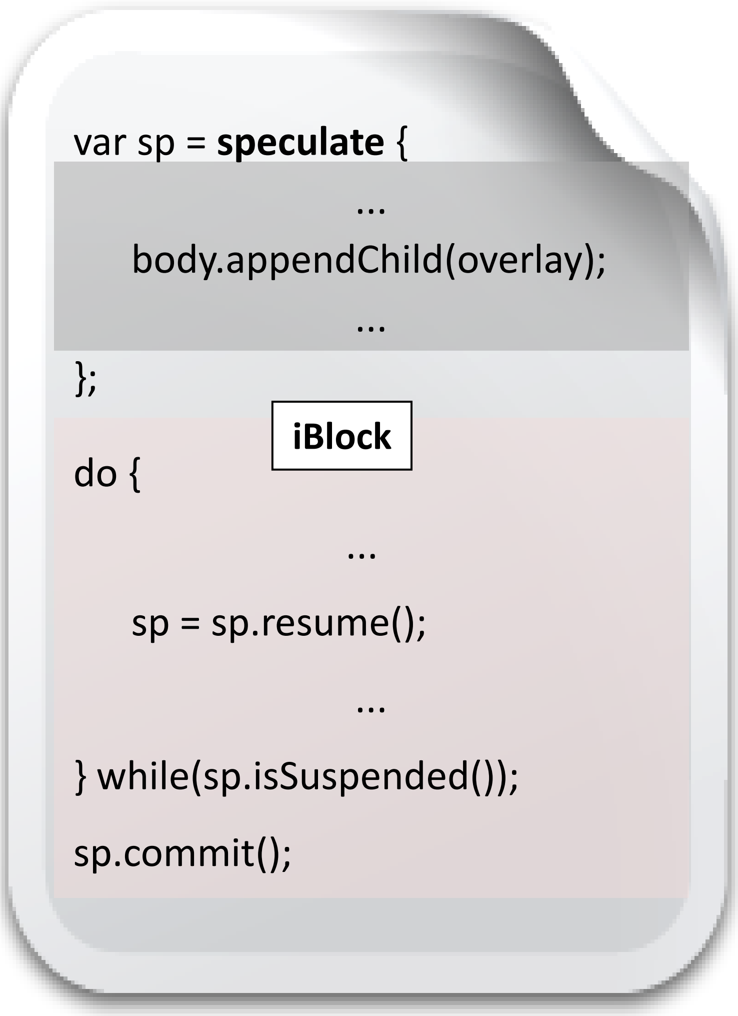
Transcript in action

```
var sp = speculate {
            ...
    body.appendChild(overlay);
            ...
};
                    iBlock
do {
            ...
    sp = sp.resume();
            ...
} while(sp.isSuspended());
sp.commit();
```

Transcript runtime system

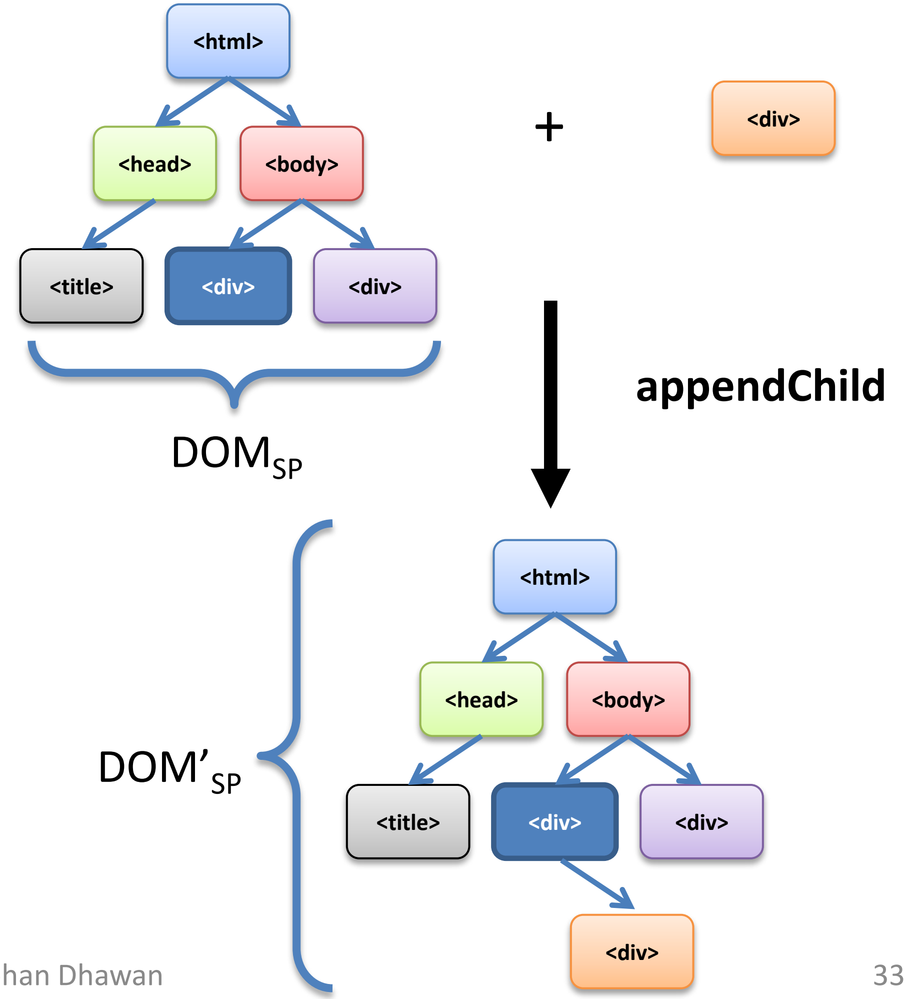


Transcript in action



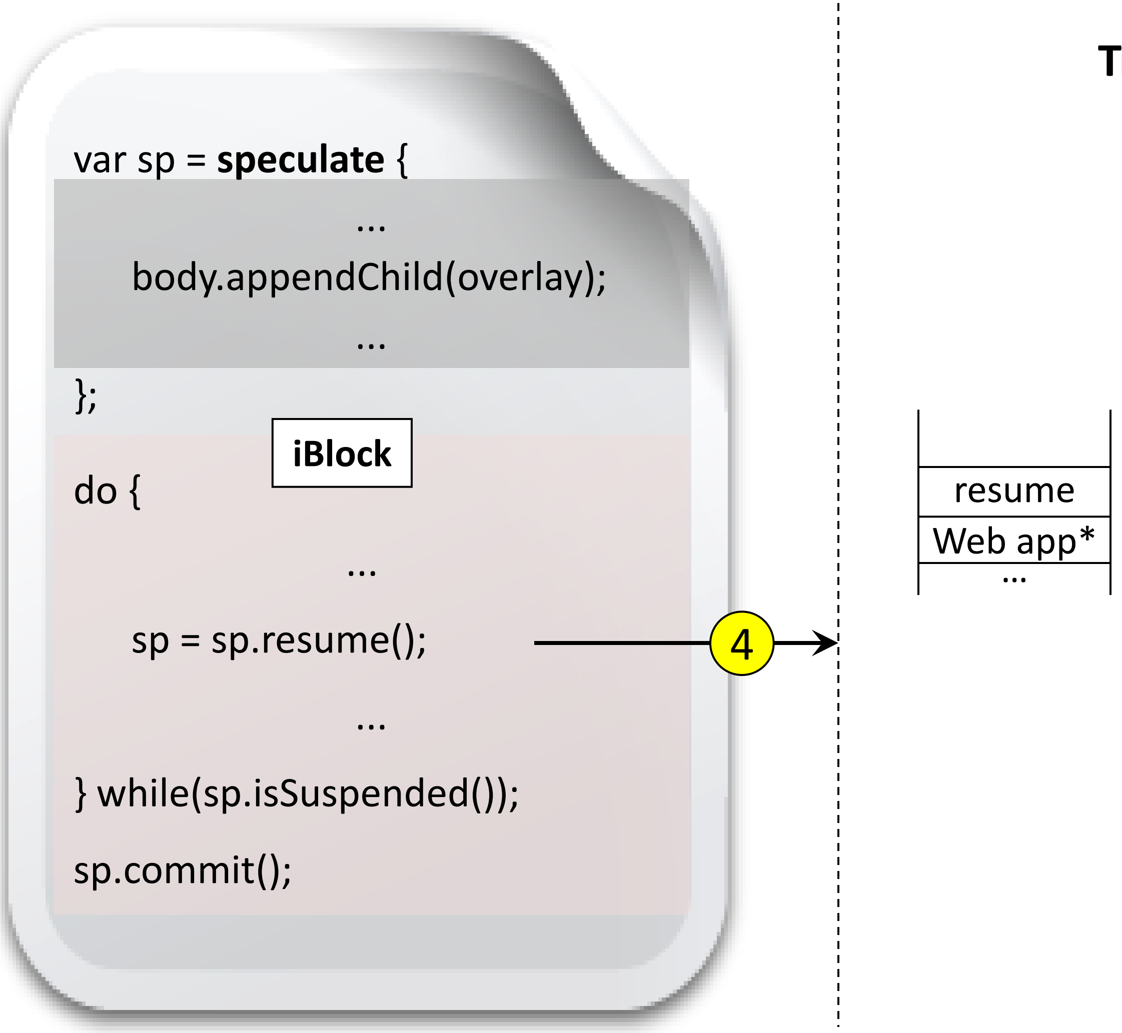
```
var sp = speculate {
                ...
    body.appendChild(overlay);
                ...
};
            iBlock
do {
               ...
    sp = sp.resume();
                ...
} while(sp.isSuspended());
sp.commit();
```

Transcript runtime system



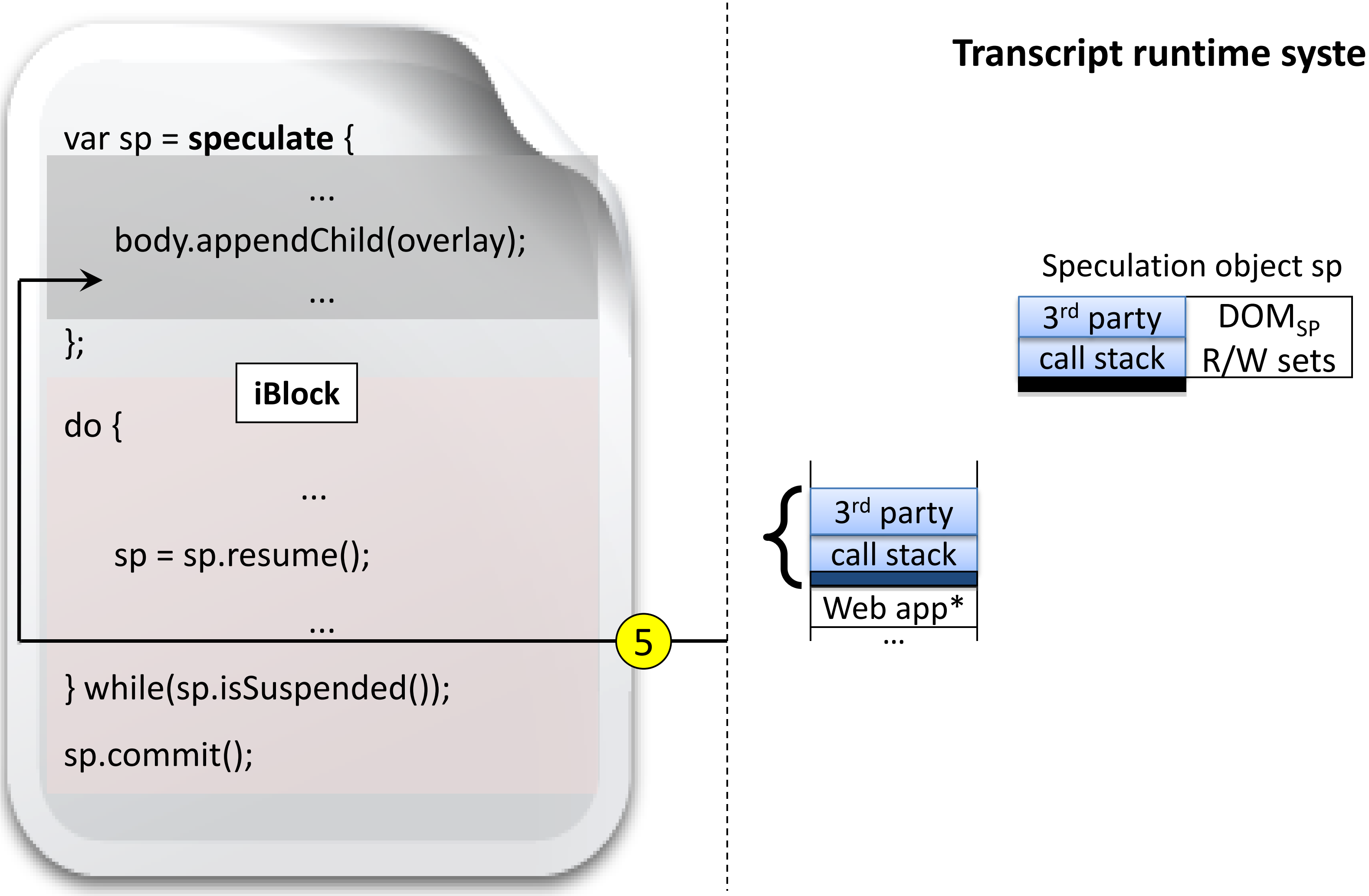
Transcript in action

Transcript runtime system



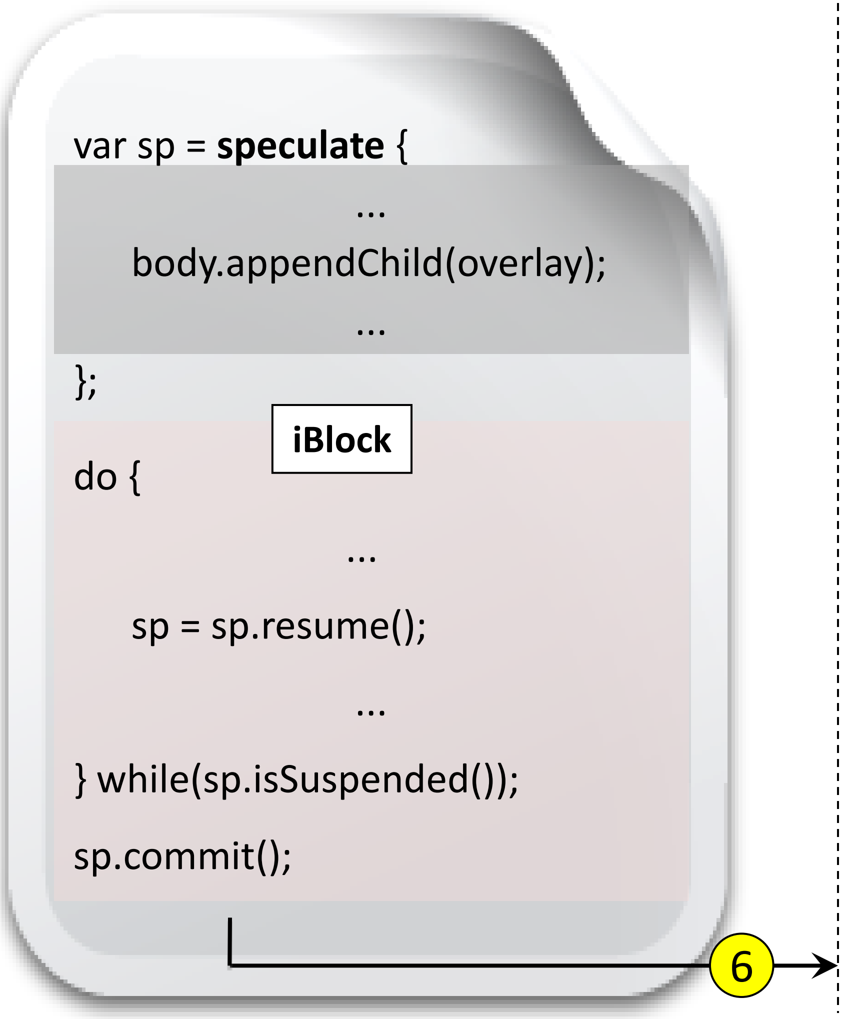
```
var sp = speculate {
                ...
    body.appendChild(overlay);
                ...
};
do {
               ...
    sp = sp.resume();
                ...
} while(sp.isSuspended());
sp.commit();
```

Transcript in action



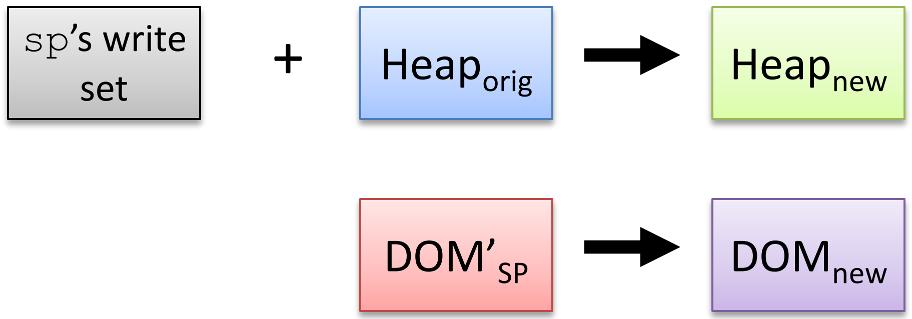
```
var sp = speculate {
                ...
    body.appendChild(overlay);
                ...
};
do {
               ...
    sp = sp.resume();
                ...
} while(sp.isSuspended());
sp.commit();
```

Transcript in action



```
var sp = speculate {
        ...
    body.appendChild(overlay);
        ...
};
do {
        ...
    sp = sp.resume();
        ...
} while(sp.isSuspended());
sp.commit();
```

Transcript runtime system



Implementation

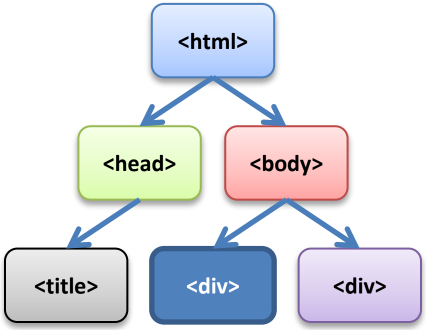
Firefox 3.7a4

SpiderMonkey

Implementation

Firefox 3.7a4

SpiderMonkey



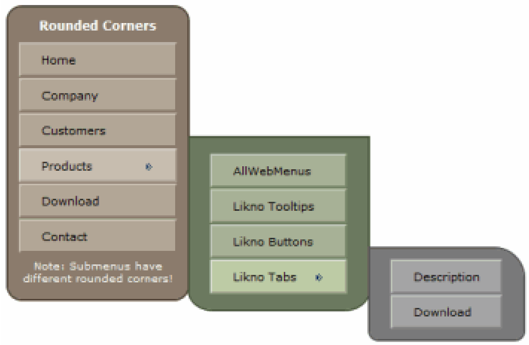
Implementation

Firefox 3.7a4

SpiderMonkey

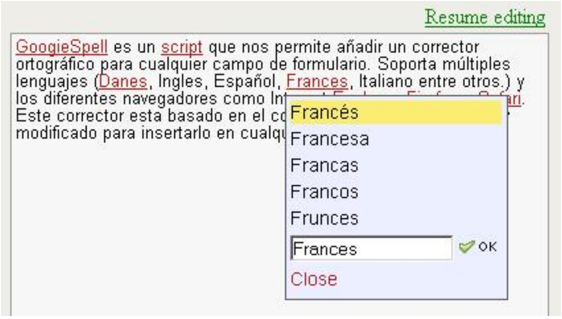
{ Speculate construct
Speculation object
Suspend/Resume
Read/Write logs } JS

Applicability of Transcript



JS Menu: No network or cookie access

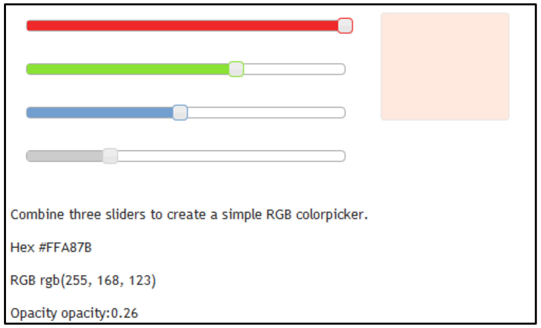
Picture Puzzle: Disallow attaching key event handlers



GoogieSpell es un script que nos permite añadir un corrector ortográfico para cualquier campo de formulario. Soporta múltiples lenguajes (Danes, Ingles, Español, Frances, Italiano entre otros.) y los diferentes navegadores como Int ari.
Este corrector esta basado en el co
modificado para insertarlo en cualqu

Spell Checker: No **Ajax** if cookies were read

GreyBox: `<iframe>`s to whitelisted URLs only



Combine three sliders to create a simple RGB colorpicker.

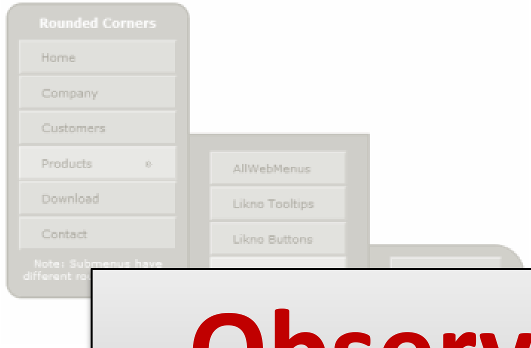
Hex #FFA87B

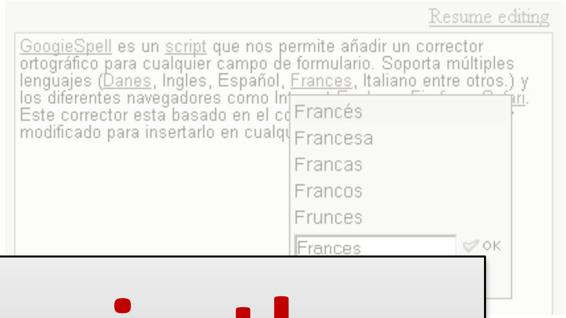
RGB rgb(255, 168, 123)

Opacity opacity:0.26

Color Picker: No `innerHTML` in host's context

Applicability of Transcript



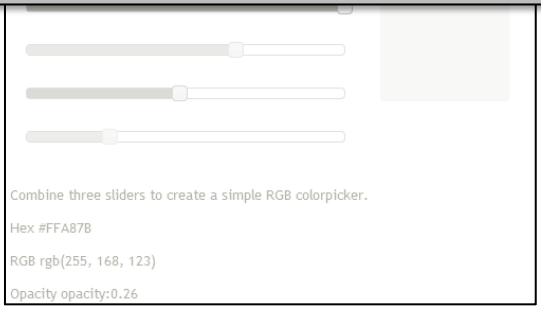


GoogieSpell es un script que nos permite añadir un corrector ortográfico para cualquier campo de formulario. Soporta múltiples lenguajes (Danes, Ingles, Español, Frances, Italiano entre otros.) y los diferentes navegadores como In
Este corrector esta basado en el co
modificado para insertarlo en cualqu

Observed no change in the behavior of third party code

JS Men

ere read



Combine three sliders to create a simple RGB colorpicker.

Hex #FFA87B

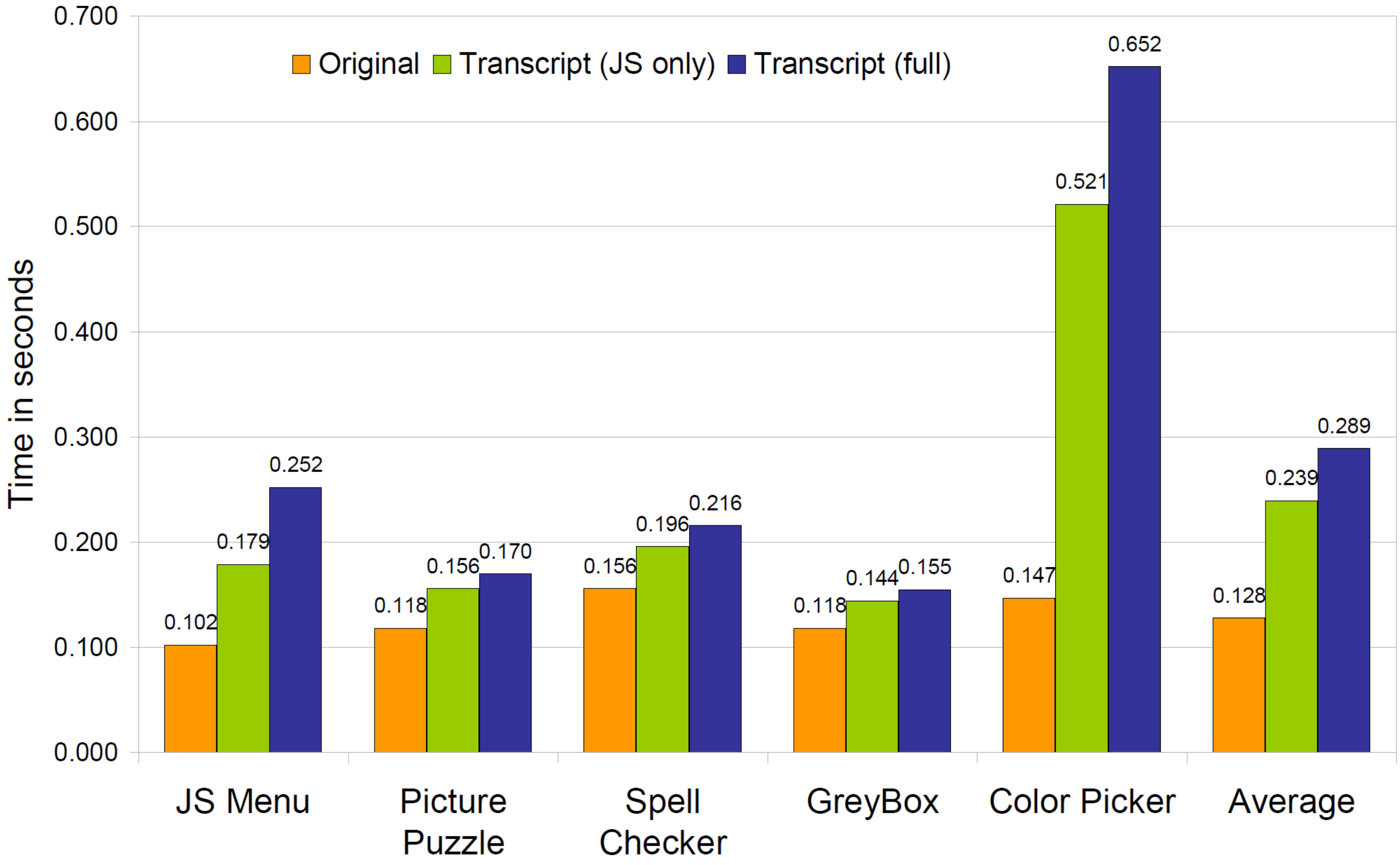
RGB rgb(255, 168, 123)

Opacity opacity:0.26

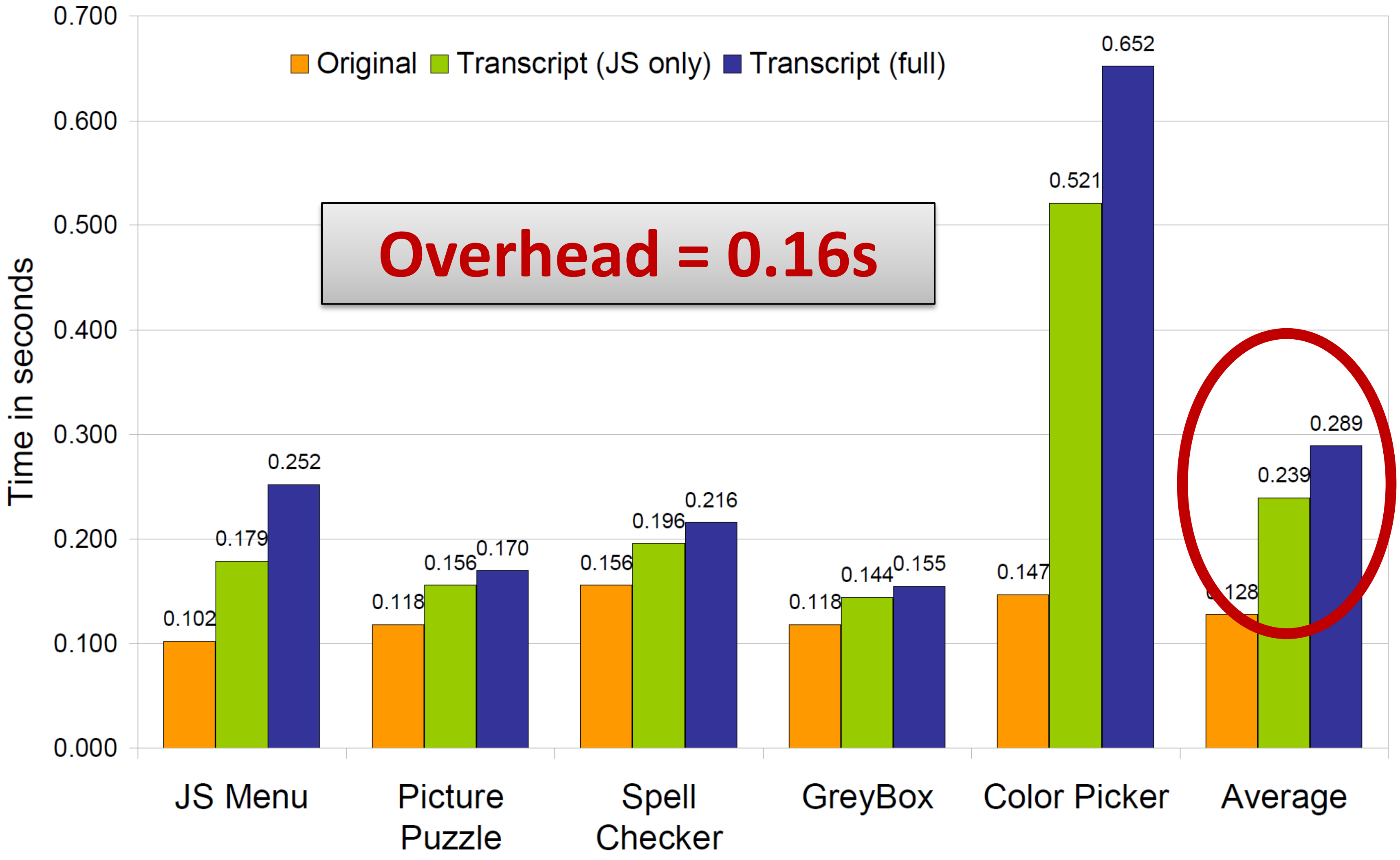
GreyBox: `<iframe>`s to whitelisted URLs only

Color Picker: No `innerHTML` in host's context

Application benchmarks

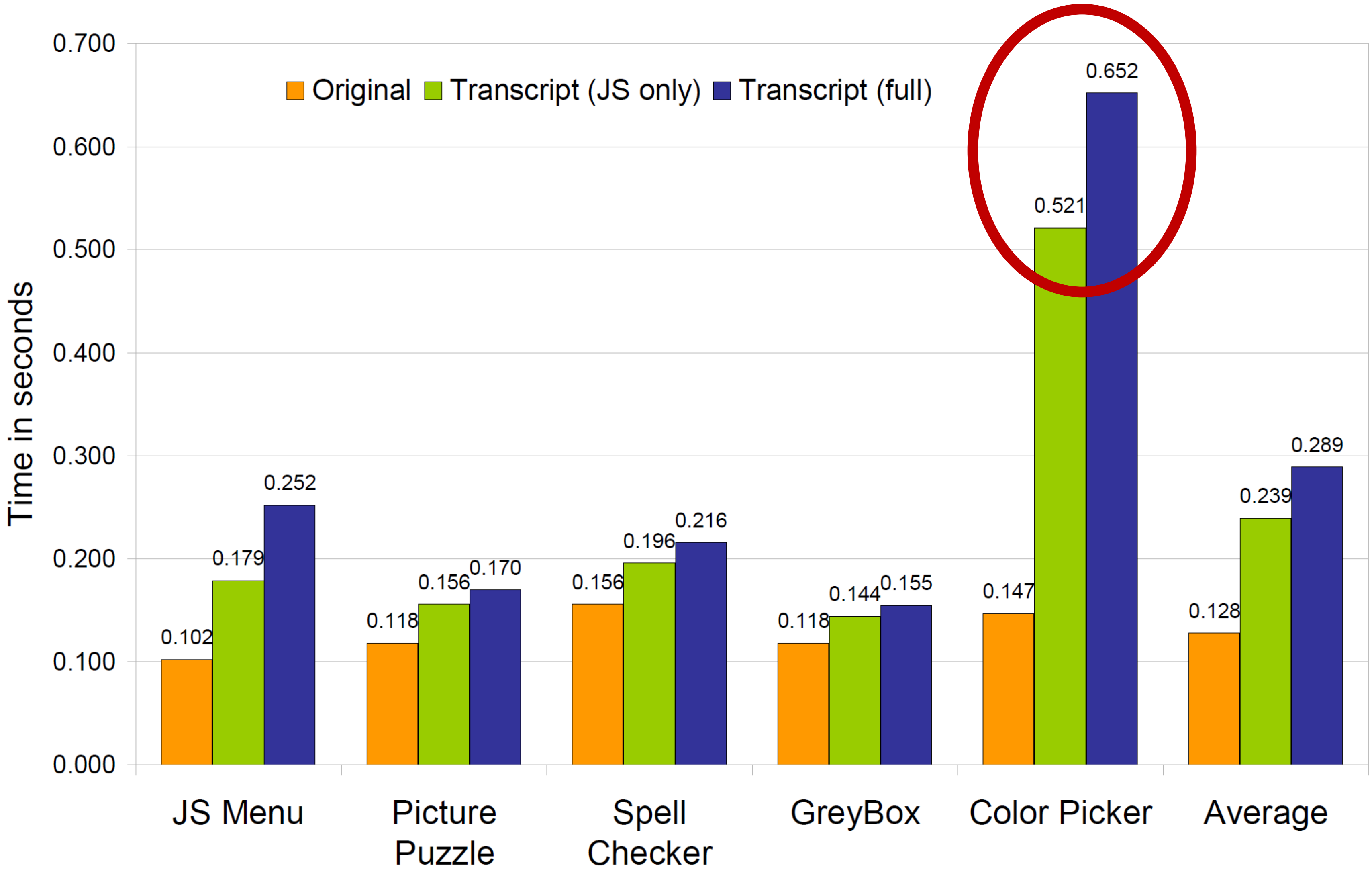


Application benchmarks



Overhead = 0.16s

Application benchmarks

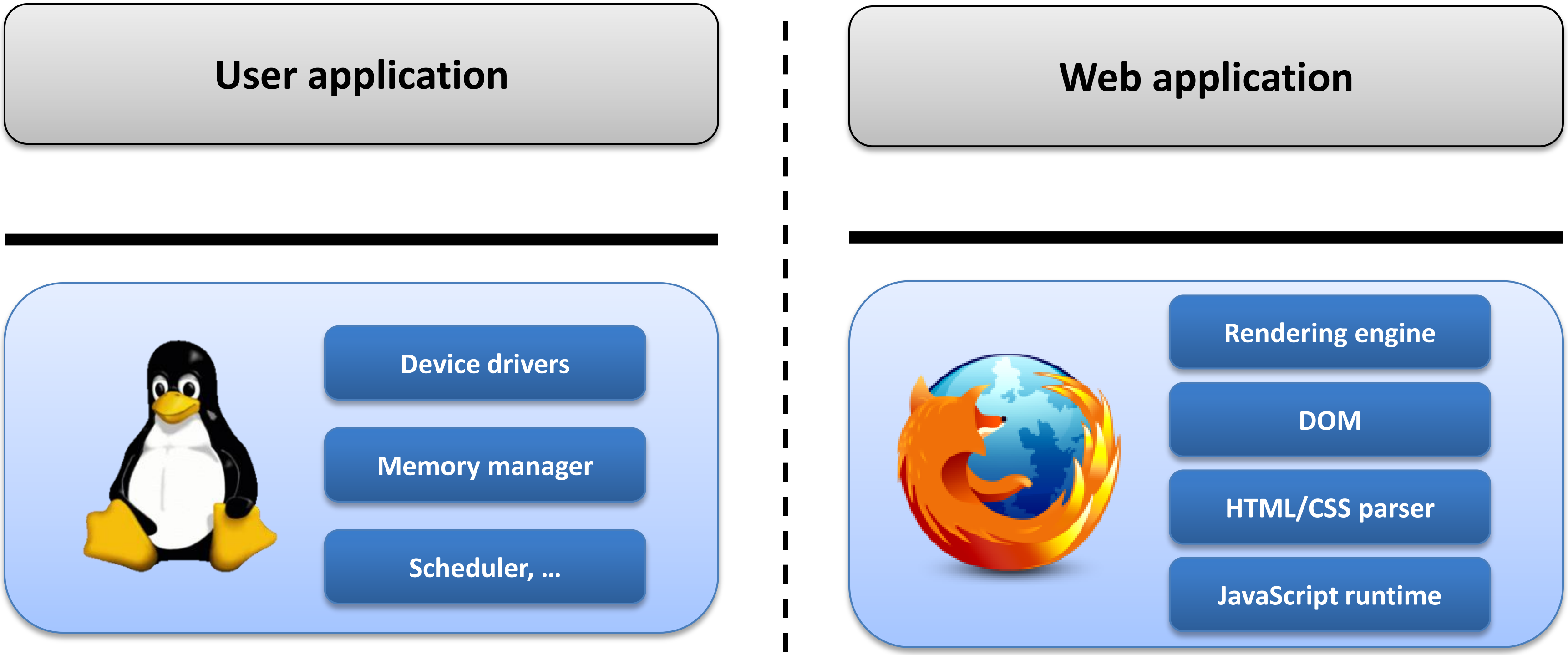


Summary: Part I

- **Sabre uses information flow tracking across browser subsystems to prevent security and privacy violations**
  - Exploited browser extensions can cause loss of sensitive information
- **Transcript implements speculative execution for JavaScript to provide isolation & recovery**
  - Enforcement of powerful security policies
  - No restriction or changes to third party code

Part II: Enhancing Web platform extensibility with Atlantis

Analogy: OS and Web browser



User application

Device drivers

Memory manager

Scheduler, …

Operating system

Web application

Rendering engine

DOM

HTML/CSS parser

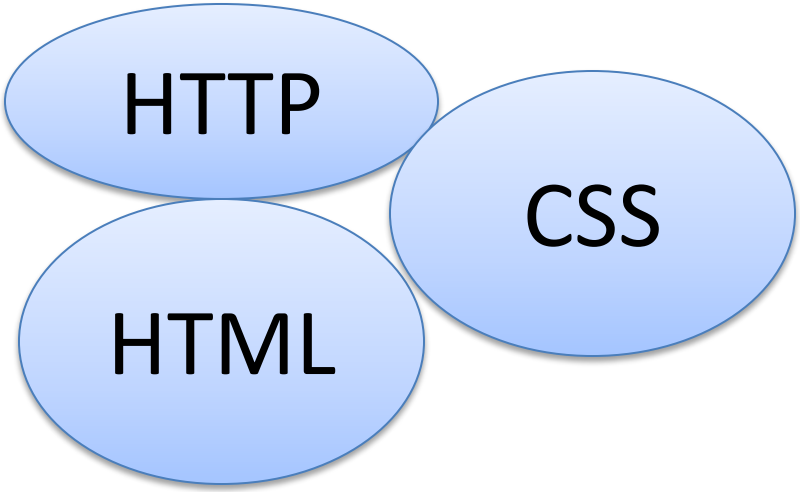
JavaScript runtime

Web browser

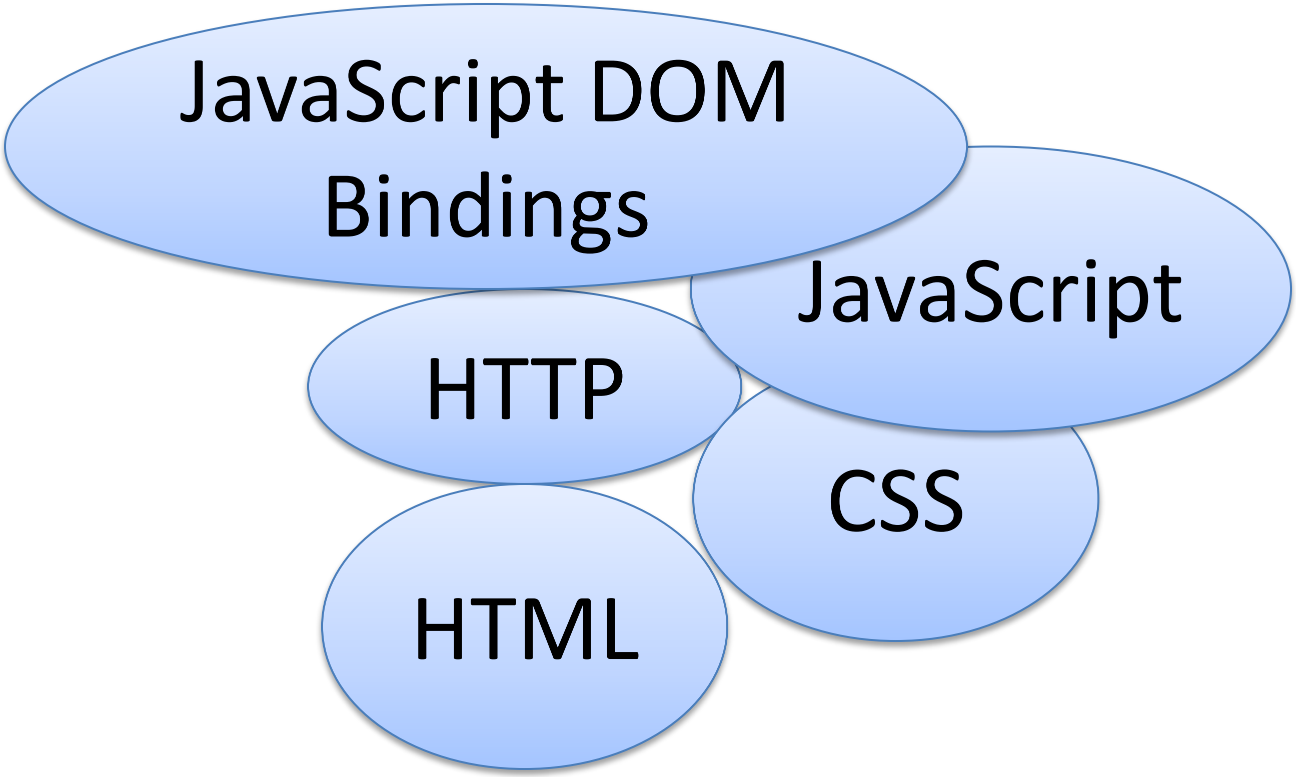
The Web protocol

HTTP

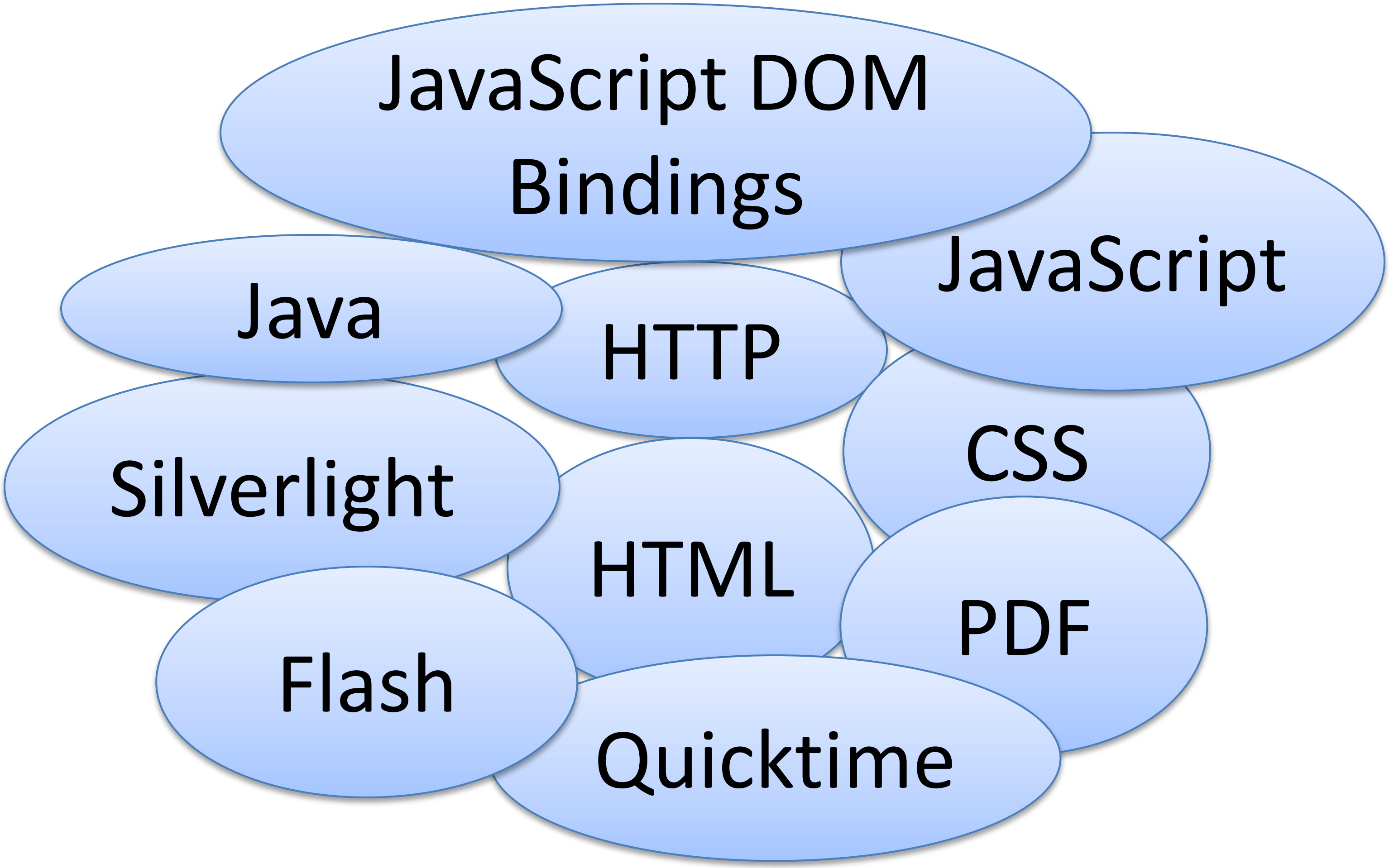
The Web protocol



The Web protocol



The Web protocol



JavaScript DOM Bindings

JavaScript

Java

HTTP

Silverlight

CSS

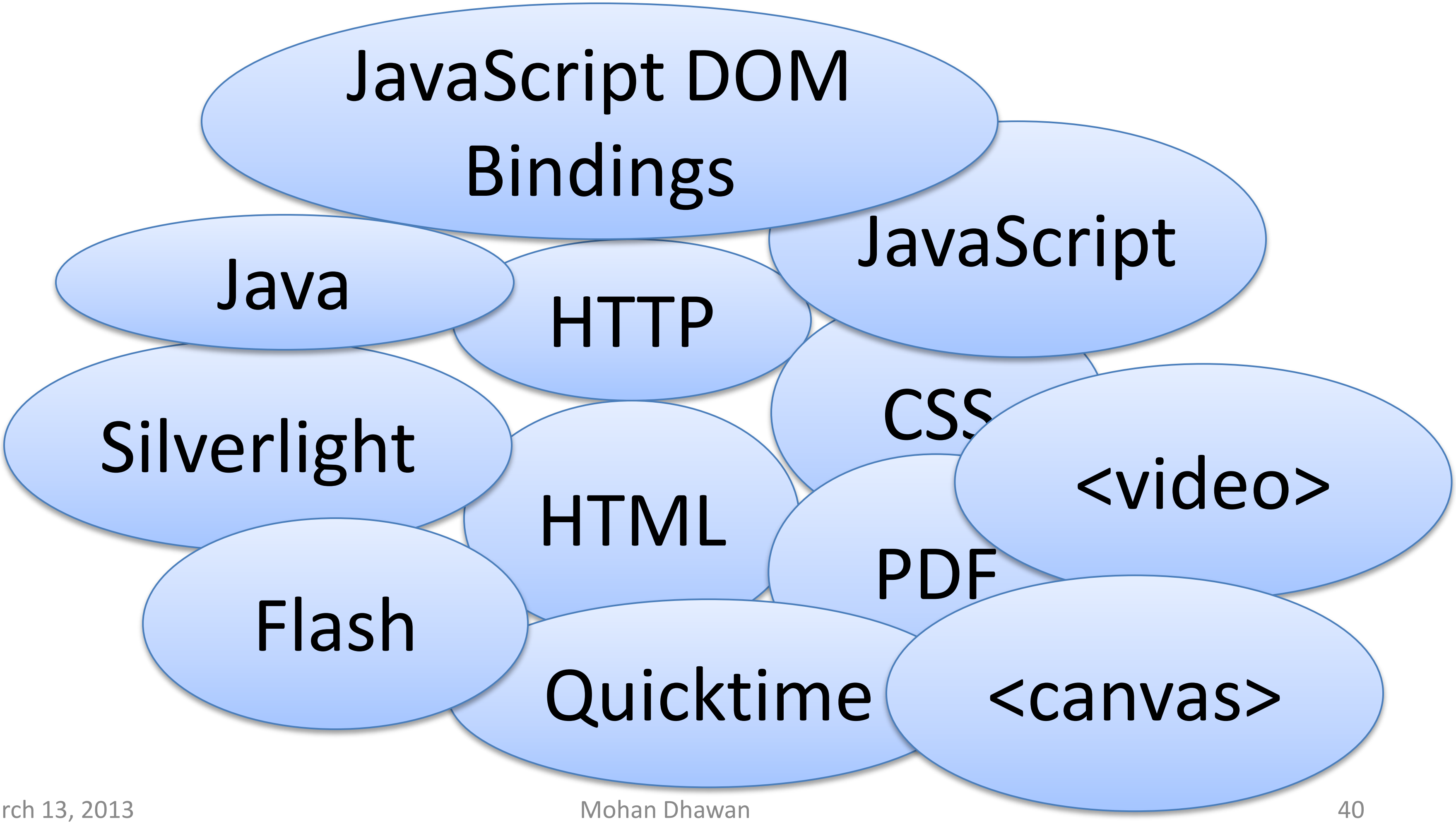
HTML

PDF

Flash

Quicktime

The Web protocol



JavaScript DOM Bindings

Java

HTTP

JavaScript

Silverlight

CSS

HTML

<video>

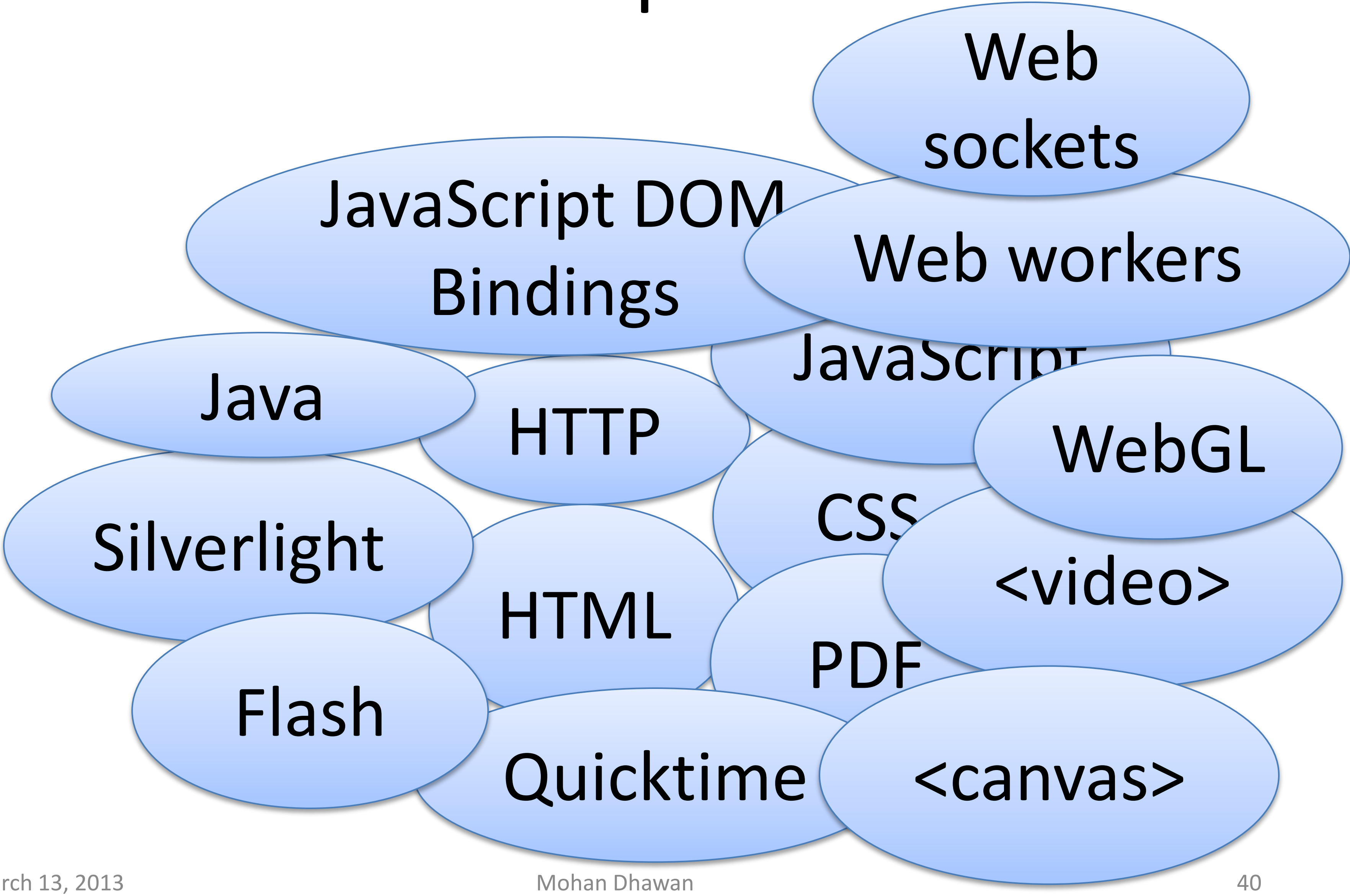
PDF

Flash

Quicktime

<canvas>

The Web protocol



Web sockets

JavaScript DOM Bindings

Web workers

Java

HTTP

JavaScript

WebGL

Silverlight

HTML

CSS

<video>

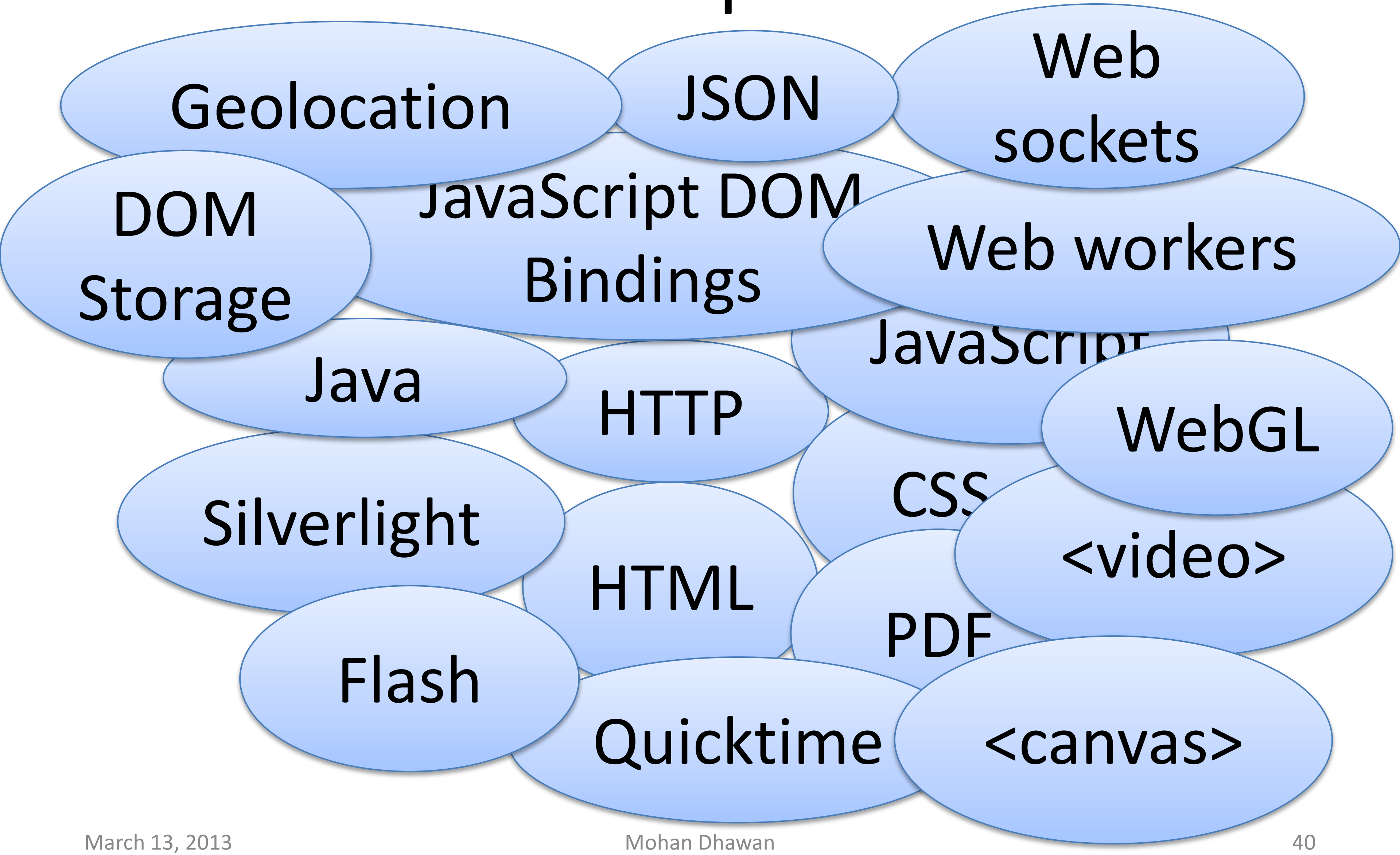
PDF

Flash

Quicktime

<canvas>

The Web protocol



Geolocation

JSON

Web sockets

DOM Storage

JavaScript DOM Bindings

Web workers

Java

HTTP

JavaScript

WebGL

Silverlight

HTML

CSS

<video>

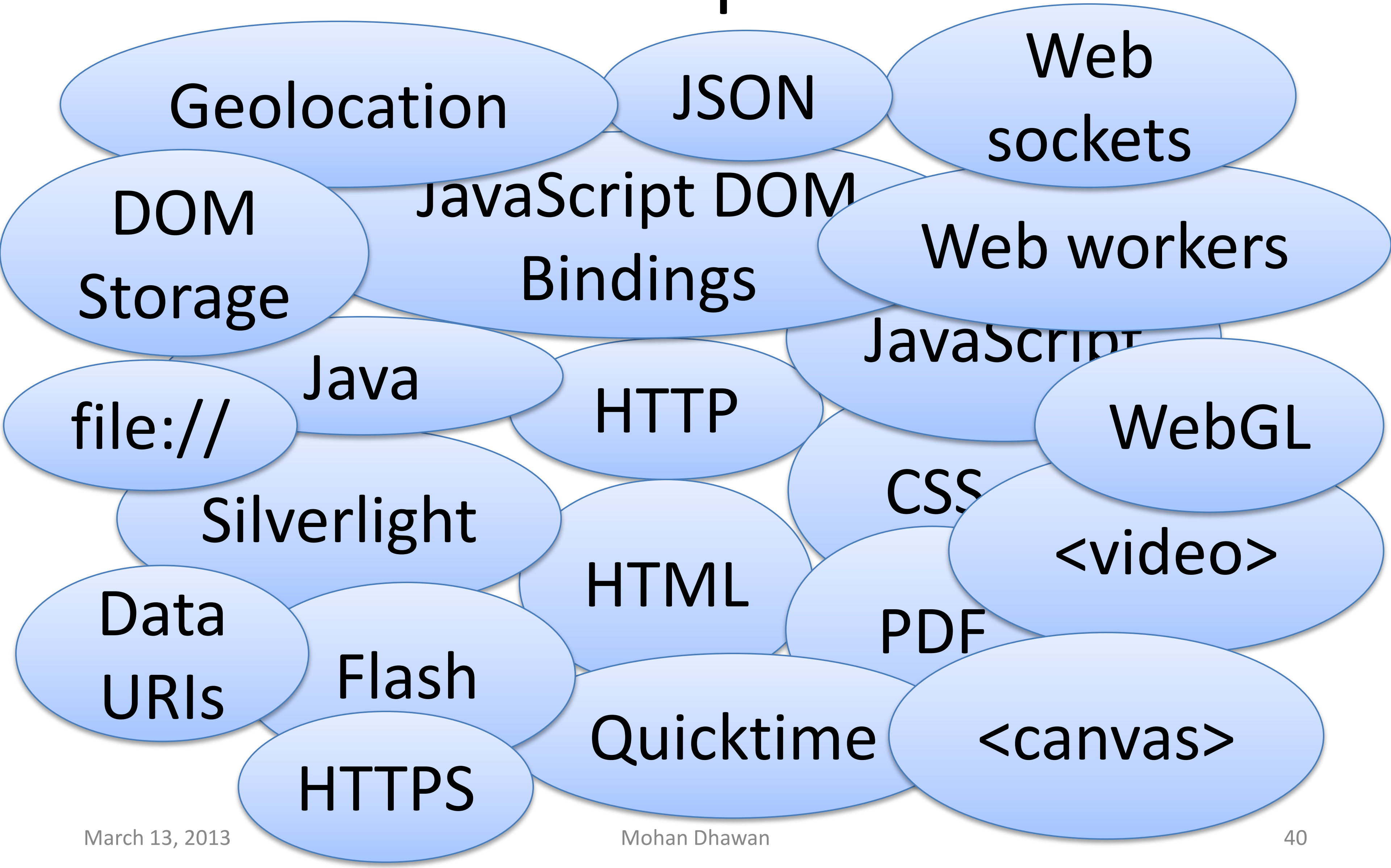
PDF

Flash

Quicktime

<canvas>

The Web protocol



Geolocation

JSON

Web sockets

DOM Storage

JavaScript DOM Bindings

Web workers

Java

JavaScript

file://

HTTP

WebGL

CSS

Silverlight

<video>

HTML

Data URIs

PDF

Flash

Quicktime

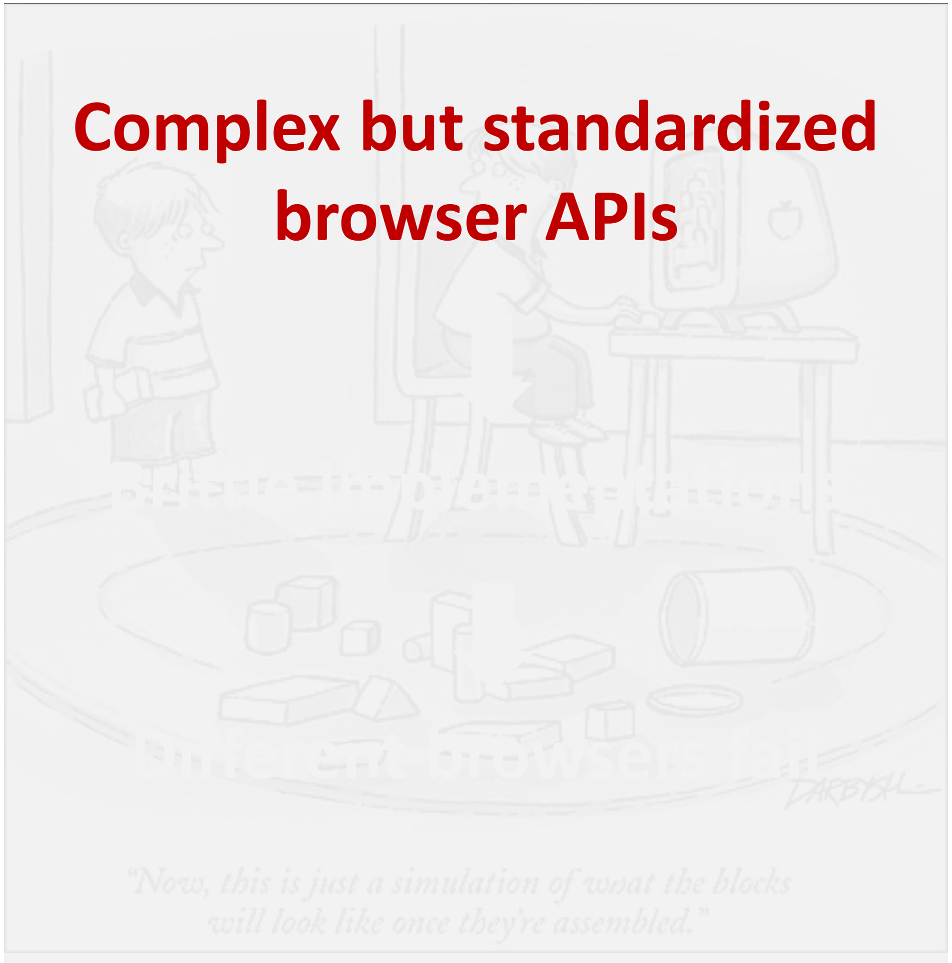
<canvas>

HTTPS

The ***complex*** Web protocol

"Now, this is just a simulation of what the blocks will look like once they're assembled."

The *complex* Web protocol



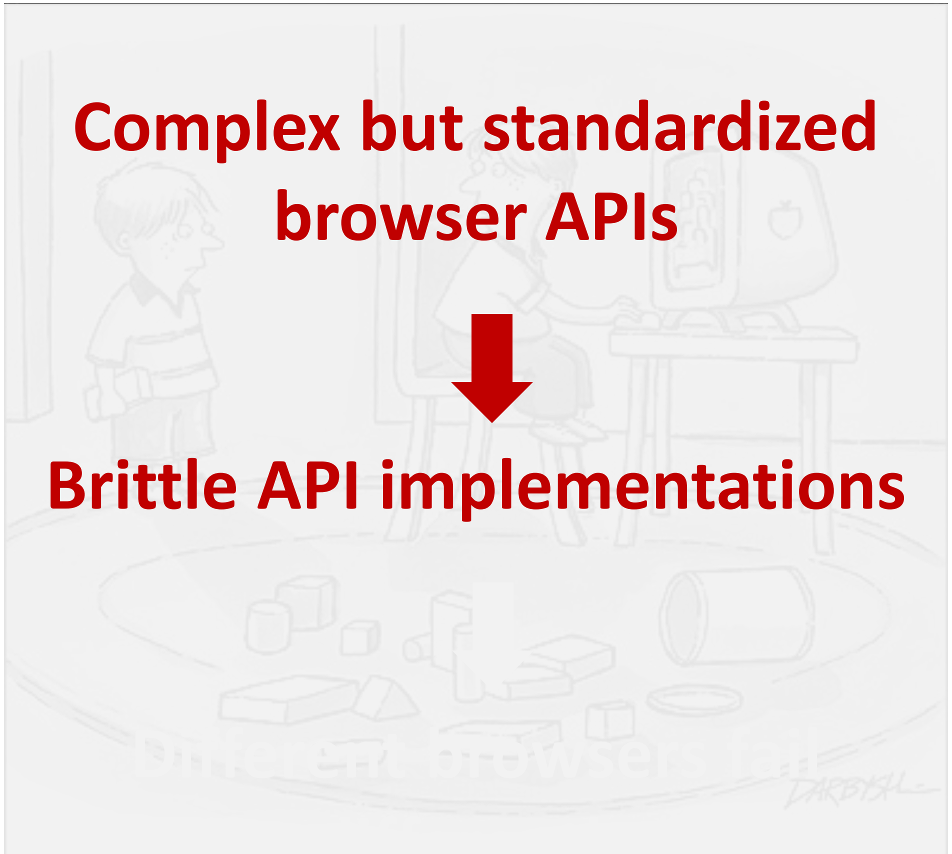
"Now, this is just a simulation of what the blocks will look like once they're assembled."

Complex but standardized browser APIs

Brittle implementations

Different browsers fail

The *complex* Web protocol



Complex but standardized browser APIs

⬇

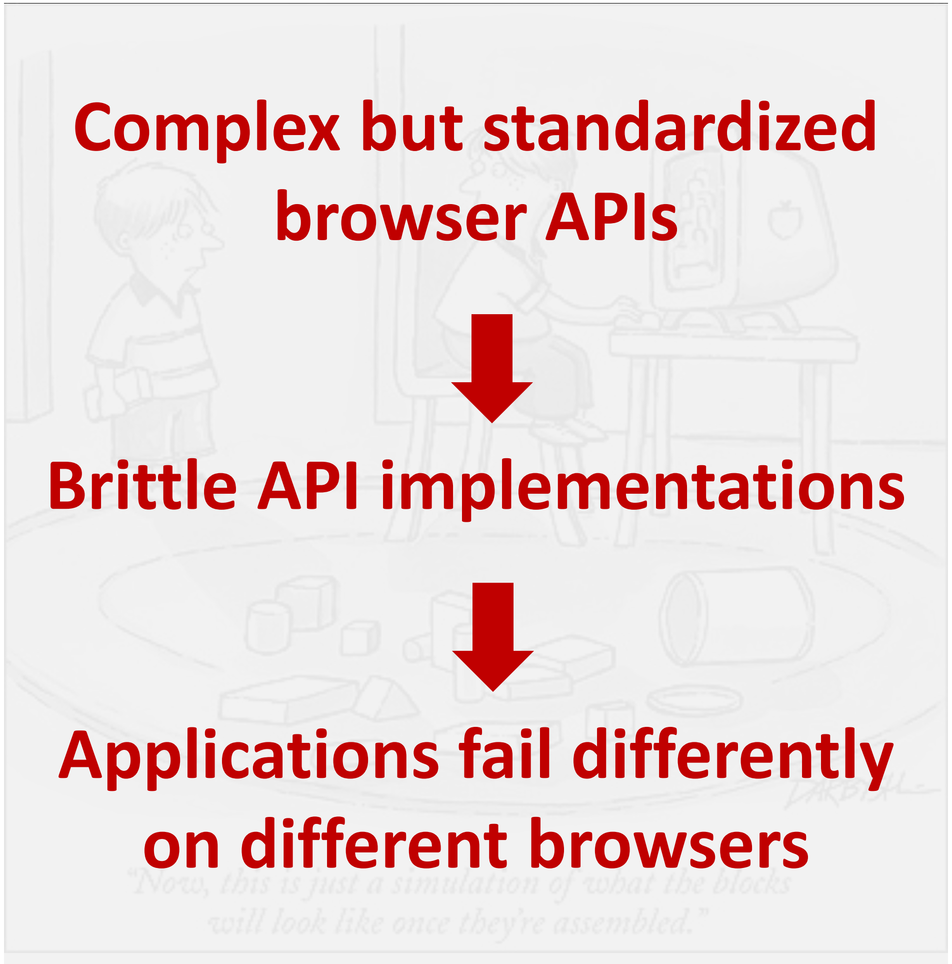
Brittle API implementations

⬇

Different browsers fail

"Now, this is just a simulation of what the blocks will look like once they're assembled."

The *complex* Web protocol



Complex but standardized browser APIs

↓

Brittle API implementations

↓

Applications fail differently on different browsers

"Now, this is just a simulation of what the blocks will look like once they're assembled."

The ***complex*** Web protocol

Complex but standardized browser APIs

Hard to write secure and robust Web applications

Applications fail differently on different browsers

Example: IE's `Event` interface bug

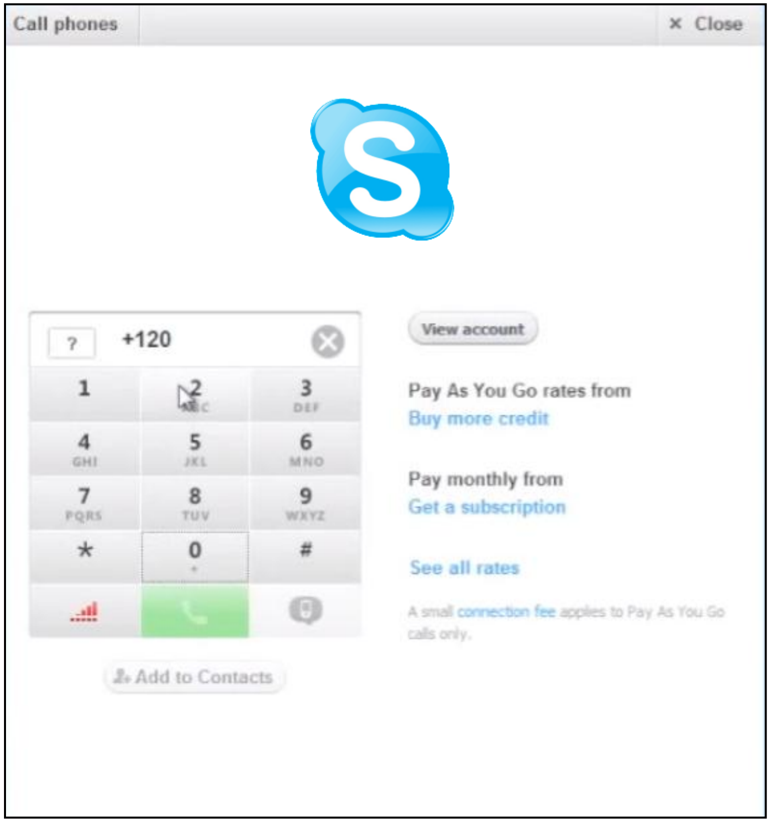
Security vulnerability in IE v6-10, allows mouse cursor to be tracked anywhere on the screen even if IE is minimized

Example: IE's `Event` interface bug

Security vulnerability in IE v6-10, allows mouse cursor to be tracked anywhere on the screen even if IE is minimized

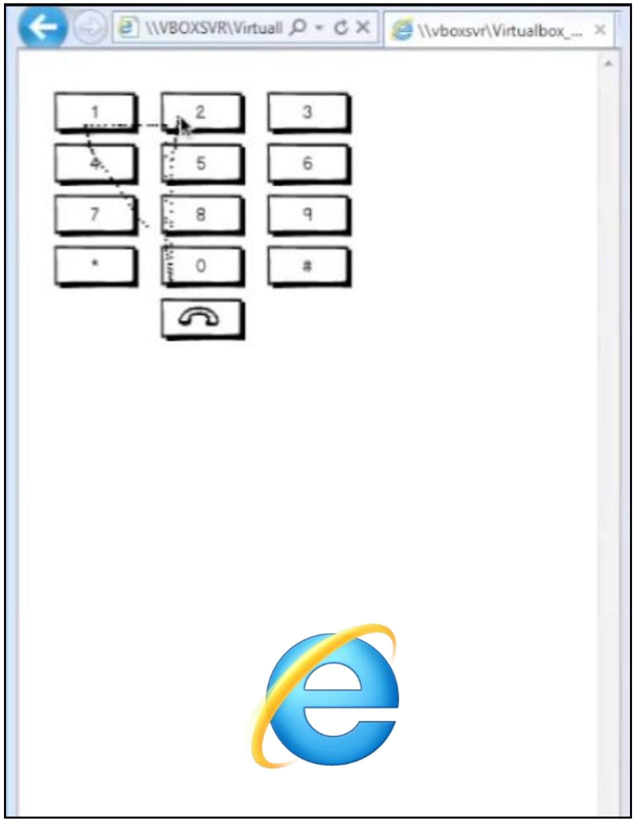
Virtual keyboards and keypads are no longer safe

Example: IE's `Event` interface bug



A small connection fee applies to Pay As You Go calls only.

Skype



IE running exploit code

Example: IE's `Event` interface bug

Security vulnerability in IE v6-10, allows mouse cursor to be tracked anywhere on the screen even if IE is minimized

An attacker can access all mouse movements simply by displaying ads on Web pages

Example: IE's `Event` interface bug

Security vulnerability in IE v6-10, allows mouse cursor to be tracked anywhere on the screen even if IE is minimized

- YouTube and NYTimes potential attack vectors
- Bug already exploited by two ad analytics firms

Example: IE's `Event` interface bug

Security vulnerability in IE v6-10, allows mouse cursor to be tracked anywhere on the screen even if IE is minimized

- IE's DOM implementation populates the `Event` object with mouse events & attributes
- JavaScript can poll for mouse coordinates, but allowed only for pages in focus with cursor in it

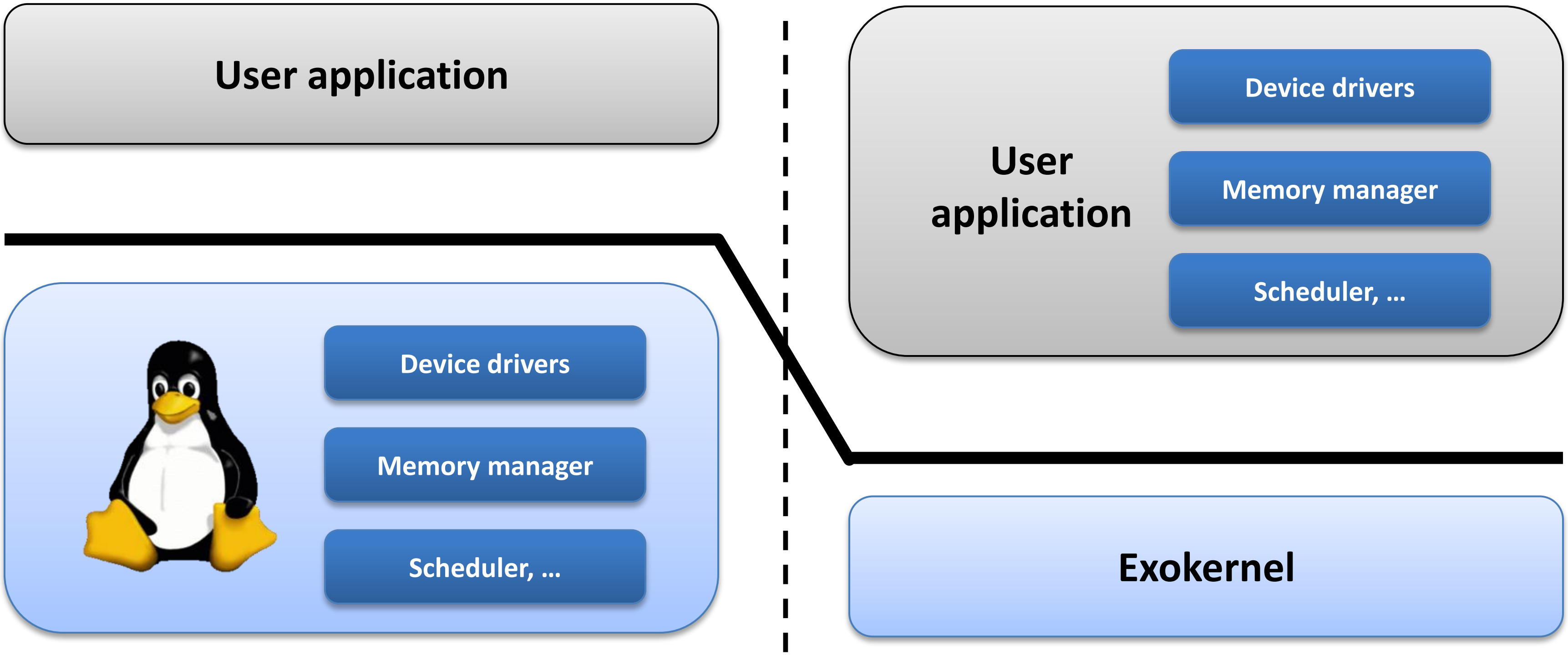
Example: IE's `Event` interface bug

Security vulnerability in IE v6-10, allows mouse cursor to be

Hard to write secure and robust Web applications

- JavaScript can poll for mouse coordinates, but allowed only for focused pages with cursor in it

Monolithic v/s Exokernel



User application

Device drivers

Memory manager

Scheduler, …

User application

Device drivers

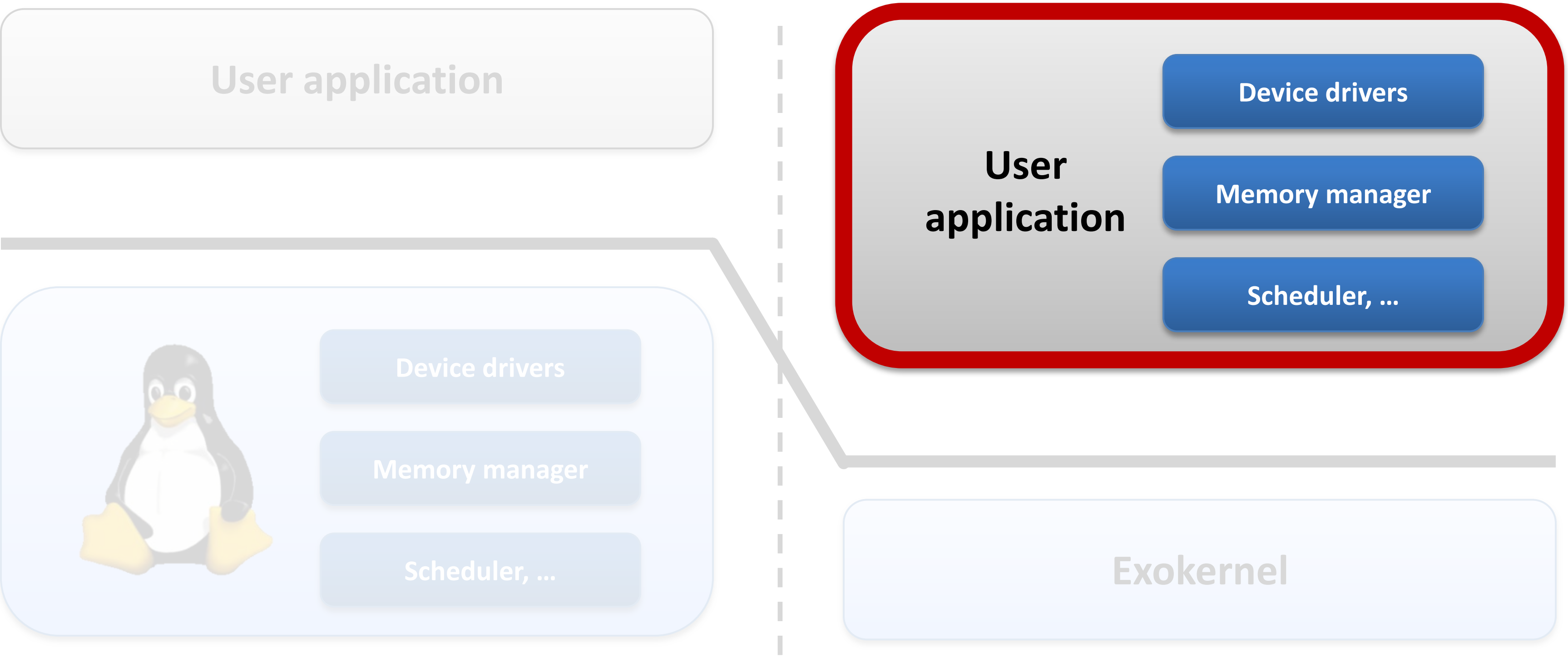
Memory manager

Scheduler, …

Exokernel

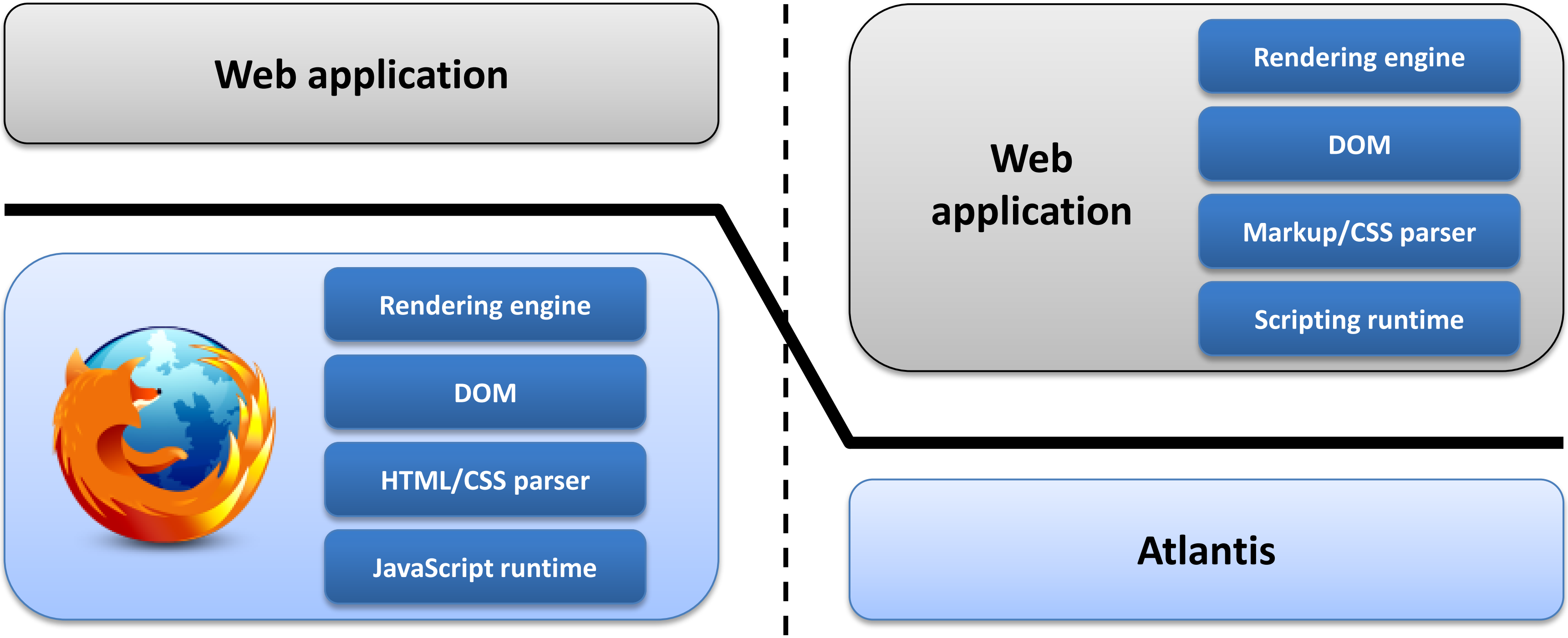
Monolithic v/s Exokernel

User application manages complexity

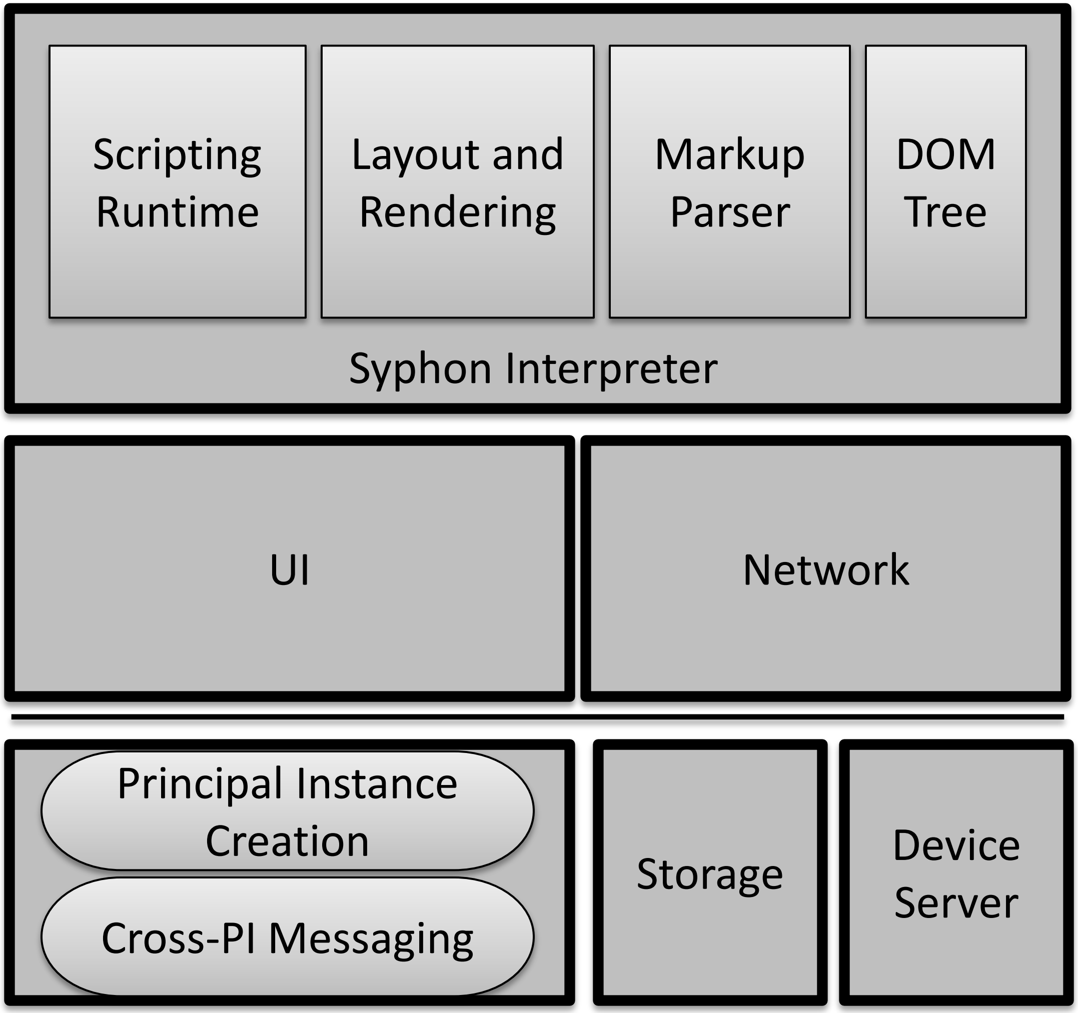


Our solution: Atlantis

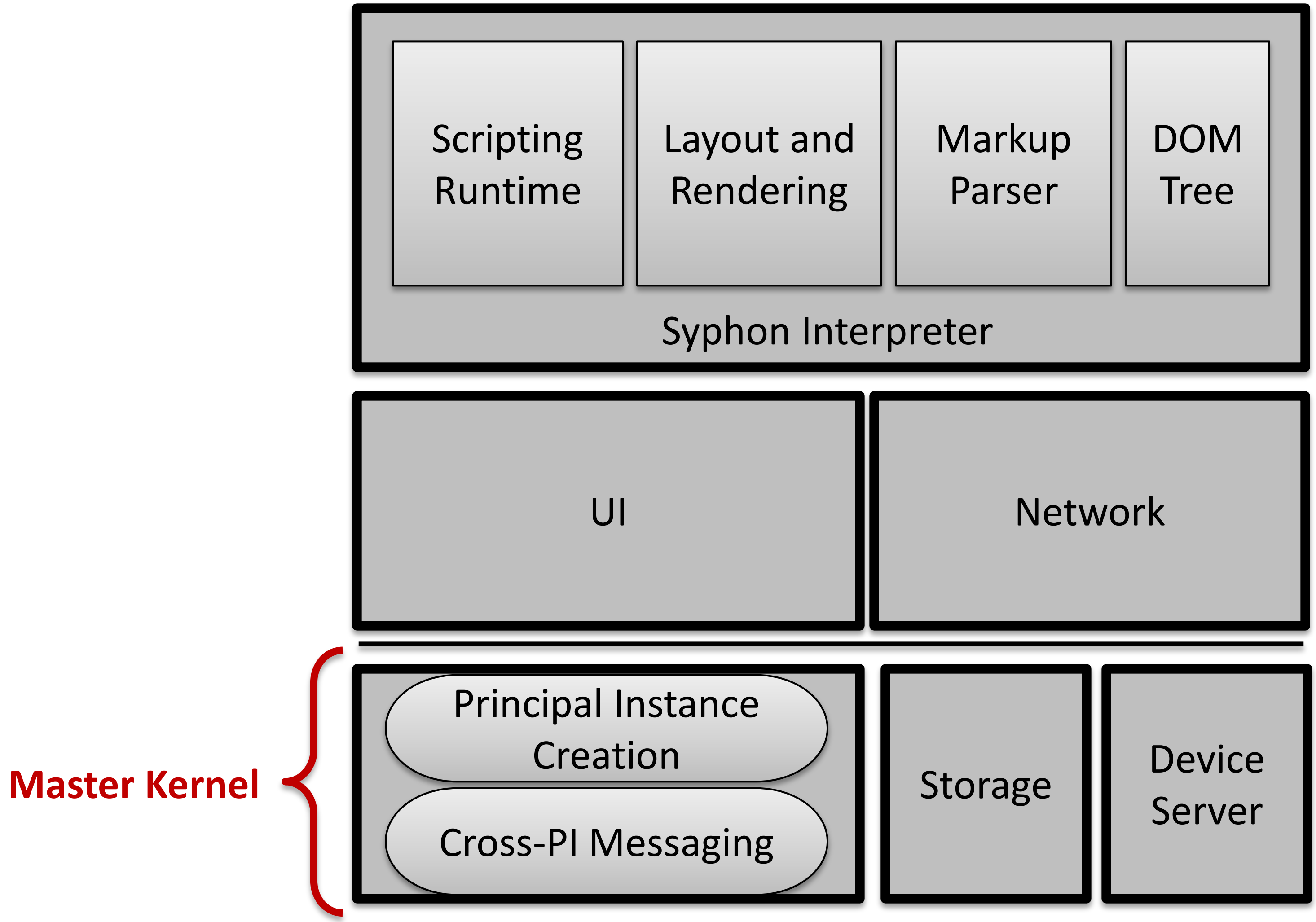
Extensibility enhances security & robustness



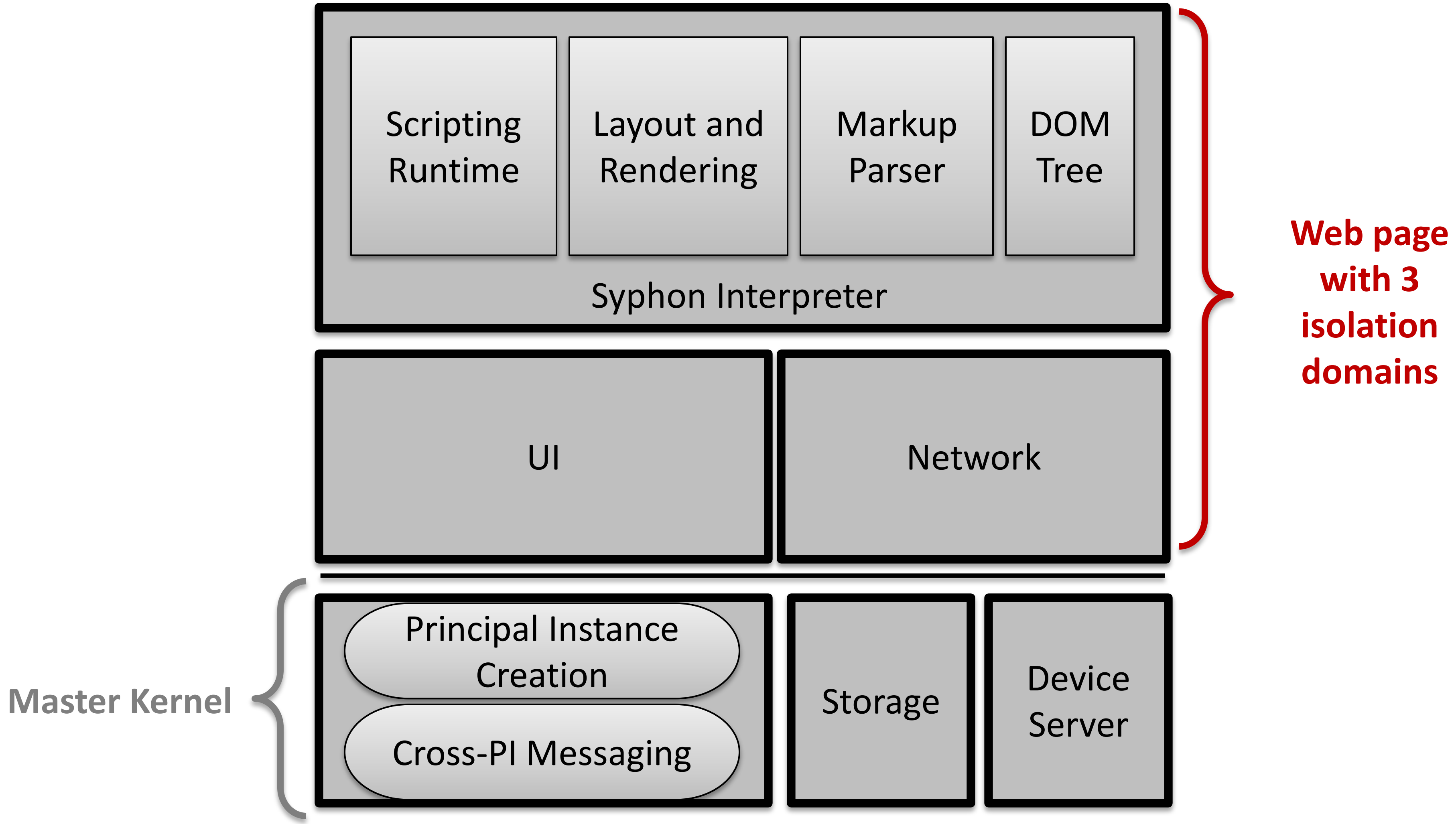
Atlantis architecture



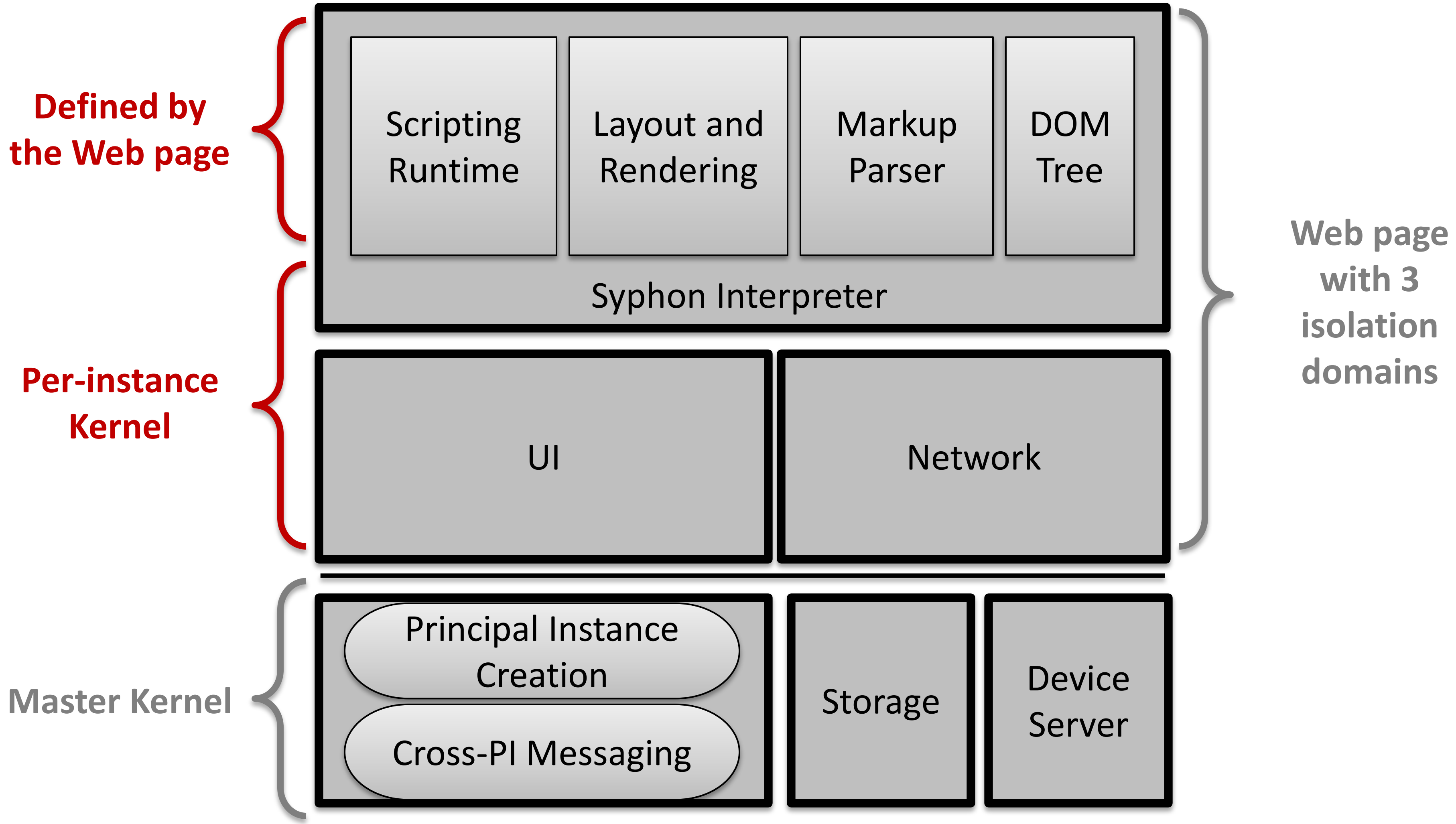
Atlantis architecture



Atlantis architecture



Atlantis architecture



Defining the Web stack

```
<environment>
  <compiler=‘http://foo/compiler.syp’>
  <markupParser=‘http://bar/mParser.js’>
  <runtime=‘http://baz/runtime.js’>
</environment>
```

Syphon Interpreter

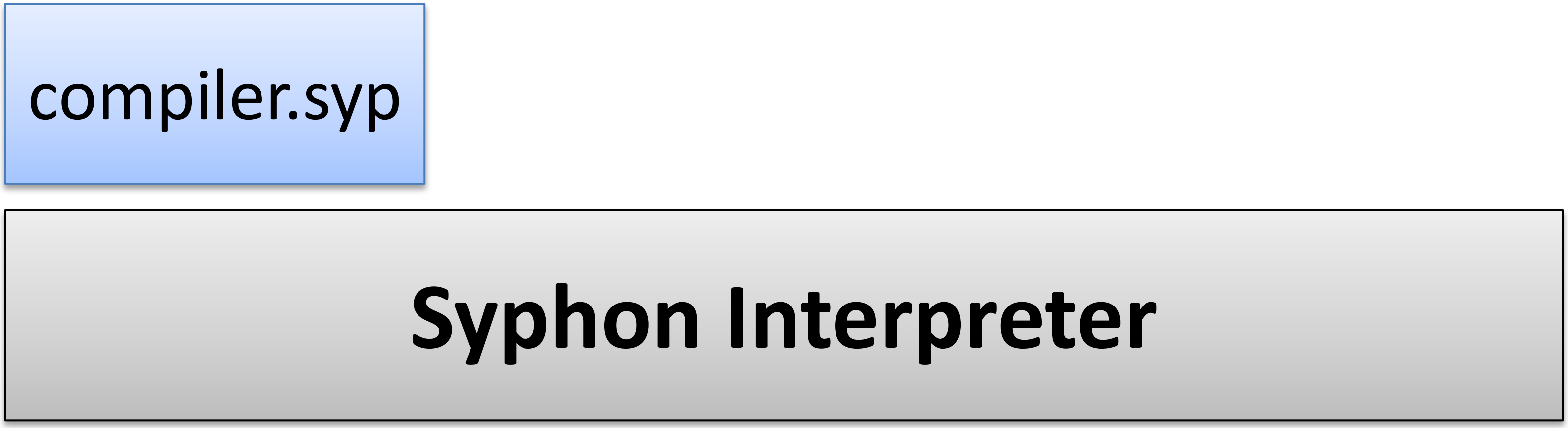
Defining the Web stack

```
<environment>
  <compiler=‘http://foo/compiler.syp’>
  <markupParser=‘http://bar/mParser.js’>
  <runtime=‘http://baz/runtime.js’>
</environment>
```

Syphon Interpreter

Defining the Web stack

```
<environment>
  <compiler=‘http://foo/compiler.syp’>
  <markupParser=‘http://bar/mParser.js’>
  <runtime=‘http://baz/runtime.js’>
</environment>
```

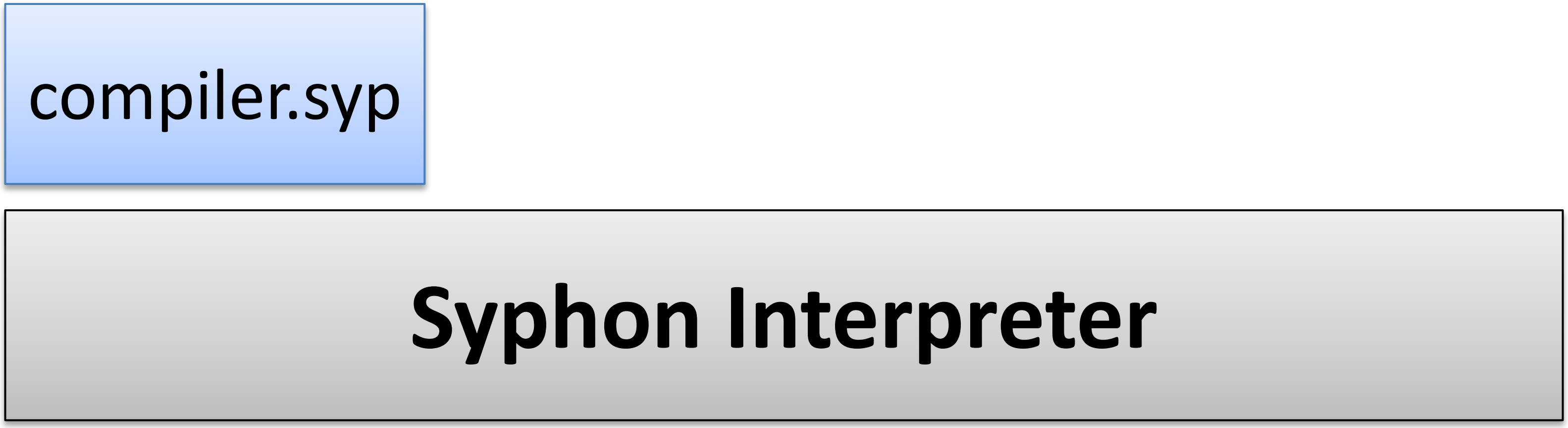


compiler.syp

Syphon Interpreter

Defining the Web stack

```
<environment>
  <compiler=‘http://foo/compiler.syp’>
  <markupParser=‘http://bar/mParser.js’>
  <runtime=‘http://baz/runtime.js’>
</environment>
```

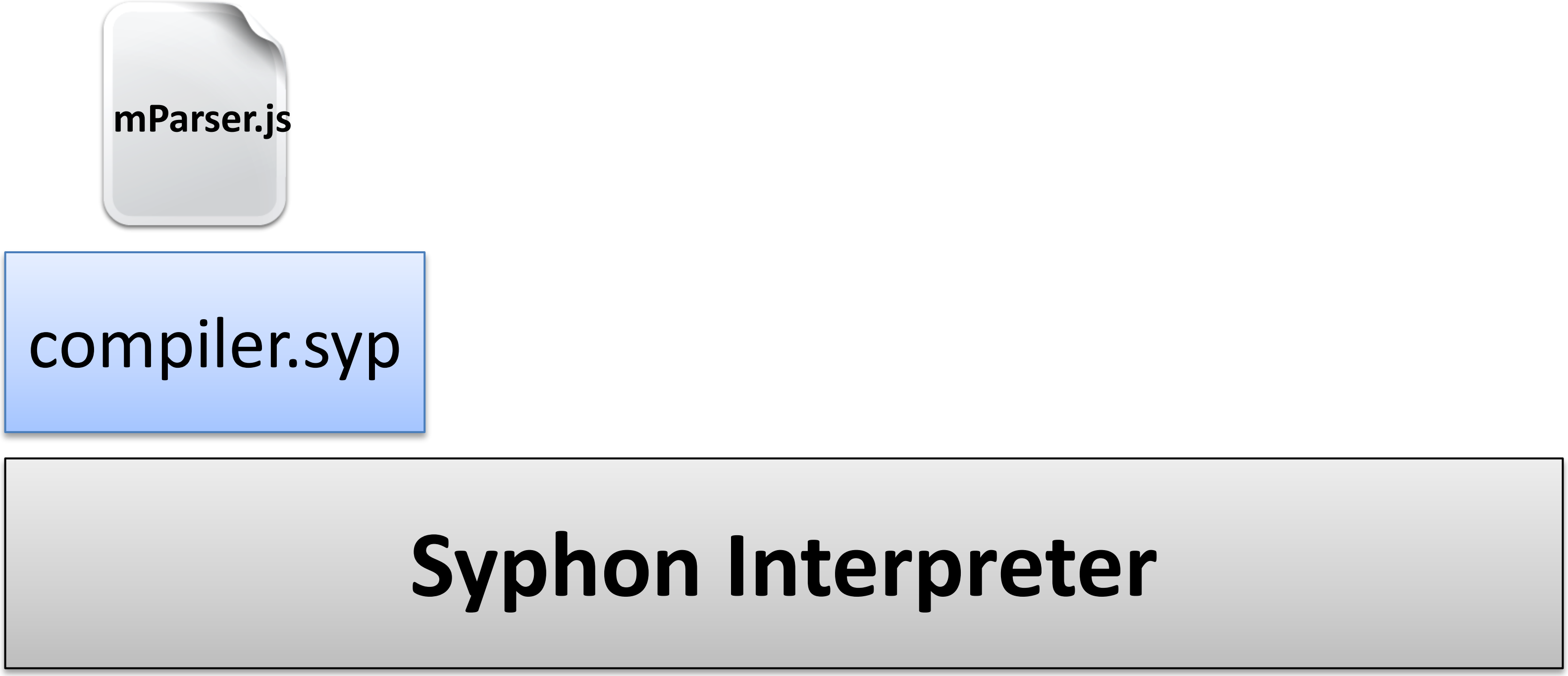


compiler.syp

Syphon Interpreter

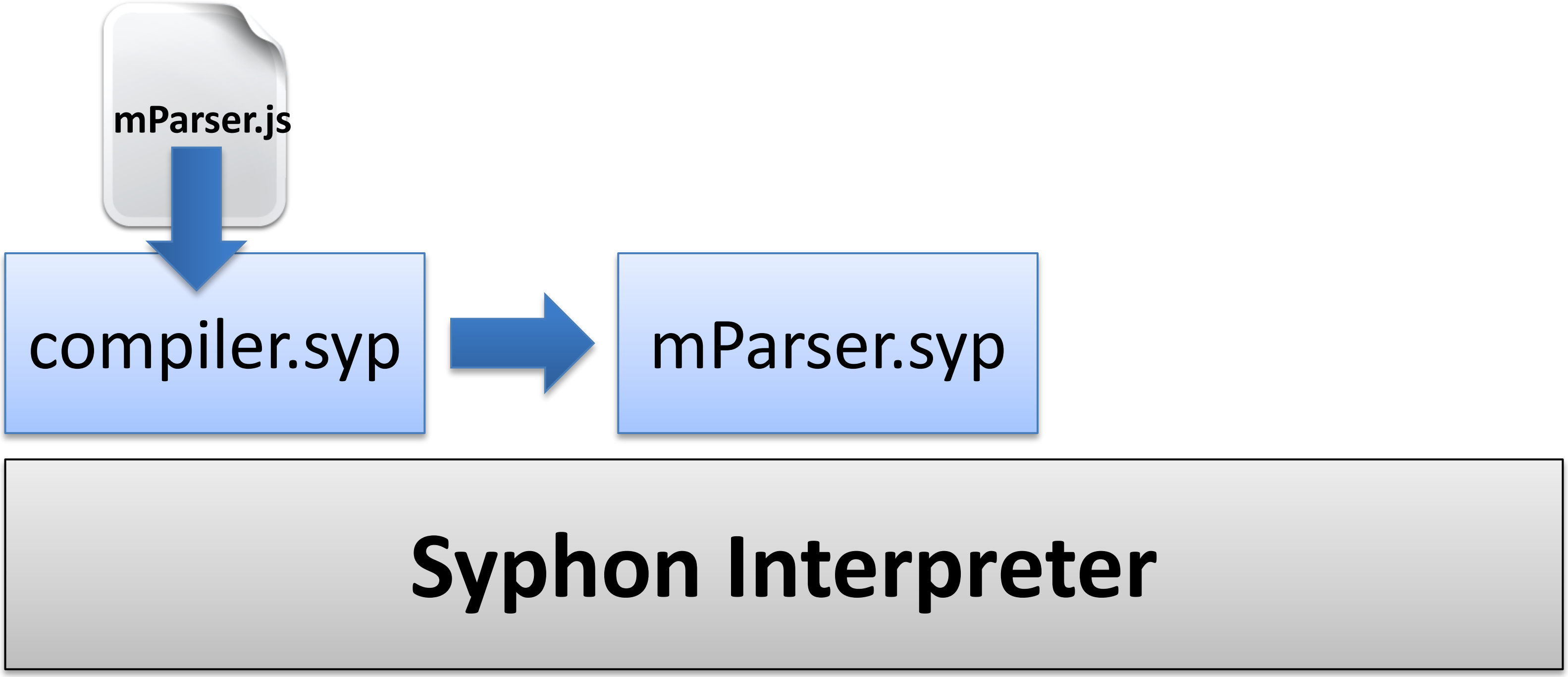
Defining the Web stack

```
<environment>
  <compiler=‘http://foo/compiler.syp’>
  <markupParser=‘http://bar/mParser.js’>
  <runtime=‘http://baz/runtime.js’>
</environment>
```



Defining the Web stack

```
<environment>
  <compiler=‘http://foo/compiler.syp’>
  <markupParser=‘http://bar/mParser.js’>
  <runtime=‘http://baz/runtime.js’>
</environment>
```



mParser.js

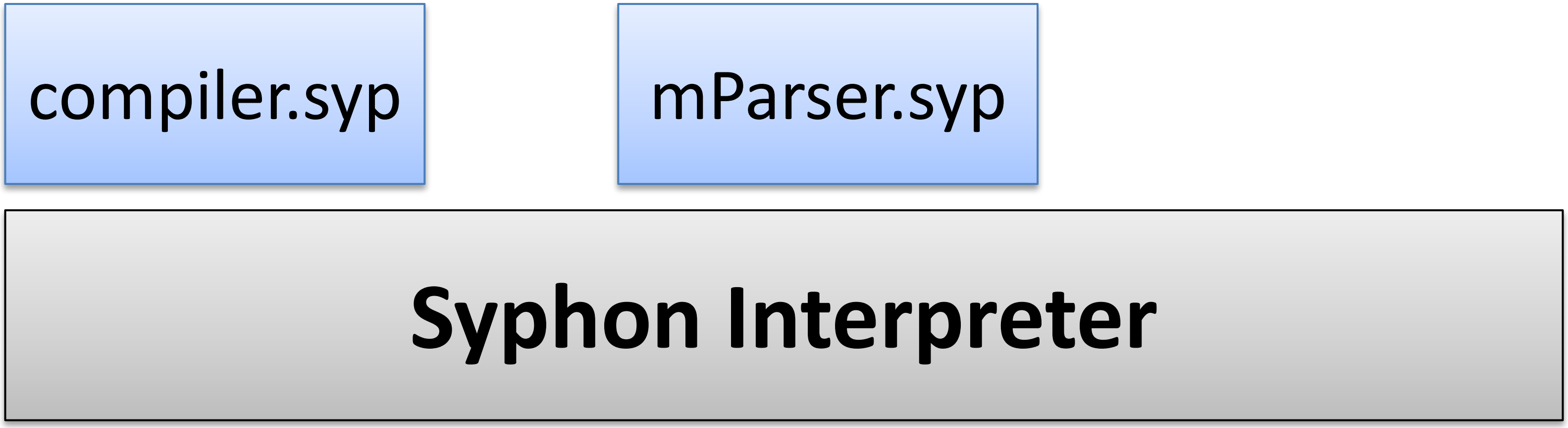
compiler.syp

mParser.syp

Syphon Interpreter

Defining the Web stack

```
<environment>
  <compiler=‘http://foo/compiler.syp’>
  <markupParser=‘http://bar/mParser.js’>
  <runtime=‘http://baz/runtime.js’>
</environment>
```



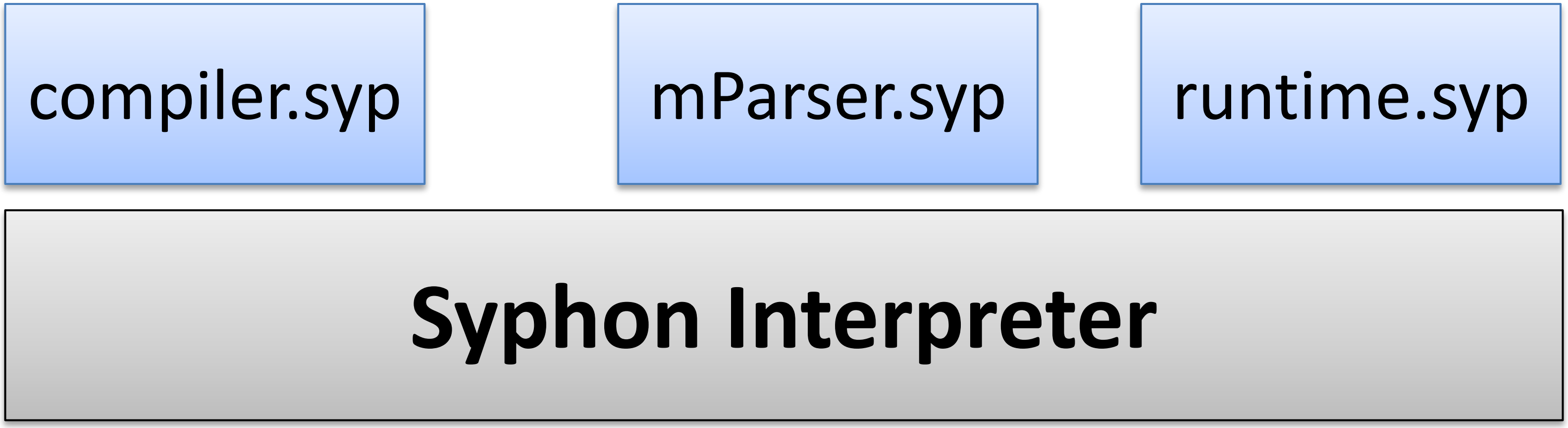
compiler.syp

mParser.syp

Syphon Interpreter

Defining the Web stack

```
<environment>
  <compiler=‘http://foo/compiler.syp’>
  <markupParser=‘http://bar/mParser.js’>
  <runtime=‘http://baz/runtime.js’>
</environment>
```



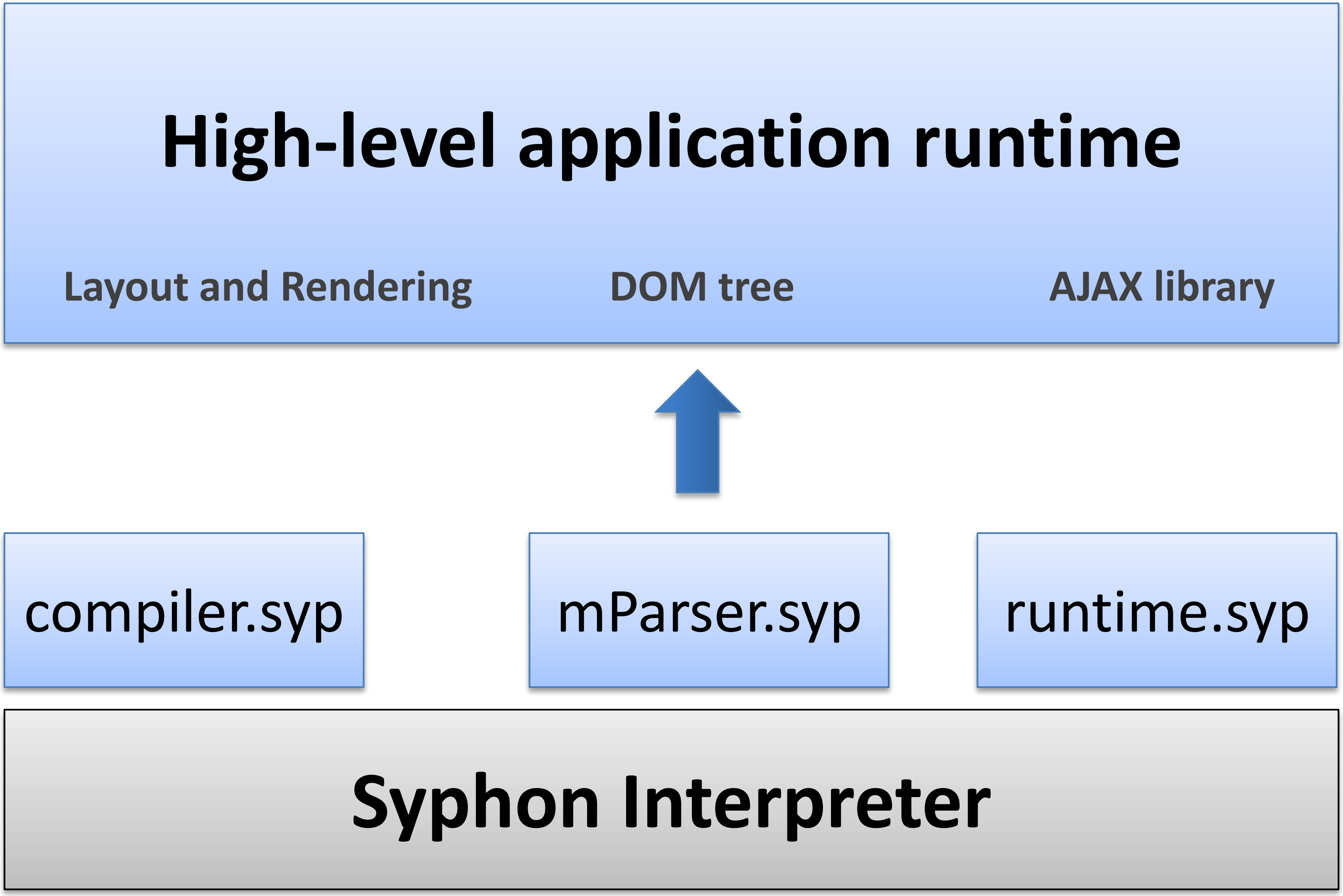
compiler.syp

mParser.syp

runtime.syp

Syphon Interpreter

Defining the Web stack



High-level application runtime

Layout and Rendering

DOM tree

AJAX library

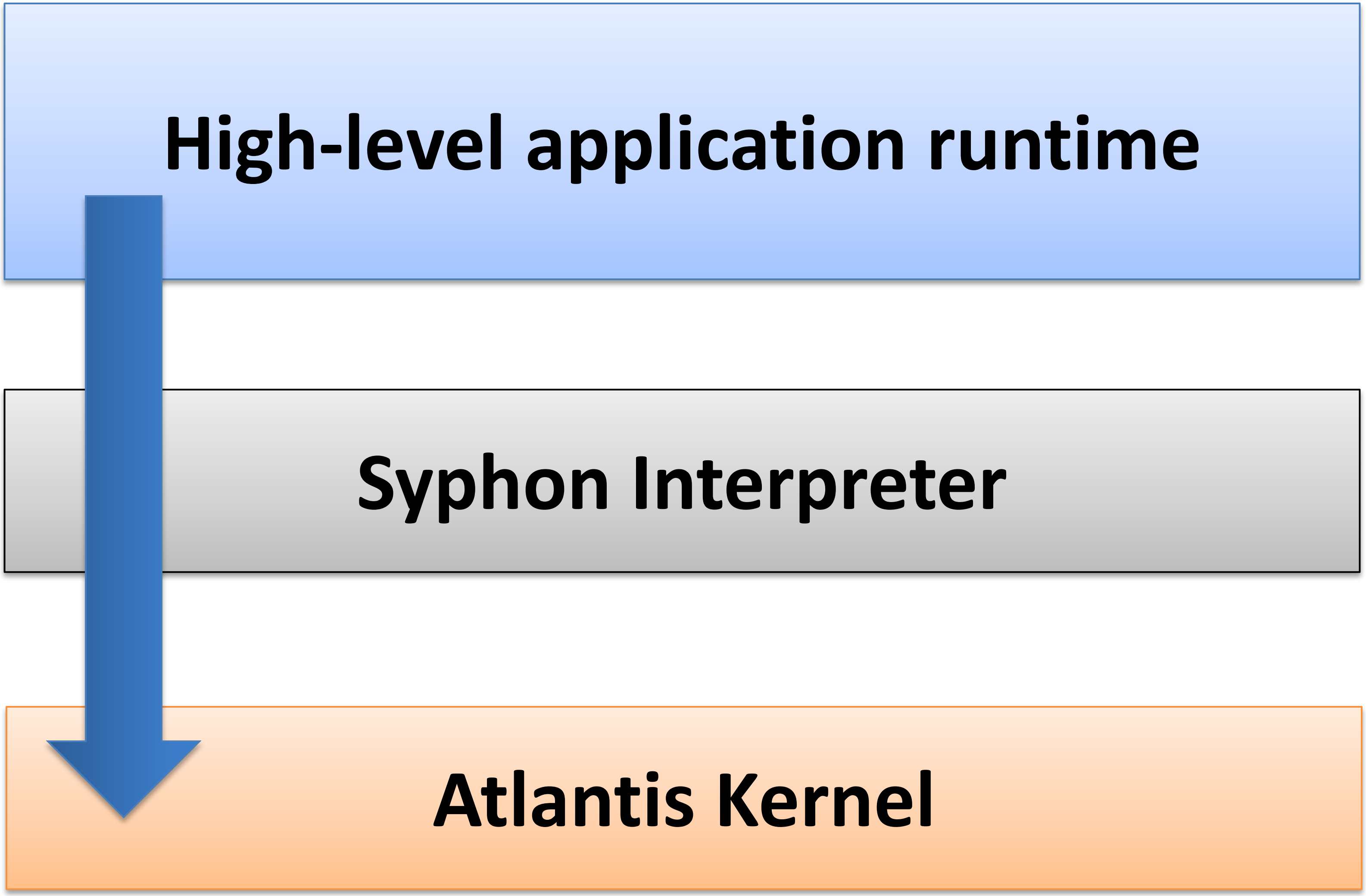
compiler.syp

mParser.syp

runtime.syp

Syphon Interpreter

Defining the Web stack

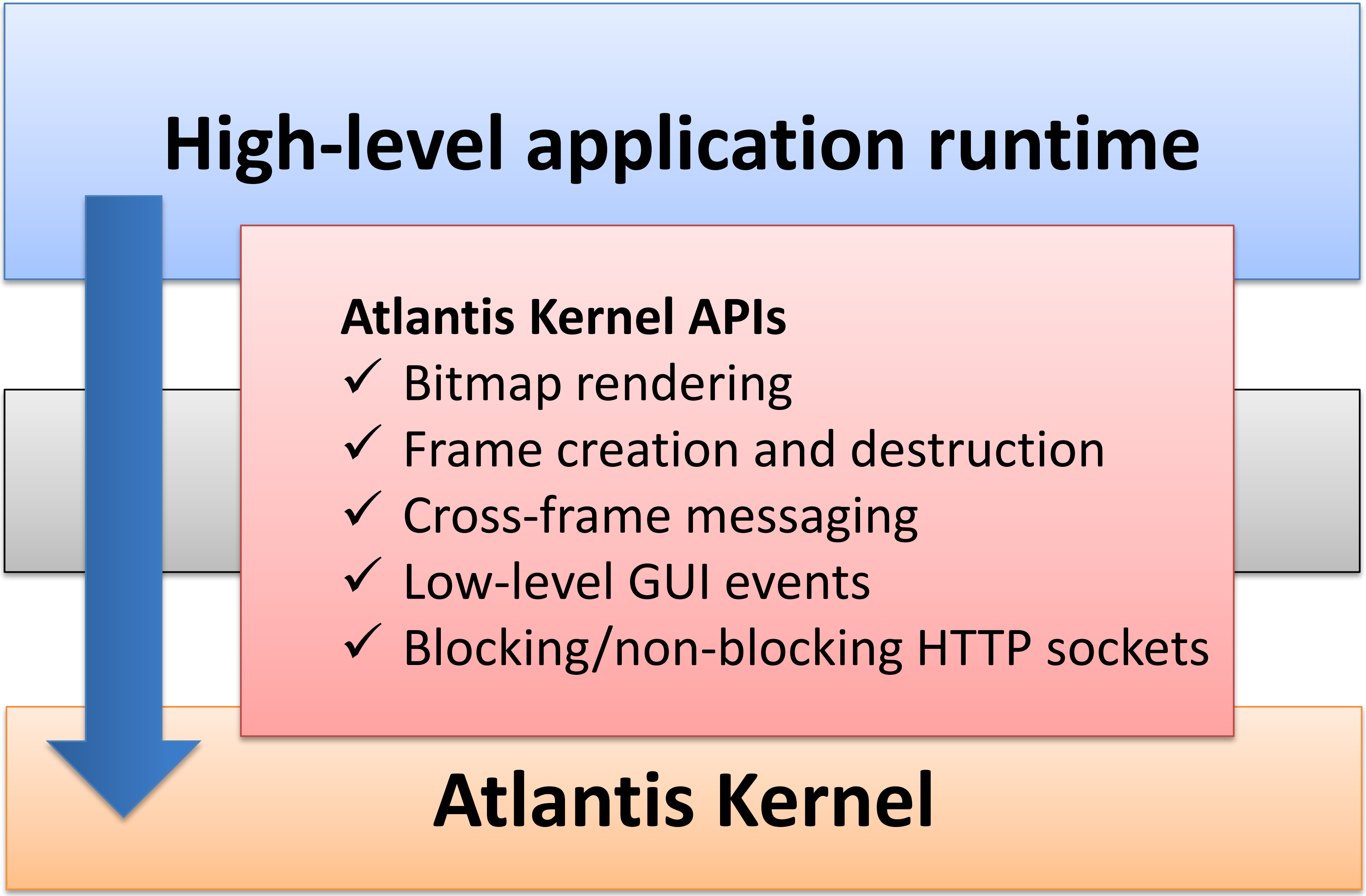


High-level application runtime

Syphon Interpreter

Atlantis Kernel

Defining the Web stack



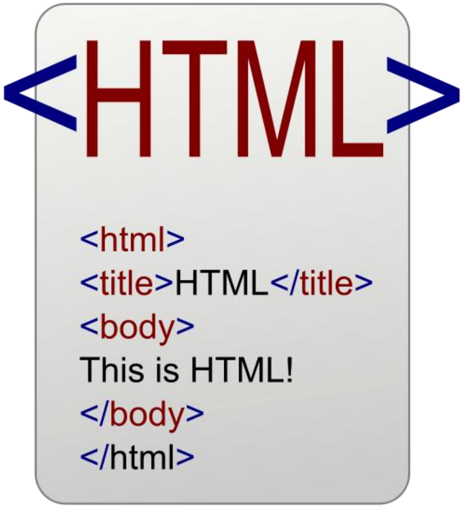
High-level application runtime

Atlantis Kernel APIs

✓ Bitmap rendering
✓ Frame creation and destruction
✓ Cross-frame messaging
✓ Low-level GUI events
✓ Blocking/non-blocking HTTP sockets

Atlantis Kernel

Default Web stack

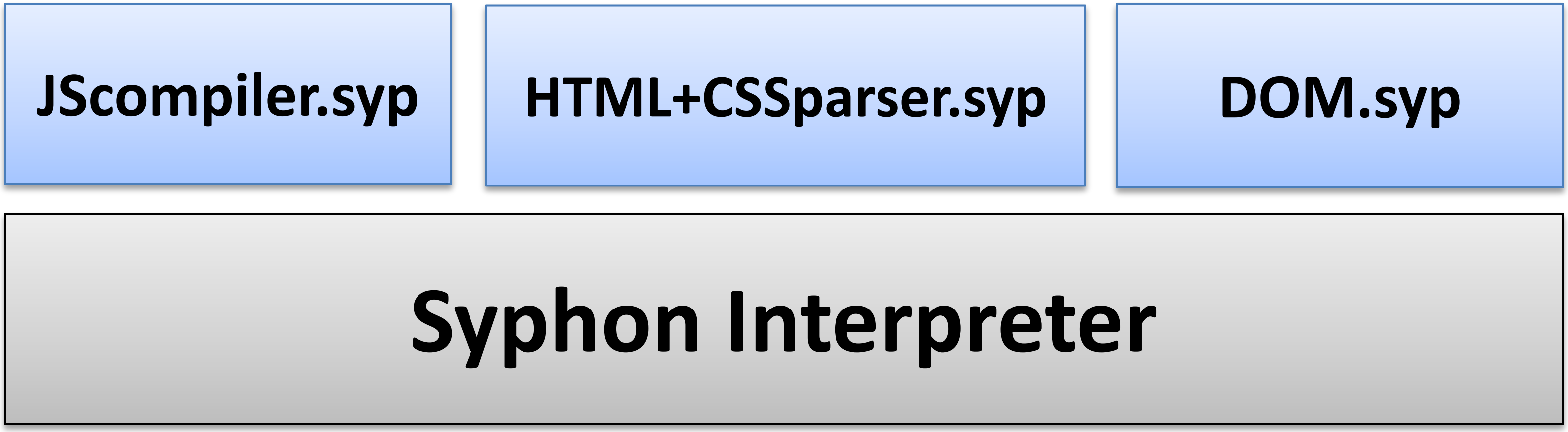


```
<html>
<title>HTML</title>
<body>
This is HTML!
</body>
</html>
```

No <environment> tag present

Default Web stack

```
<html>
<title>HTML</title>
<body>
This is HTML!
</body>
</html>
```



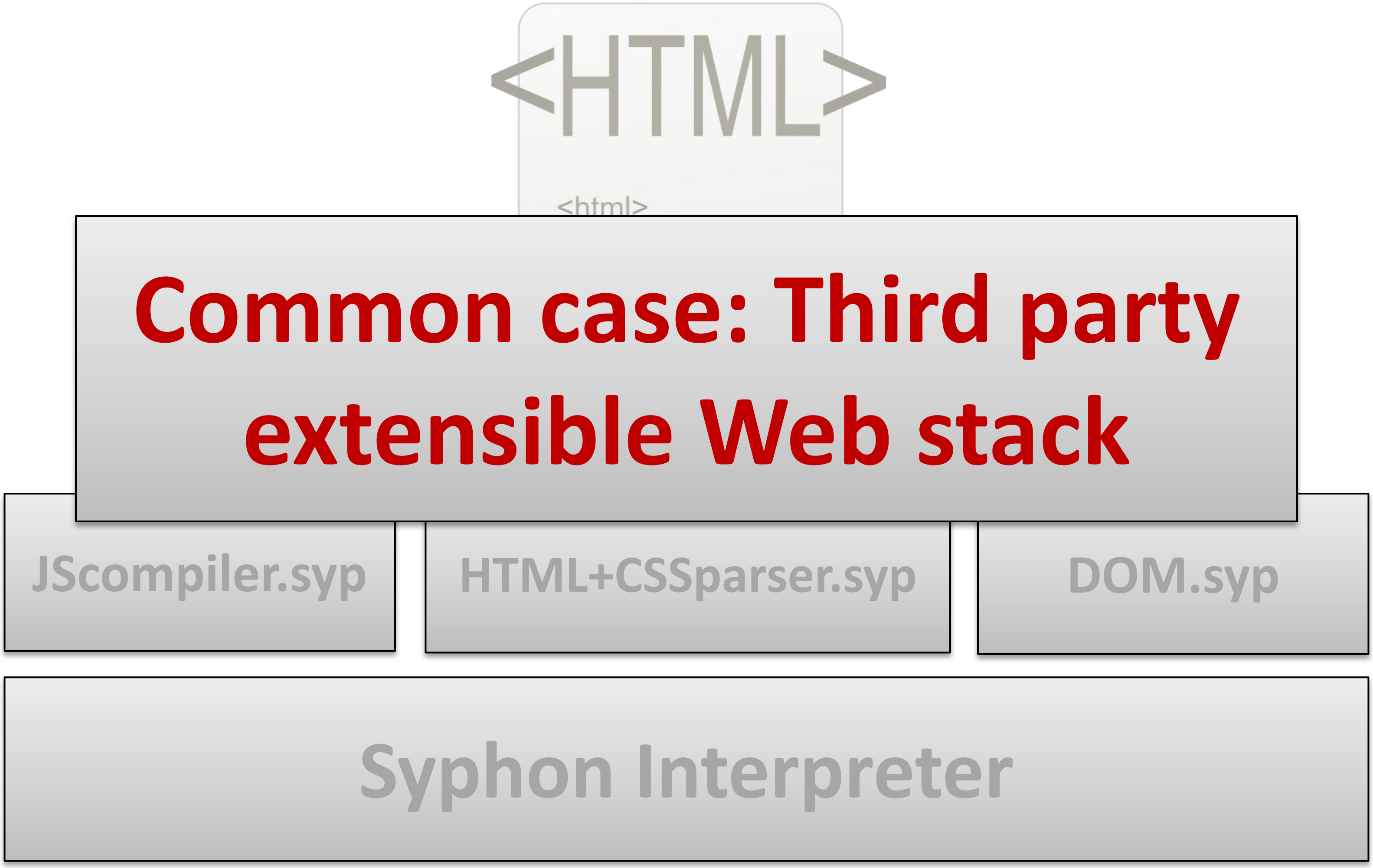
JScompiler.syp

HTML+CSSparser.syp

DOM.syp

Syphon Interpreter

Default Web stack



Common case: Third party extensible Web stack

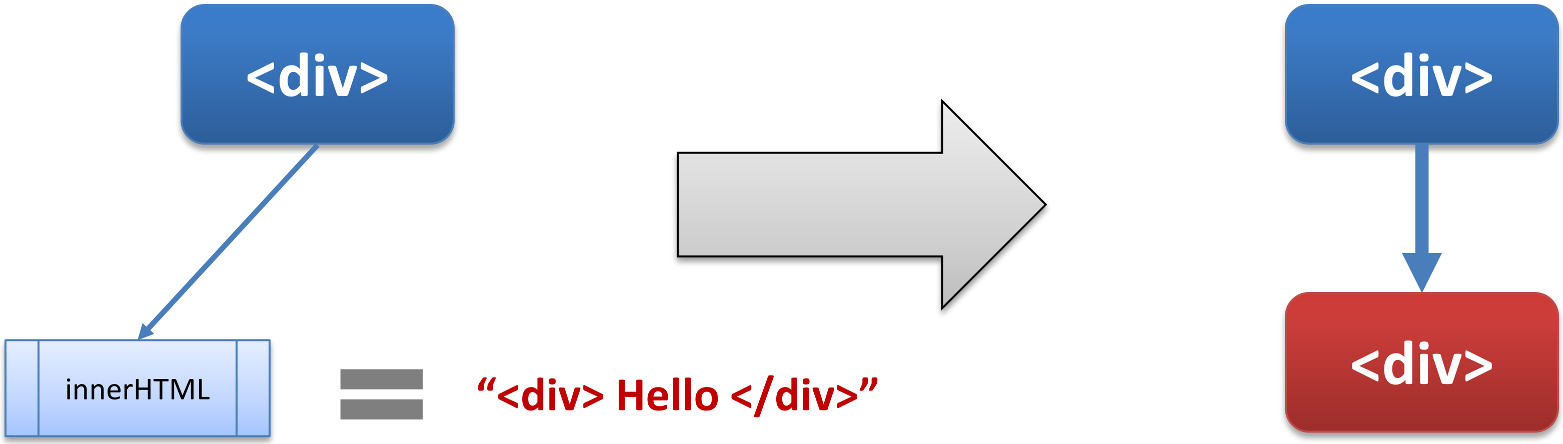
JScompiler.syp

HTML+CSSparser.syp

DOM.syp

Syphon Interpreter

Extensibility



<div>

innerHTML

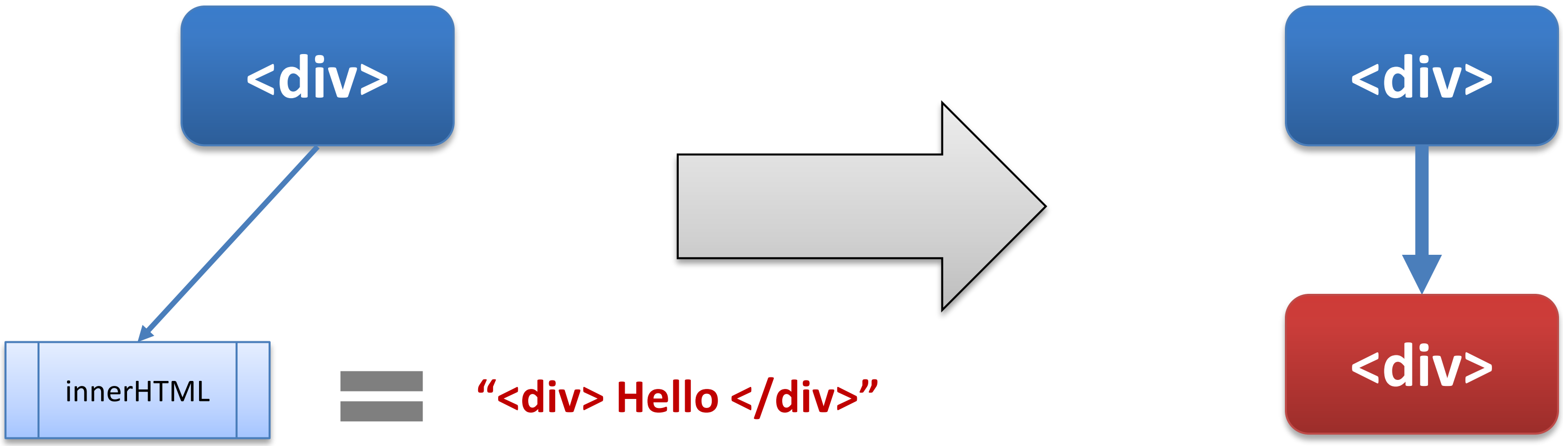
=

“<div> Hello </div>”

<div>

<div>

Extensibility



<div>

innerHTML

=

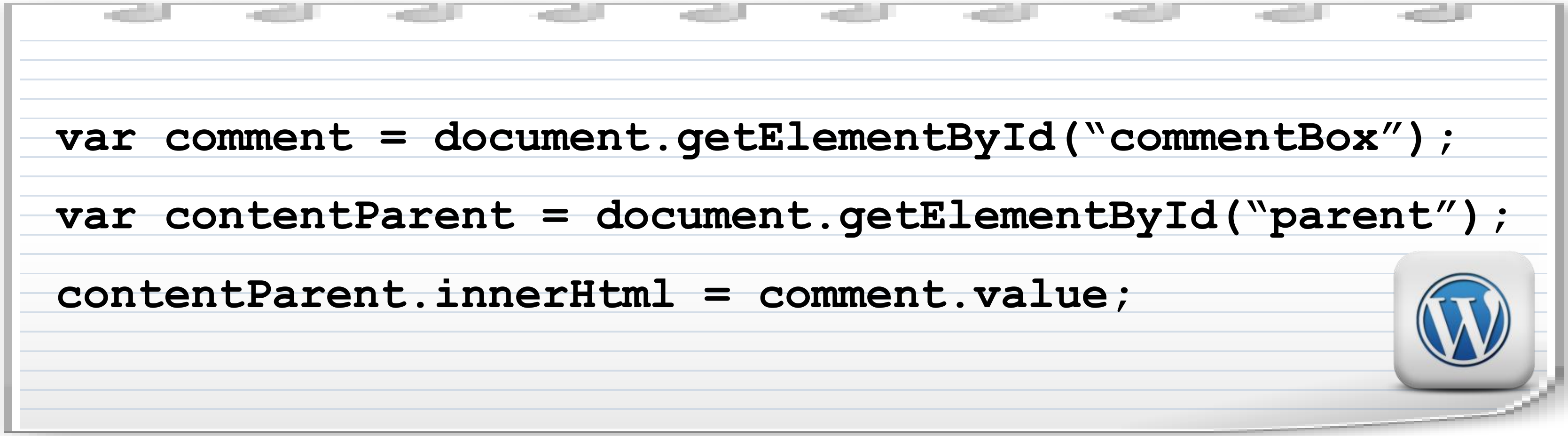
“<div> Hello </div>”

<div>

<div>

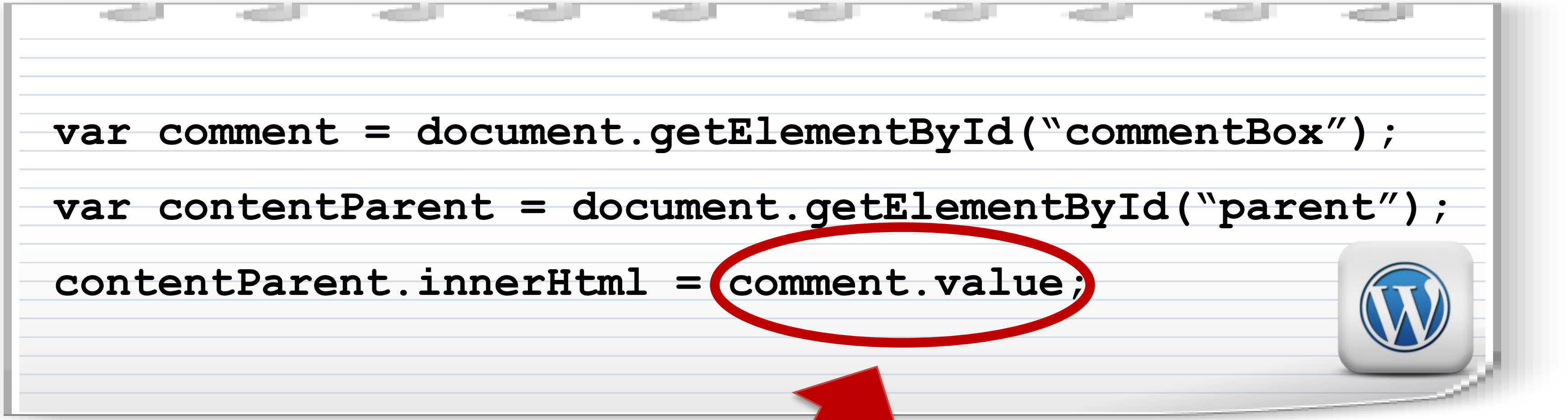
Enables JavaScript code injection attacks or XSS

Extensibility



```
var comment = document.getElementById(“commentBox”);
var contentParent = document.getElementById(“parent”);
contentParent.innerHtml = comment.value;
```

Extensibility



```
var comment = document.getElementById(“commentBox”);
var contentParent = document.getElementById(“parent”);
contentParent.innerHtml = comment.value;
```

What if this is
malicious JavaScript ?

Extensibility

```
var comment = document.getElementById("commentBox");
```

Ability to shim `innerHTML` and automatically install a sanitizer

What if this is malicious JavaScript ?

Extensibility

```
var comment = document.getElementById("commentBox");
```

Ability to shim `innerHTML` and automatically install a sanitizer

What if this is malicious JavaScript ?

DENIED

Extensibility

Developers own the DOM in Atlantis

<html>

<head>

<body>

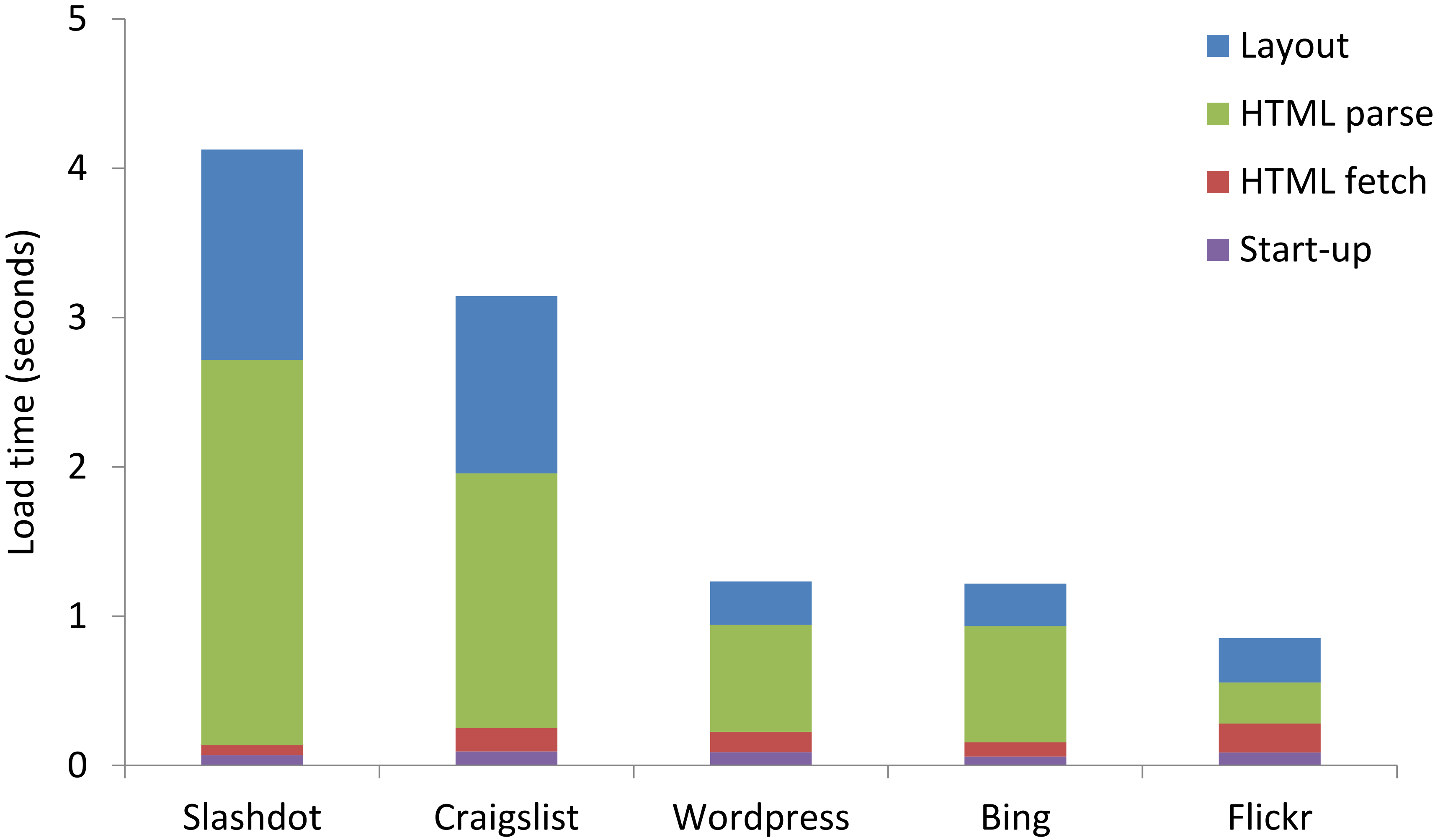
<title>

<div>

<div>

GLASBERGEN

Web page load time



Summary: Part II

- **The Web protocol is complex and huge**
  - No individual browser gets it all right
- JavaScript frameworks, microkernel browsers
  - Useful but cannot hide all browser quirks or introspect black-box components
- **Atlantis is an exokernel browser**
  - Kernel handles low-level networking, GUI events, bitmap rendering
  - Application defines higher-level abstractions
  - Strong security and powerful extensibility

Conclusion and Future directions

Conclusion

- Modern browsers provide limited extensibility with much less security **[ACSAC’09**, **ECOOP’12a]**
- Extensibility is important for developing novel browser-based user applications **[IMC’12]**
- **Transcript [PLAS’10**, **ECOOP’12b]** and **Atlantis [SOSP’11]** reason about browser extensibility from ***languages*** and ***systems*** perspectives to provide novel solutions

Future directions

- **Next-generation Web browser**
  - Abstractions for building novel user applications
  - Mobile, Internet-enabled AR/HUD and consumer devices
- **Security & Privacy**
  - Content-based security for web applications
  - Impact of new HTML5 and legacy browser APIs on end-user privacy

Acknowledgements

- **Dissertation advisors**
  - Vinod Ganapathy and Liviu Iftode
- **PhD committee members**
  - Uli Kremer and Kapil Singh
- **External collaborators**
  - Chung-chieh Shan (Indiana University)
  - Vern Paxson (UC Berkeley / ICSI Berkeley)
  - Renata Cruz Teixeira (LIP6 Paris)
  - Christian Kreibich, Mark Allman, Nicholas Weaver (ICSI Berkeley)
  - James Mickens (Microsoft Research Redmond)
  - Úlfar Erlingsson (Google)
- **Discolab members**
  - Aniruddha Bohra, Arati Baliga, Steve Smaldone, Pravin Shankar, Lu Han, Shakeel Butt, Rezwana Karim, Amruta Gokhale, Liu Yang, Nader Boushehrinejadmoradi, and several other past and present members

Thank you.

Contact information

http://paul.rutgers.edu/~mdhawan/

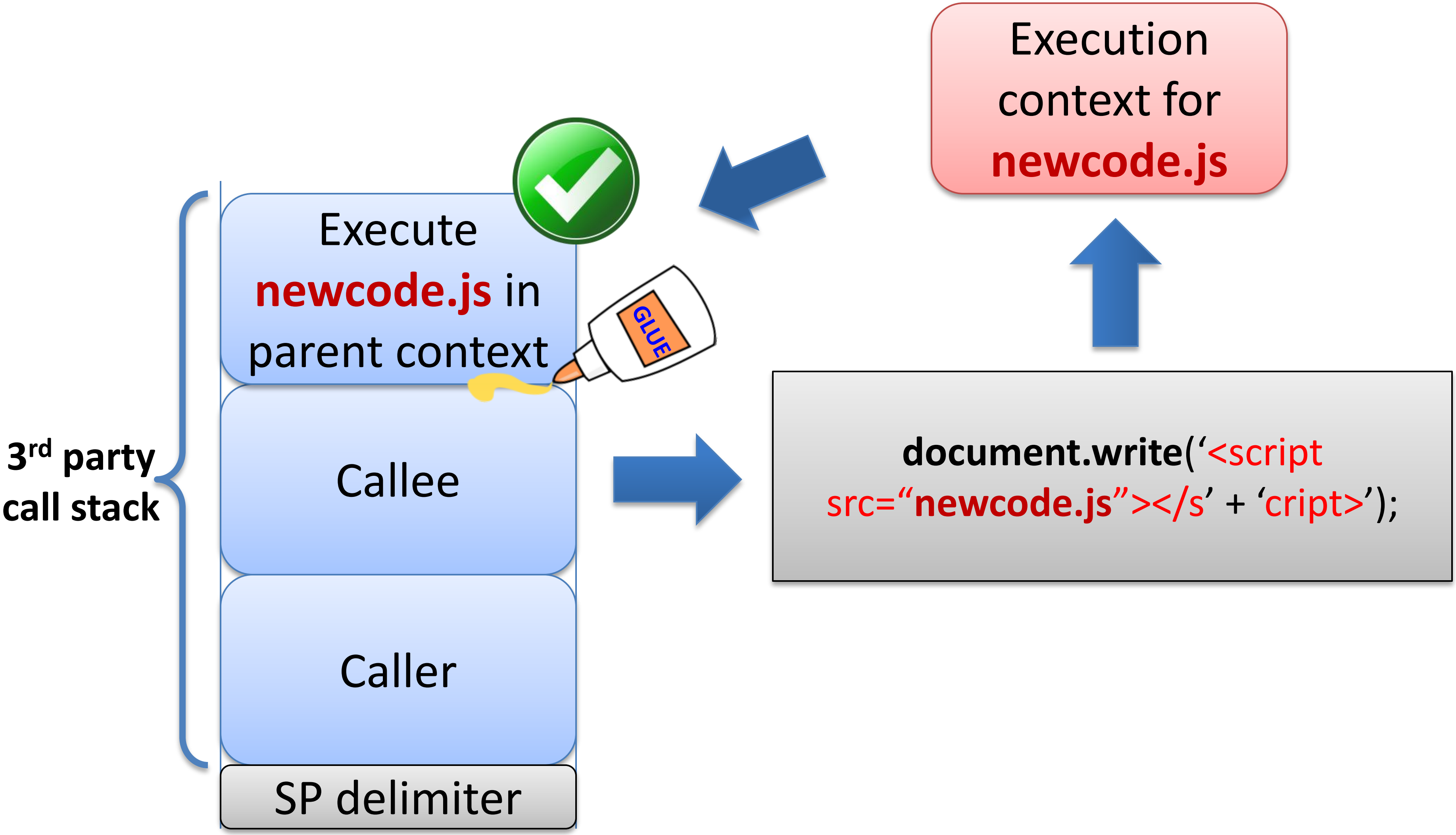
mdhawan@cs.rutgers.edu

Backup slides

Defense against UI redressing attack

```
var commitSp = true;
var sp = speculate {
                    …
    document.body.appendChild(overlay);
};
                    iBlock
do{
    var obj = sp.getObject(),  arg = sp.getArgs();
    switch(sp.getCause()) {
        case “appendChild“:
        if (uiRedressing(arg[0]))   commitSp = false;
        else   obj.appendChild(arg[0]);
        break;
    }; /* end switch */
    sp = sp.resume();
}while(sp.isSuspended());
If (commitSp)   sp.commit();
```

Dynamic script loading



Execution context for **newcode.js**

Execute **newcode.js** in parent context

Callee

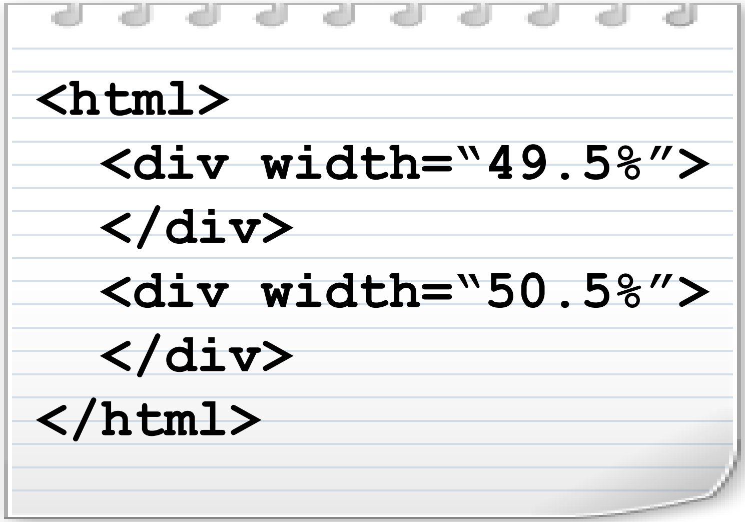
Caller

SP delimiter

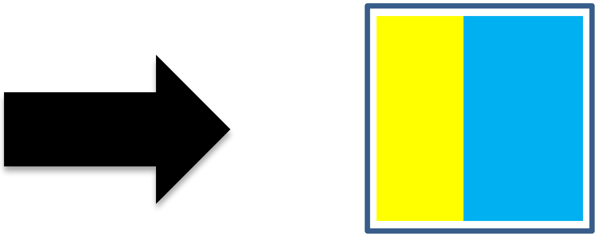
3rd party call stack

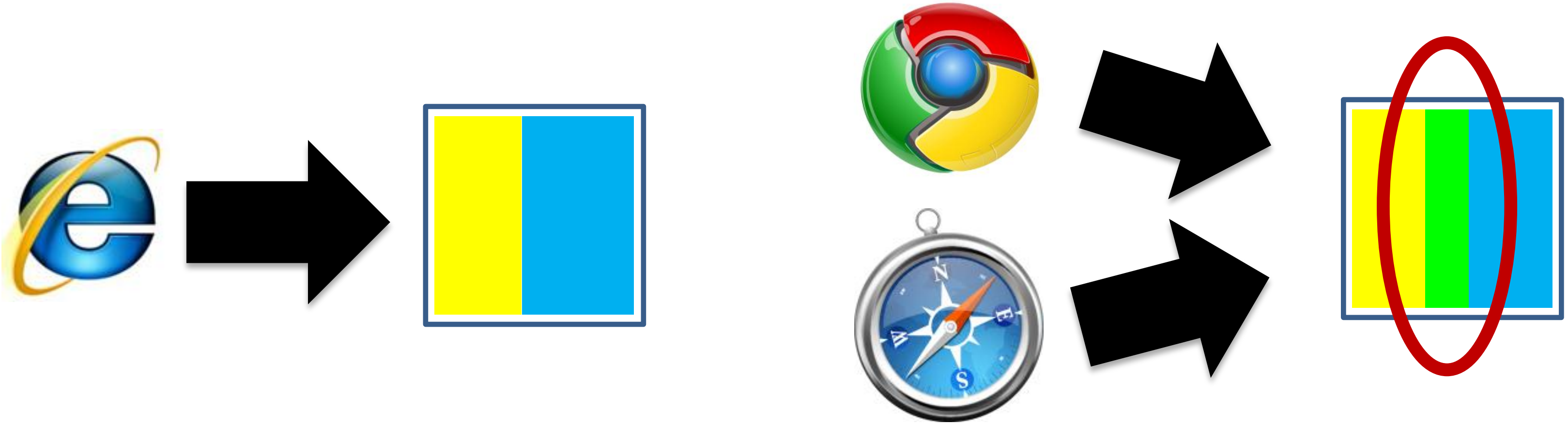
document.write(‘<script src=“**newcode.js**”></s’ + ‘cript>’);

Example: Layout and rendering

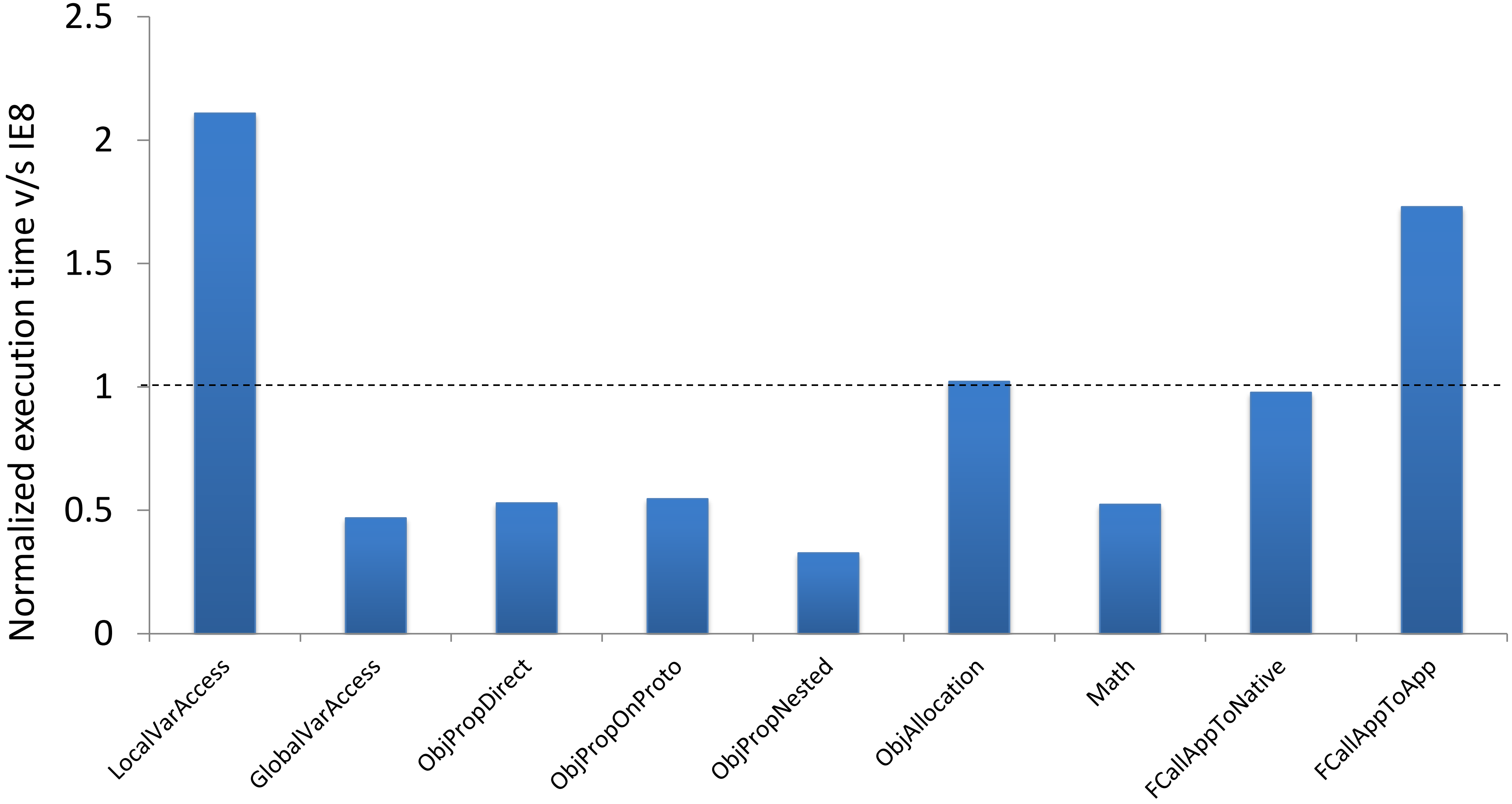


```
<html>
   <div width="49.5%">
   </div>
   <div width="50.5%">
   </div>
</html>
```





Microbenchmarks


Normalized execution time v/s IE8
LocalVarAccess
GlobalVarAccess
ObjPropDirect
ObjPropOnProto
ObjPropNested
ObjAllocation
Math
FCallAppToNative
FCallAppToApp