Stander Symposium, University of Dayton
April 22, 2020

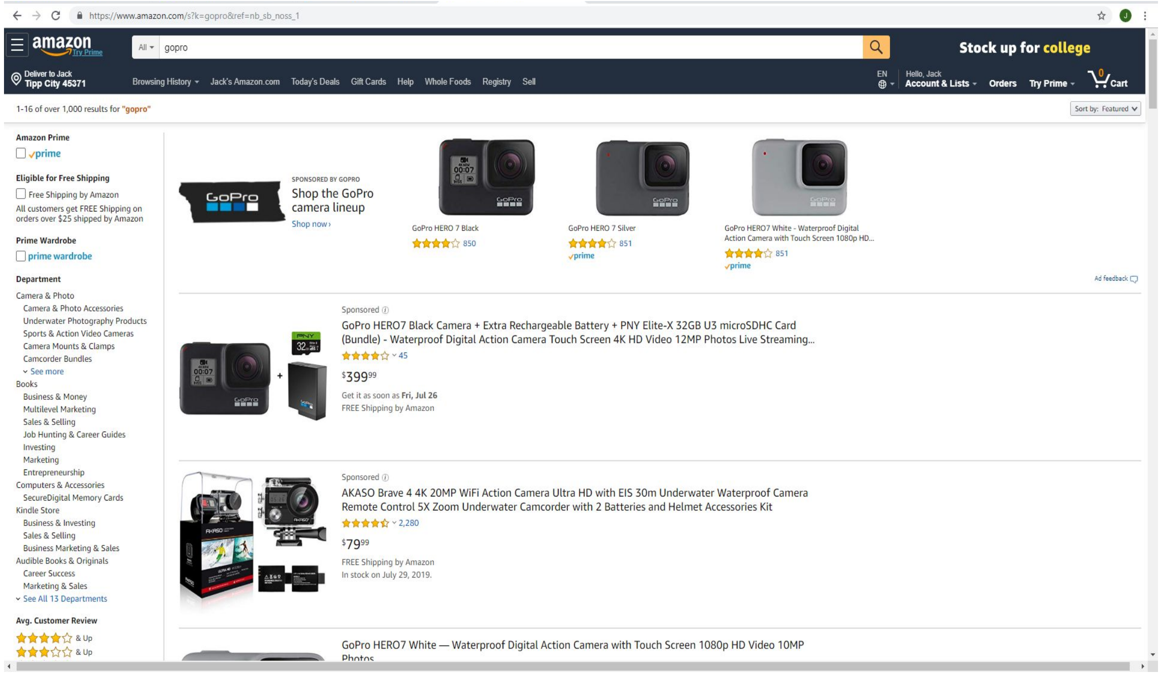
MyWebGuard: Toward a User-Oriented Tool for Security and Privacy Protection on the Web

Panchakshari N. Hiremath*, Jack Armentrout*, Son Vu, Tu N. Nguyen, Quang Tran Minh, and Phu H. Phung*

* Intelligent System Security Lab
Department of Computer Science, University of Dayton
https://isseclab-udayton.github.io/

The paper is published in the 6th International Conference on Future Data and Security Engineering 2019 (FDSE'2019), Nha Trang City, Vietnam, November 27-29, 2019
Link: https://bit.ly/2VsEAhM

Privacy on the web- Tracker Example



https://www.amazon.com/s?k=gopro&ref=nb_sb_noss_1

amazon Try Prime

All gopro

Stock up for college

Deliver to Jack
Tipp City 45371

Browsing History Jack's Amazon.com Today's Deals Gift Cards Help Whole Foods Registry Sell

EN Hello, Jack Account & Lists Orders Try Prime 0 Cart

1-16 of over 1,000 results for "gopro"

Sort by: Featured

Amazon Prime

□ prime

Eligible for Free Shipping

□ Free Shipping by Amazon

All customers get FREE Shipping on orders over $25 shipped by Amazon

Prime Wardrobe

□ prime wardrobe

Department

Camera & Photo
- Camera & Photo Accessories
- Underwater Photography Products
- Sports & Action Video Cameras
- Camera Mounts & Clamps
- Camcorder Bundles
- See more

Books
- Business & Money
- Multilevel Marketing
- Sales & Selling
- Job Hunting & Career Guides
- Investing
- Marketing
- Entrepreneurship

Computers & Accessories
- SecureDigital Memory Cards

Kindle Store
- Business & Investing
- Sales & Selling
- Business Marketing & Sales

Audible Books & Originals
- Career Success
- Marketing & Sales

See All 13 Departments

Avg. Customer Review

★★★★☆ & Up

★★★☆☆ & Up

SPONSORED BY GOPRO

Shop the GoPro camera lineup

Shop now ›

GoPro HERO 7 Black ★★★★☆ 850

GoPro HERO 7 Silver ★★★★☆ 851 prime

GoPro HERO7 White - Waterproof Digital Action Camera with Touch Screen 1080p HD... ★★★★☆ 851 prime

Ad feedback

Sponsored

GoPro HERO7 Black Camera + Extra Rechargeable Battery + PNY Elite-X 32GB U3 microSDHC Card (Bundle) - Waterproof Digital Action Camera Touch Screen 4K HD Video 12MP Photos Live Streaming...

★★★★☆ 45

$399.99

Get it as soon as Fri, Jul 26

FREE Shipping by Amazon

Sponsored

AKASO Brave 4 4K 20MP WiFi Action Camera Ultra HD with EIS 30m Underwater Waterproof Camera Remote Control 5X Zoom Underwater Camcorder with 2 Batteries and Helmet Accessories Kit

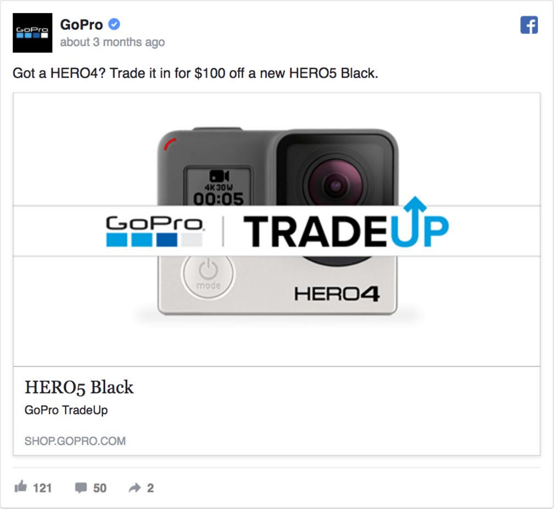
★★★★☆ 2,280

$79.99

FREE Shipping by Amazon

In stock on July 29, 2019.

GoPro HERO7 White — Waterproof Digital Action Camera with Touch Screen 1080p HD Video 10MP Photos



GoPro
about 3 months ago

Got a HERO4? Trade it in for $100 off a new HERO5 Black.

HERO5 Black

GoPro TradeUp

SHOP.GOPRO.COM

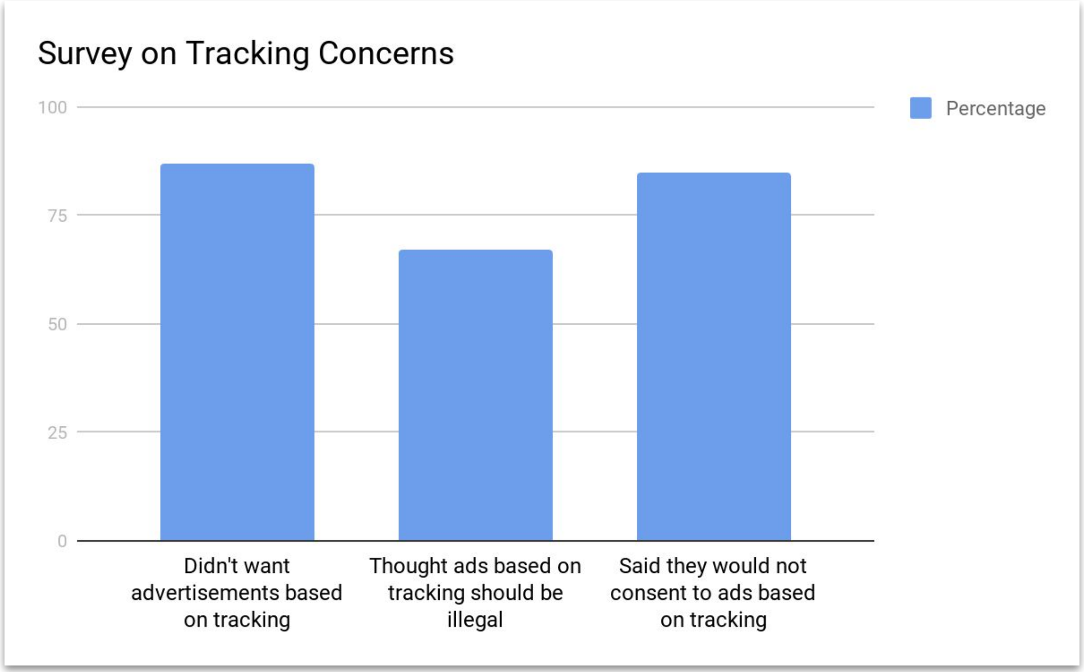
121 50 2

User Concerns

- Amount of malicious content on web?
  - Around 18.5 million websites are compromised at a given time each week
  - Average website attacked 44 times a day
- What are the options for a user?
  - Do Not Track- Websites do not have to honour
  - Blocker Extensions
  - Brave Browser

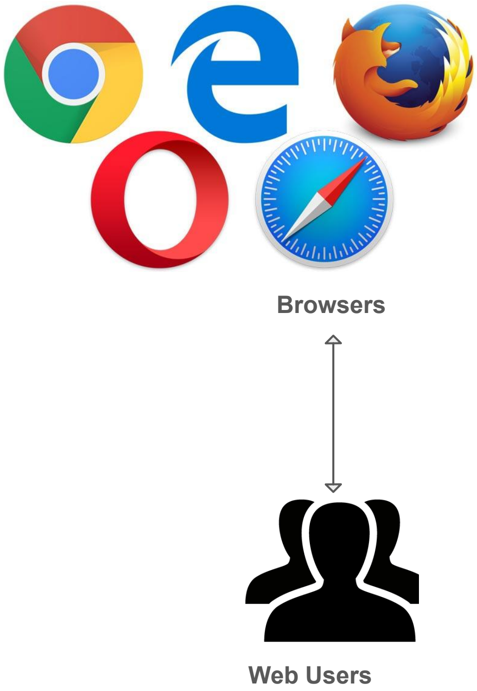
https://www.securityweek.com/185-million-websites-infected-malware-any-time

User Tracking Concerns



Mayer, J.R., Mitchell, J.C.: Third-party web tracking: Policy and technology. In: 2012 IEEE Symposium on Security and Privacy. pp. 413–427. IEEE (2012)

Existing solutions

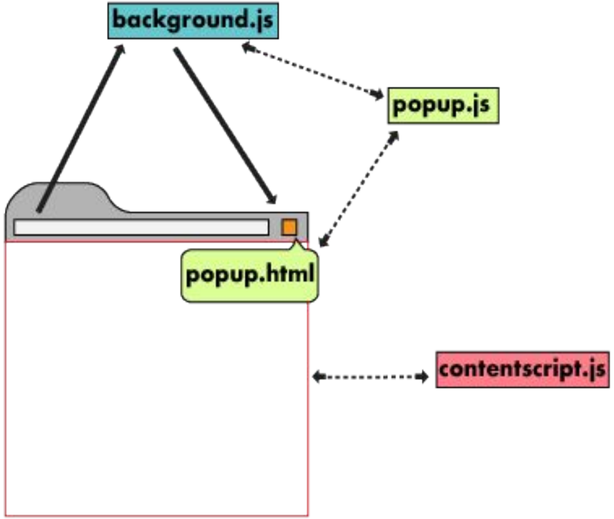


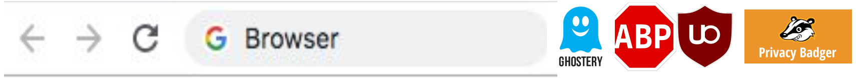
- There are more than 80 browsers in the industry, including popular ones such as Google Chrome, Apple Safari, Mozilla Firefox.
- Some of these are more committed to privacy than others such as Brave who disable third-party cookies to ensure user privacy, which in turn can limit usability.

Is user safe from only browser?

Browser Extensions

- A browser extension is a small software module for customizing a web browser.
- Extensions are small software programs that customize the browsing experience. They enable users to tailor Chrome functionality and behavior to individual needs or preferences.
- They are built on web technologies such as HTML, JavaScript, and CSS.



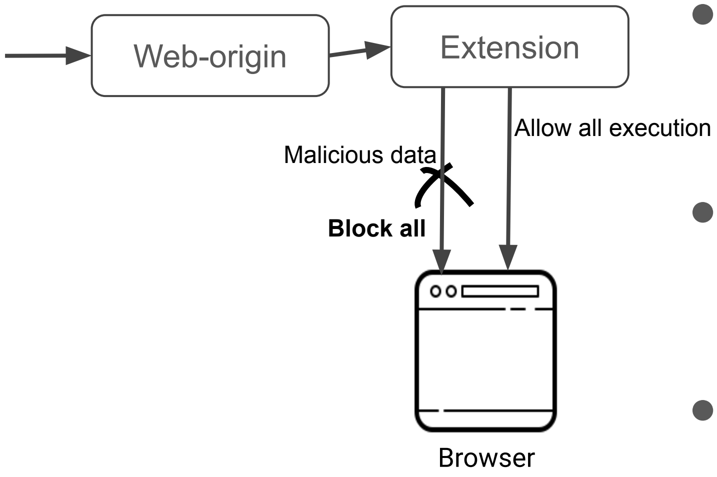


Is user safe from browser and extensions?

Web Users

- There are many browser extensions for privacy and top extensions are, Ghostery, Ublock, Simple Blocker, and AdBlock.
- Still, can attackers gain access to user data?

Limitations of existing solutions



Block all or do nothing.

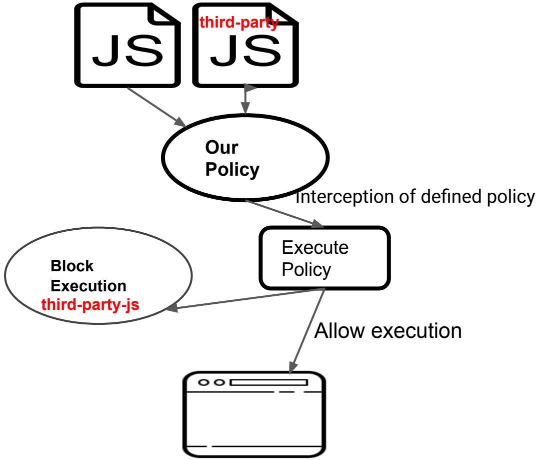
- Existing browser extensions only enforce block on all the attacks or allow there is no categorization.
- Extensions are predefined, so there are new trackers or other third-party content they are not blocked by these extensions.
- Popular security extensions like Ghostery and uBlock do not detect data leakage from sources and sinks.

Motivation

- Preserve user privacy on the web
  - Third-party trackers
  - Malicious injected webpage content
- Allow for an ethical middle ground for the collection of user data with the consent of the user
- User-centric
  - User defined control for third-party privacy accessibility
  - Allow user in real time to make privacy relevant decisions

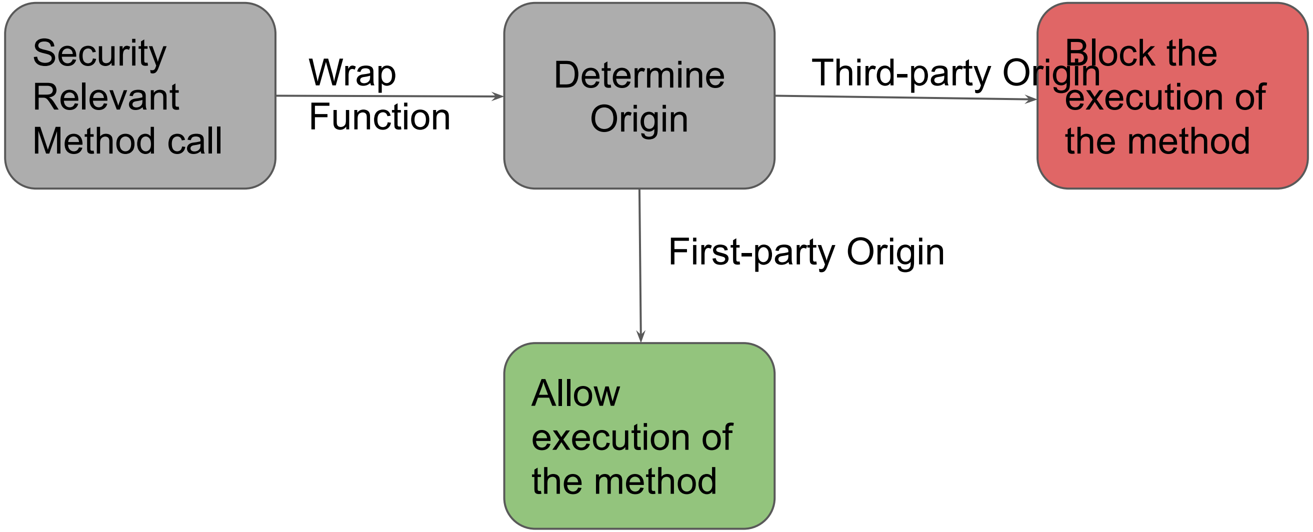
Our Approach

- Monitor JavaScript sources and sinks, distinguishing origin of code
  - Sources and Sinks: Where any JS API can execute
  - Utilize runtime stack to distinguish between first/third-party code
- Enforce policies on these channels to protect against privacy violations, based on code origin



How do we enforce a policy?

- When a monitored JavaScript API is called
  - Determine origin of code using runtime stack
  - Screen through relevant policy
  - Allow API to proceed or block the call in the case of a violation
    - Consult the user in the case of a privacy violation to allow for an override if requested


Security Relevant Method call
Wrap Function
Determine Origin
Third-party Origin
Block the execution of the method
First-party Origin
Allow execution of the method

Policy Example: Read Cookie

If the determined origin is not allowed to read the cookie, then we block the request

```
Object.defineProperty(document, "cookie",
{get: function(){ //JavaScript attempts to read the cookie
 //Determine the origin of the code
      //if origin is allowed
           //return the original value
     //else
           //block the request

  },
  //...
});
```

Policy Example: Image Policies

Img sources are wrapped and passed through policies to protect against malicious content in img sources

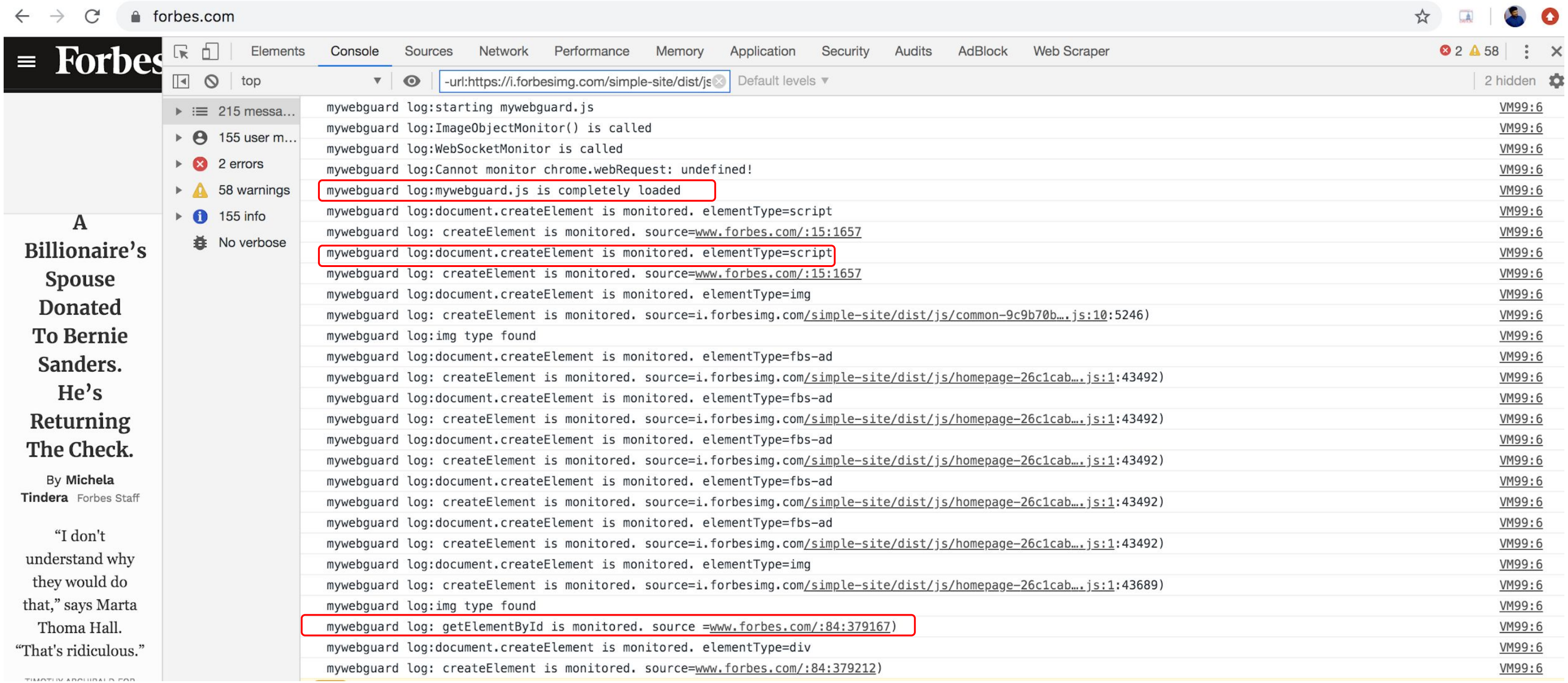
```
var imgPolicy = {
    get: function(obj, prop) {/* policies for get */},
    set: function(obj, prop, value) {/* policies for set */}
};

//save the original image

class ImageWrapper {
    constructor(height, width) {
        //create image object from original image
        //pass image object through relevant policy
        //return sanitized image
    }
}

//replace the requested image with sanitized image
```

Interception of operation



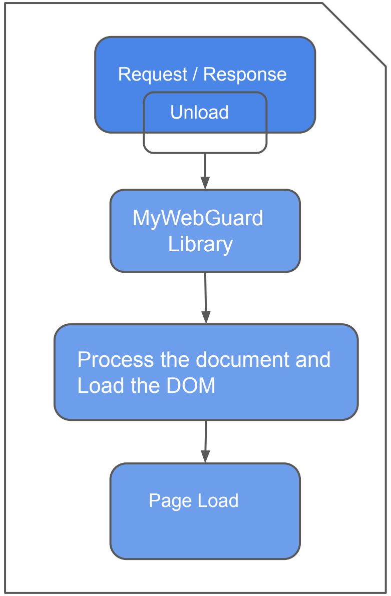
A Billionaire's Spouse Donated To Bernie Sanders. He's Returning The Check.

By Michela Tindera Forbes Staff

"I don't understand why they would do that," says Marta Thoma Hall. "That's ridiculous."

```
mywebguard log:starting mywebguard.js                                                          VM99:6
mywebguard log:ImageObjectMonitor() is called                                                  VM99:6
mywebguard log:WebSocketMonitor is called                                                      VM99:6
mywebguard log:Cannot monitor chrome.webRequest: undefined!                                    VM99:6
mywebguard log:mywebguard.js is completely loaded                                              VM99:6
mywebguard log:document.createElement is monitored. elementType=script                         VM99:6
mywebguard log: createElement is monitored. source=www.forbes.com/:15:1657                     VM99:6
mywebguard log:document.createElement is monitored. elementType=script                         VM99:6
mywebguard log: createElement is monitored. source=www.forbes.com/:15:1657                     VM99:6
mywebguard log:document.createElement is monitored. elementType=img                            VM99:6
mywebguard log: createElement is monitored. source=i.forbesimg.com/simple-site/dist/js/common-9c9b70b….js:10:5246)   VM99:6
mywebguard log:img type found                                                                  VM99:6
mywebguard log:document.createElement is monitored. elementType=fbs-ad                         VM99:6
mywebguard log: createElement is monitored. source=i.forbesimg.com/simple-site/dist/js/homepage-26c1cab….js:1:43492) VM99:6
mywebguard log:document.createElement is monitored. elementType=fbs-ad                         VM99:6
mywebguard log: createElement is monitored. source=i.forbesimg.com/simple-site/dist/js/homepage-26c1cab….js:1:43492) VM99:6
mywebguard log:document.createElement is monitored. elementType=fbs-ad                         VM99:6
mywebguard log: createElement is monitored. source=i.forbesimg.com/simple-site/dist/js/homepage-26c1cab….js:1:43492) VM99:6
mywebguard log:document.createElement is monitored. elementType=fbs-ad                         VM99:6
mywebguard log: createElement is monitored. source=i.forbesimg.com/simple-site/dist/js/homepage-26c1cab….js:1:43492) VM99:6
mywebguard log:document.createElement is monitored. elementType=fbs-ad                         VM99:6
mywebguard log: createElement is monitored. source=i.forbesimg.com/simple-site/dist/js/homepage-26c1cab….js:1:43492) VM99:6
mywebguard log:document.createElement is monitored. elementType=img                            VM99:6
mywebguard log: createElement is monitored. source=i.forbesimg.com/simple-site/dist/js/homepage-26c1cab….js:1:43689) VM99:6
mywebguard log:img type found                                                                  VM99:6
mywebguard log: getElementById is monitored. source =www.forbes.com/:84:379167)                VM99:6
mywebguard log:document.createElement is monitored. elementType=div                            VM99:6
mywebguard log: createElement is monitored. source=www.forbes.com/:84:379212)                  VM99:6
```

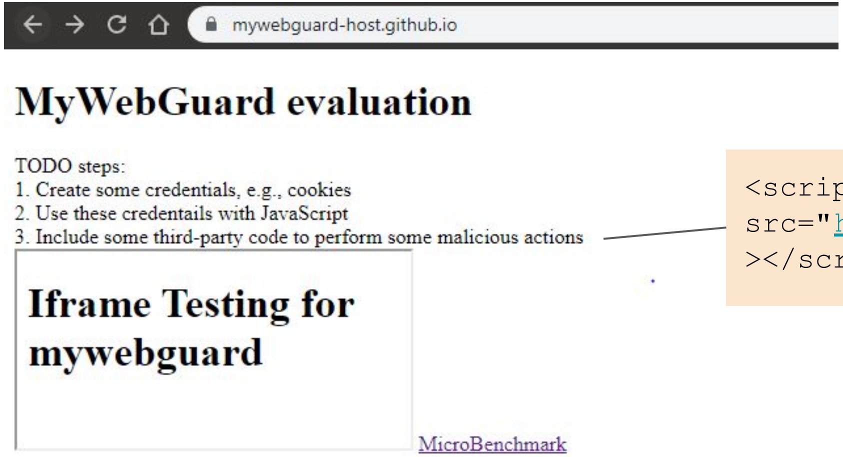
MyWebGuard Browser Extension Implementation



- We have developed a JavaScript library and deployed in the browser extension to self-protect the web users.
- Our interception library(CoreFlashJax) run first before a web page is loaded, we have implemented our JavaScript library code in innerHTML property so that when page loads it will be set as a first current page.
- We have implemented interception for data source access and data sink channels.

Evaluation Setup

- We set up on our host websites (first-party) with third-party JavaScript code implemented
  - We test our extension on the host website with simulated attacks from third party code



MyWebGuard evaluation

TODO steps:
1. Create some credentials, e.g., cookies
2. Use these credentails with JavaScript
3. Include some third-party code to perform some malicious actions

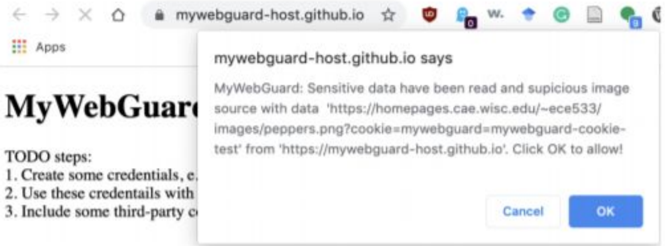
Iframe Testing for mywebguard

MicroBenchmark

```
<script
src="https://mywebguard-thirdparty.github.io/script.js "
></script>
```

Demonstration

We notice that data leakage and tracking requests are caught by MyWebGuard and users would be notified



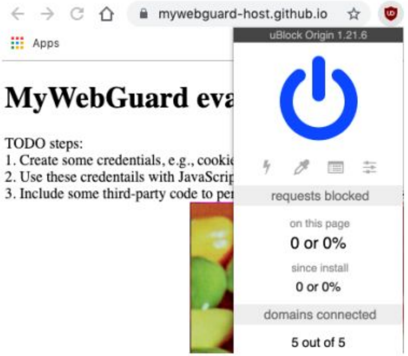
MyWebGuar

TODO steps:
1. Create some credentials, e.
2. Use these credentails with
3. Include some third-party c

mywebguard-host.github.io says

MyWebGuard: Sensitive data have been read and supicious image source with data 'https://homepages.cae.wisc.edu/~ece533/images/peppers.png?cookie=mywebguard=mywebguard-cookie-test' from 'https://mywebguard-host.github.io'. Click OK to allow!

However, the simulated data leakage and tracking requests were ignored by uBlock, one of the popular browser privacy extensions



MyWebGuard eva

TODO steps:
1. Create some credentials, e.g., cooki
2. Use these credentails with JavaScrip
3. Include some third-party code to pe

requests blocked

on this page

0 or 0%

since install

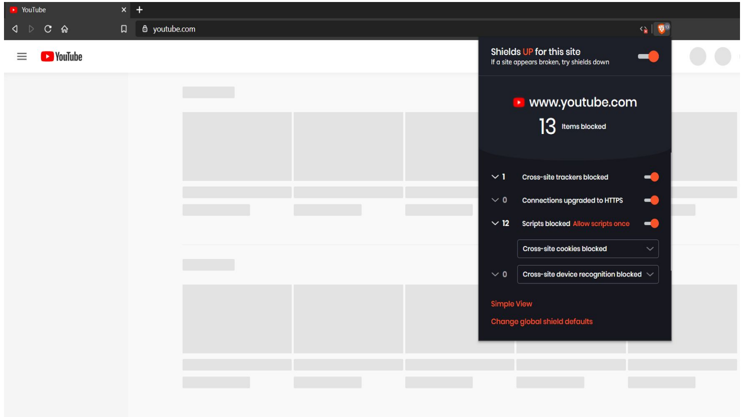
0 or 0%

domains connected

5 out of 5

Functionality

- When examining Brave browser, which has a JavaScript-blocking mechanism, we test some websites
- We notice several <u>breakages</u> and <u>loading issues</u> (such as YouTube)

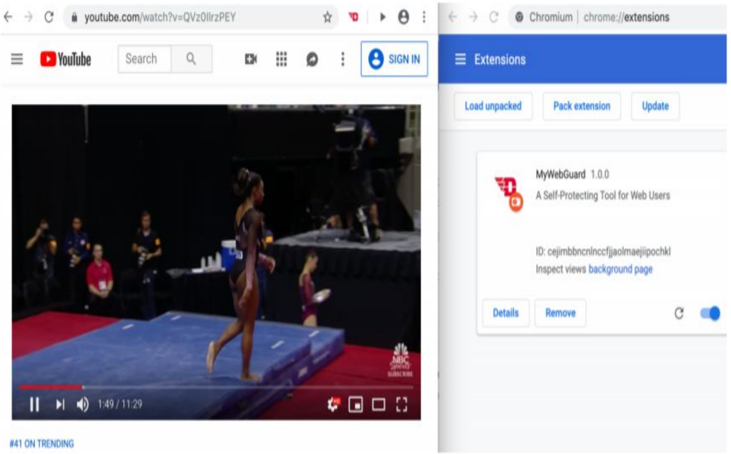


Shields UP for this site
If a site appears broken, try shields down

www.youtube.com
13 Items blocked

1 Cross-site trackers blocked
0 Connections upgraded to HTTPS
12 Scripts blocked Allow scripts once
Cross-site cookies blocked
0 Cross-site device recognition blocked

Simple View
Change global shield defaults



youtube.com/watch?v=QVz0llrzPEY

Chromium | chrome://extensions

Extensions

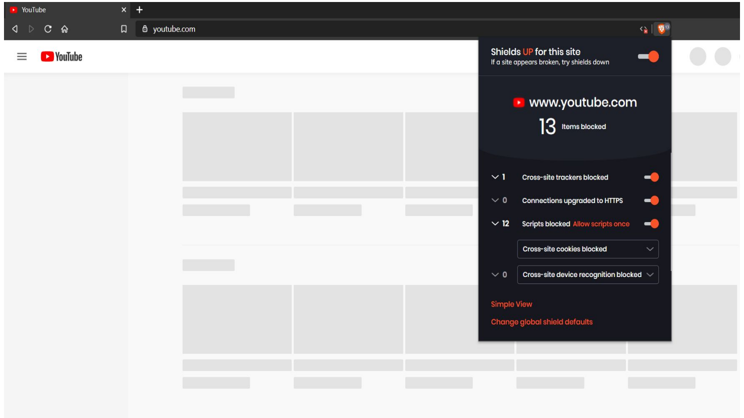
Load unpacked
Pack extension
Update

MyWebGuard 1.0.0
A Self-Protecting Tool for Web Users
ID: cejimbbncnlnccfjjaolmaejiipochkl
Inspect views background page

Details
Remove

Functionality

- We do not notice any issues when loading those websites (like YouTube) with MyWebGuard

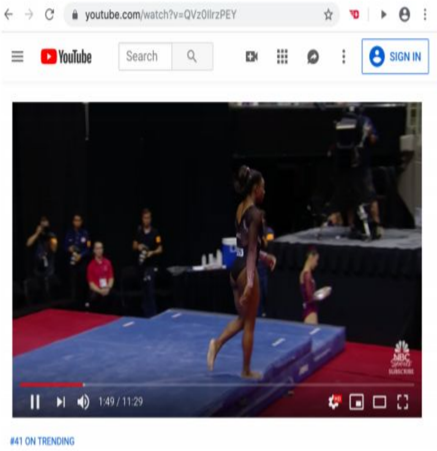


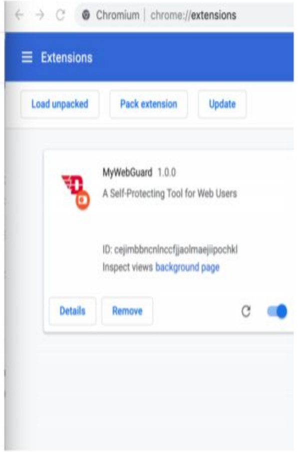
Shields UP for this site
If a site appears broken, try shields down

www.youtube.com
13 Items blocked

1 Cross-site trackers blocked
0 Connections upgraded to HTTPS
12 Scripts blocked Allow scripts once
Cross-site cookies blocked
0 Cross-site device recognition blocked

Simple View
Change global shield defaults





Chromium | chrome://extensions

Extensions

Load unpacked | Pack extension | Update

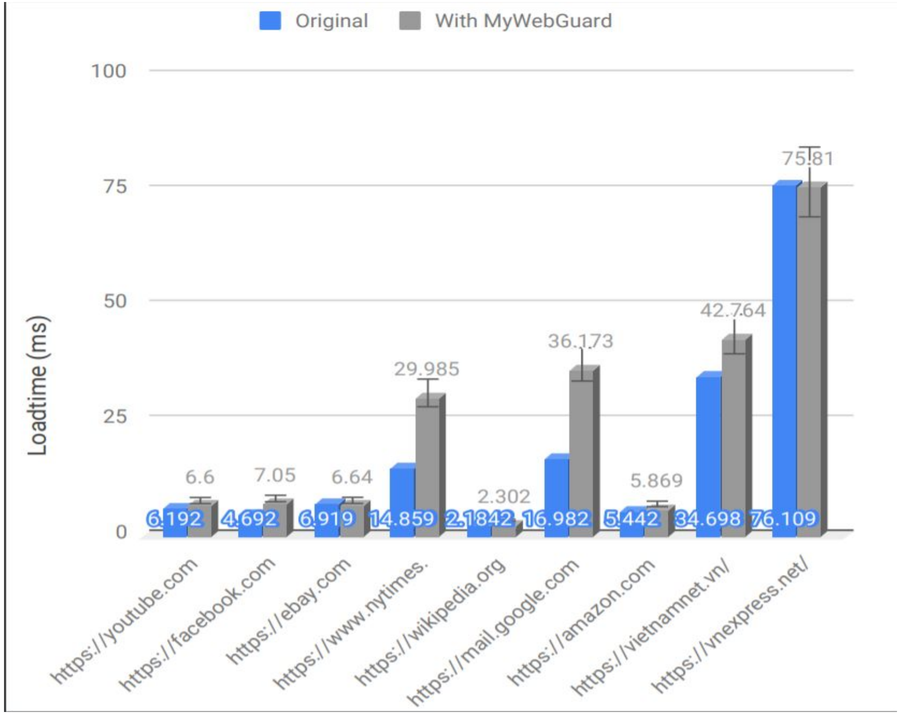
MyWebGuard 1.0.0
A Self-Protecting Tool for Web Users

ID: cejimbbncnlncfjjaolmaejiipochkl
Inspect views background page

Details | Remove

Runtime Evaluation

- We tested MyWebGuard with both Chromium and Brave browsers (on Ubuntu 18.04.2 LTS) on real websites
    - The overheads are not noticeable as shown in the graph



Contribution

- Browser-agnostic approach to preventing privacy leakage not monitored by contemporary solutions
- Present a compromise to “all-or-nothing” filter lists
- Advances conventional same-origin policy standard by enforcing different policies for each source of code
- Evaluation of approach overhead shows a lightweight yet effective implementation

Future Work

- Extend and refine policies and enforcement mechanism
  - Machine learning to produce practical policies
  - Effectiveness when built into a browser
- Allow for end-users to customize privacy preferences
- Perform large-scale evaluations of MyWebGuard
  - On top websites
  - Interference with co-existing browser extensions

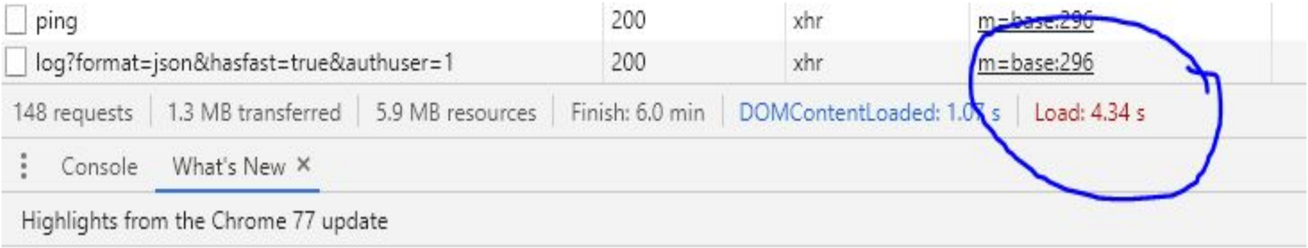
Thank You

Intelligent System Security Lab
Department of Computer Science, University of Dayton
https://isseclab-udayton.github.io/

Runtime Evaluation

We now test our extension on different sites (such as EBay, Amazon, FaceBook…)

To avoid anomalies, we test each site 10 times, recording the loading times (time for a site to finish loading its required contents



□ ping	200	xhr	m=base:296
□ log?format=json&hasfast=true&authuser=1	200	xhr	m=base:296

148 requests | 1.3 MB transferred | 5.9 MB resources | Finish: 6.0 min | DOMContentLoaded: 1.07 s | Load: 4.34 s

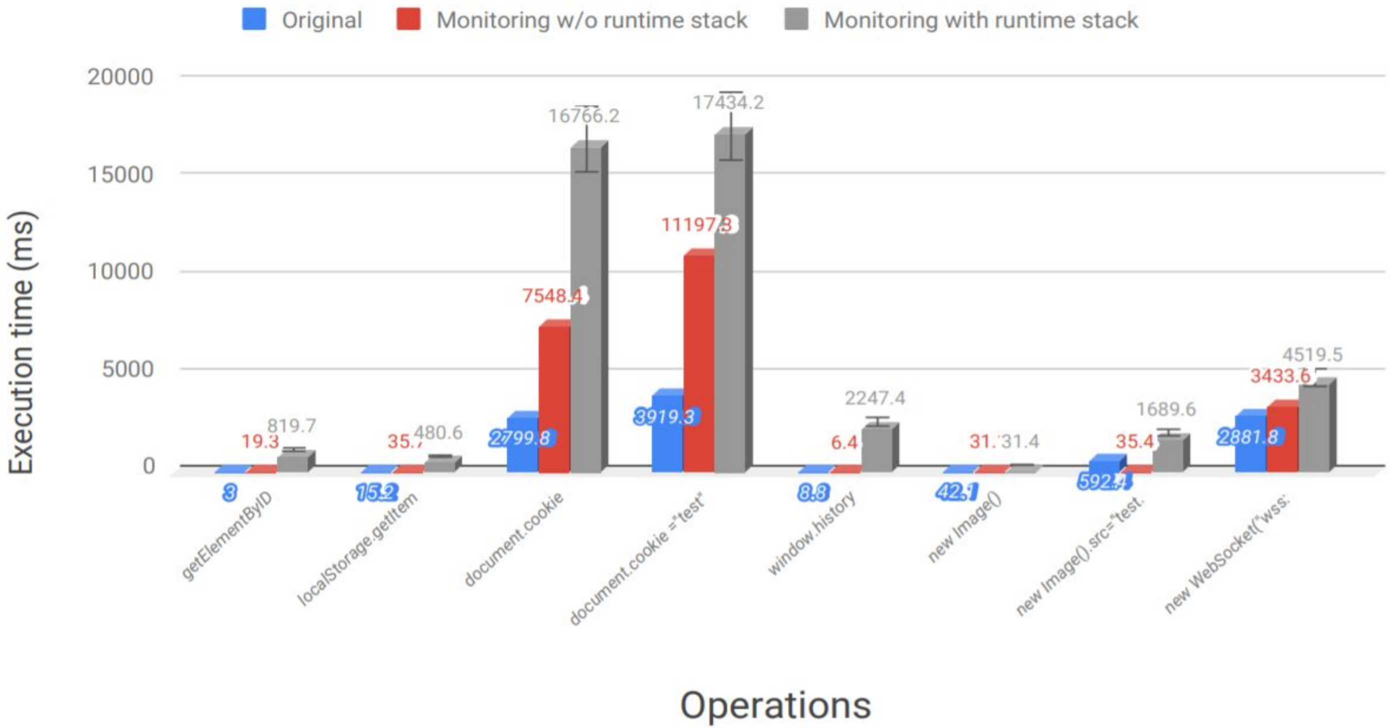
Highlights from the Chrome 77 update

Runtime Evaluation

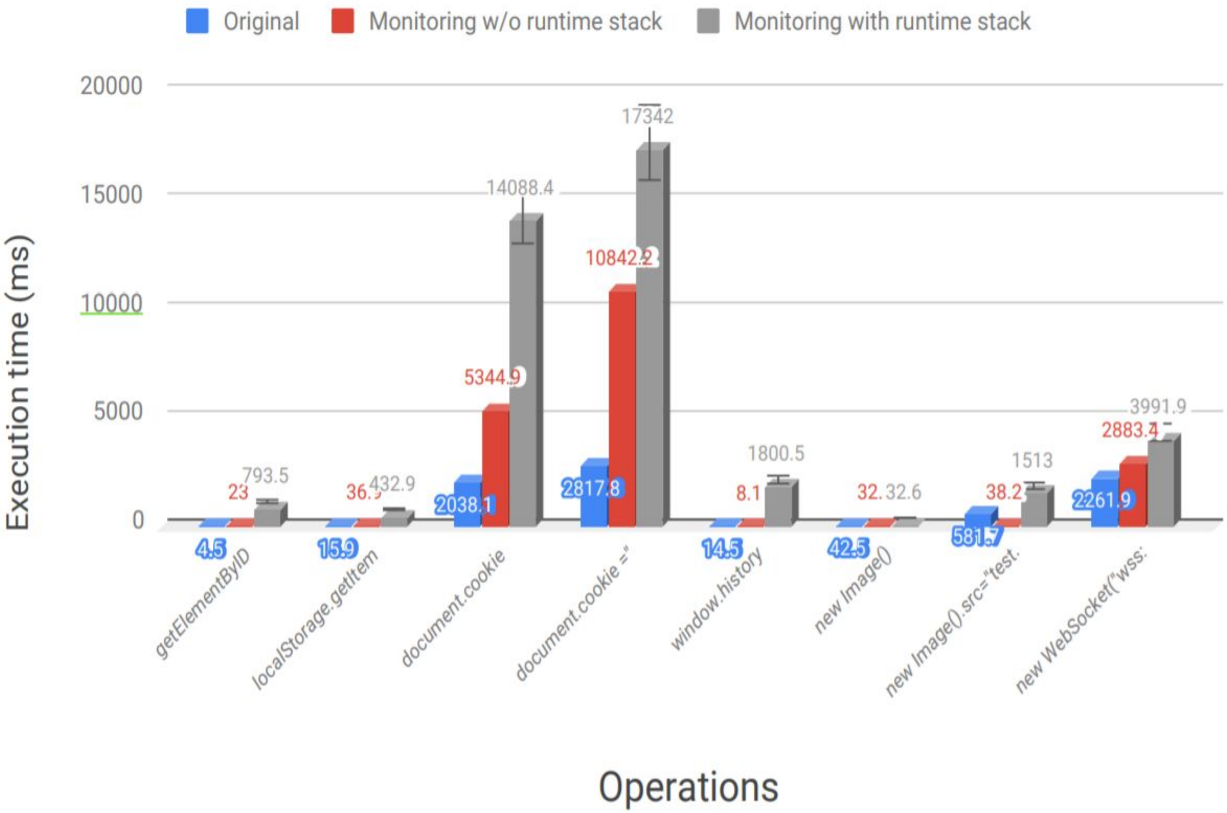
We tested MyWebGuard with both Chromium and Brave browsers (on Ubuntu 18.04.2 LTS) using our testing simulation

There exists a slowdown time on both browsers, which is due to the runtime stack that helps track the code origin

Performance overhead in Chromium



Performance overhead in Brave


🟦 Original
🟥 Monitoring w/o runtime stack
⬜ Monitoring with runtime stack
Execution time (ms)
getElementByID
localStorage.getItem
document.cookie
document.cookie ="
window.history
new Image()
new Image().src="test.
new WebSocket("wss:
Operations