COMP 4108 – COMPUTER SYSTEMS SECURITY

Assignment 4

Student Name: Ben Cendana
Student #: 100811212
Date: April 9 2018

Contents

1.0: Sandboxing

1.1: Is Sandboxing A Specific Technology??

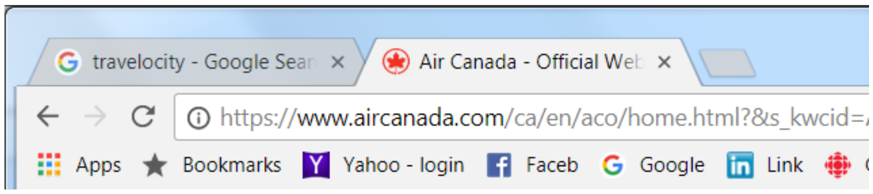

travelocity - Google Sear
Air Canada - Official Web
https://www.aircanada.com/ca/en/aco/home.html?&s_kwcid=
Apps
Bookmarks
Yahoo - login
Faceb
Google
Link

Figure 1: Chrome Sandboxing

From a conceptual perspective sandboxing is not a specific technology but rather a concept that attempts to isolate code, processes and applications through the means of containment.

Since different vendors may try to implement sandboxing in different ways there is no such specific technology, but the goal of separating applications to provide a higher level of security is universally the same for all vendors. Whether or not each vendor achieves a perfect sandbox is left to the method of implementation by the vendor.

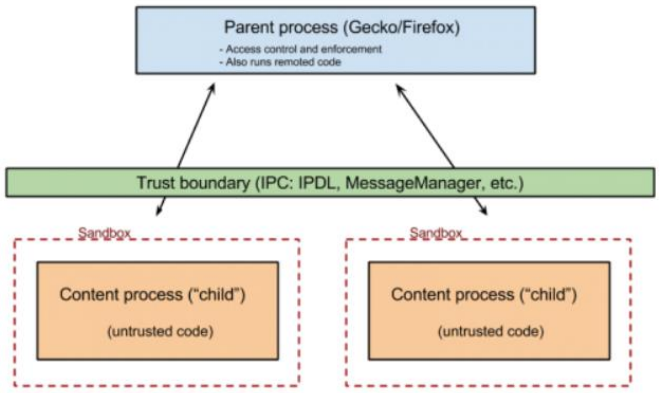

Parent process (Gecko/Firefox)
- Access control and enforcement
- Also runs remoted code
Trust boundary (IPC: IPDL, MessageManager, etc.)
Sandbox
Content process ("child")
(untrusted code)
Sandbox
Content process ("child")
(untrusted code)

Figure 2: Firefox Sandboxing

For example in Figures 1-2, both Chrome and Firefox attempt to implement sandboxing in different ways. Chromes method of sandboxing is to use tabs while Firefox attempts to implement sandboxing at the process level.

The method of implementation by both browsers are clearly different and both have there advantages and disadvantages, but as previously mentioned the goal of containment is the same for both Chrome and Firefox.

2.0: Protection Boundaries within a Process Vs. Protection Boundaries within an Operating System.

2.1: Protection Boundaries Within A Process

Since processes involve multithreading its very difficult to apply a protection boundary on each process, this is because in a multithreaded environment the thread and CPU scheduler must be made aware of what each process is executing or what part of memory is being accessed. As a consequence each process becomes aware of what task the other process is executing and is no longer isolated from the rest of the system.

2.2: Protection Boundaries Within An Operating Systems

Unlike a process its easier to apply protection boundaries to an operating system because the kernel has assigned blocks of memory that only the operating system can access.

Assuming virtual machine or VM ware is being used the hypervisor can help to create a level of abstraction by providing a level of control between the physical memory and the operating system. In some cases the memory might not even exist and actually be virtual memory.

Therefore its easier to apply a protection boundary to an operating system since the OS gets allocated memory that only the kernel can access and if VM is used the hypervisor strictly controls the memory use, creation and allocation.

3.0: Implementing Security Restrictions.

Since function calls access memory to complete a code subroutine and have direct access to the physical memory it can be argued that it is less secure since there is no control on what it can access.

In contrast operating system calls are based on the user or application making some type of request for the operating system to perform, if these requests are approved it can be executed.

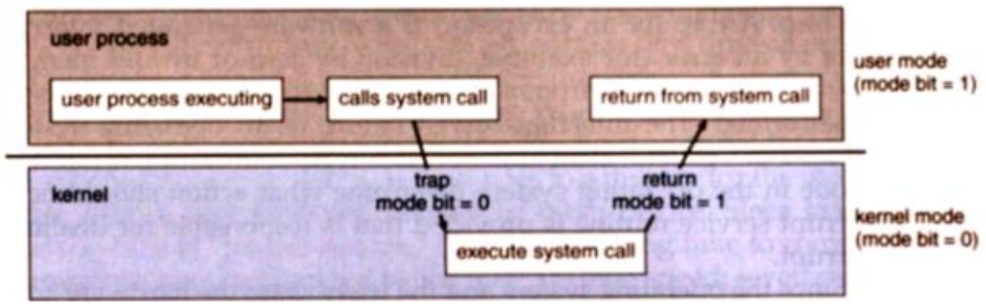


Figure 3: An Example Of A System Call Being Executed

As we can see in Figure 3 the operating system operates in two modes user mode and kernel mode, the kernel mode has full access to the CPU were as the user mode lacks any direct access to the CPU or memory.

In order for the user mode to gain access to the CPU it must either go through an API or the kernel mode.

As a result this layout indirectly features an interface with security restrictions, this is because all system calls must first be made in the user mode and if the request is valid the kernel mode will execute the request.

Thus operating system calls are far superior to function calls as an interface with security restrictions because of the layer of control to the physical hardware.

4.0: language Runtimes – Security Properties

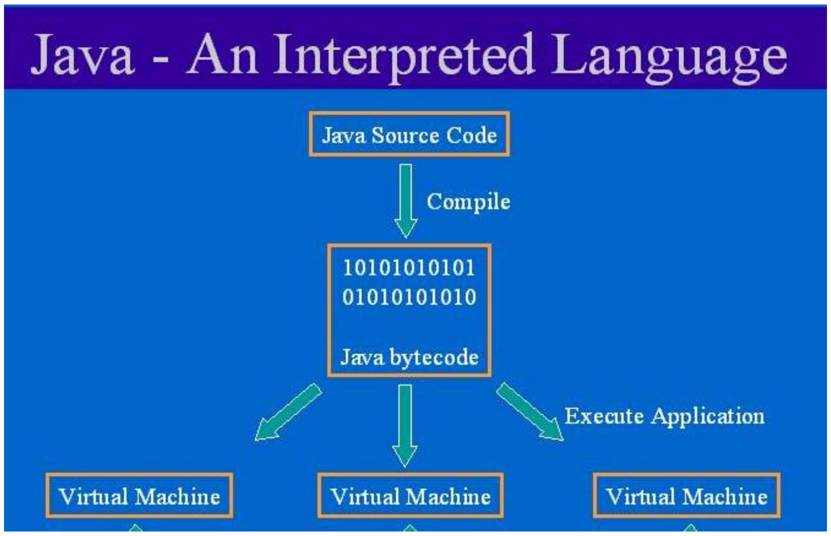


Figure 4: Java Interpreted Language Architecture

4.1: Language Runtime and Security

Interpreted languages such as the JVM runtime(Java Virtual machine) differ from compiled code as the code is never actually compiled after executed.

Instead its converted into a bytecode which is only readable by the JVM runtime, the JVM reads the bytecode, compiles it into machine code and then the CPU executes the machine code.

This offers a level of abstraction which then offers a layer of security and control as the JVM is the only application that actually has direct access to the CPU or memory.

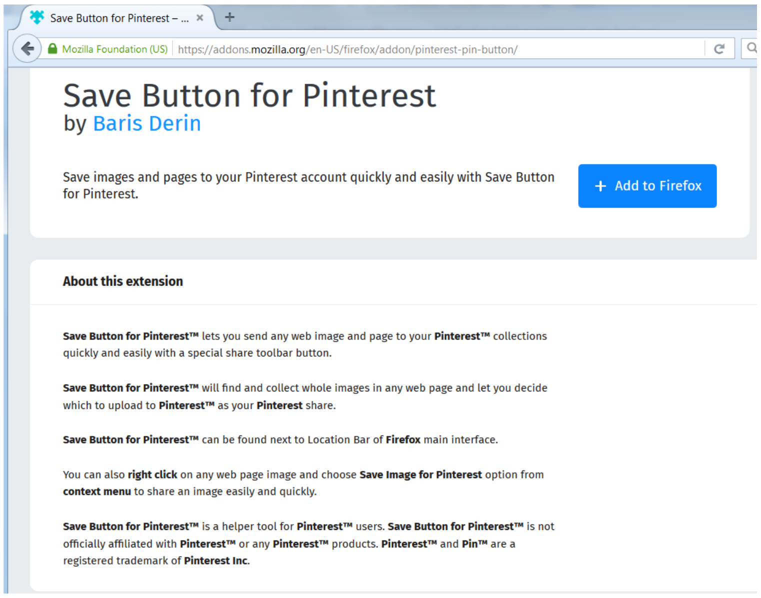
4.2: Machine Code Binaries and Security

Machine code binaries are considered less secure and don't offer the same security guarantees simple because they have direct access to the physical hardware.

Once the code binary is compiled into machine code and executed it is directly run by the CPU and accesses the memory. if the binary is malicious there is no longer any level of abstraction to prevent the binary from manipulating the physical memory or altering the kernel files.

5.0: Firefox Pinterest Save Button Extensions

5.1: What Does The Extension Do?



Save Button for Pinterest – ...

Mozilla Foundation (US) https://addons.mozilla.org/en-US/firefox/addon/pinterest-pin-button/

Save Button for Pinterest
by Baris Derin

Save images and pages to your Pinterest account quickly and easily with Save Button for Pinterest.

+ Add to Firefox

About this extension

Save Button for Pinterest™ lets you send any web image and page to your **Pinterest™** collections quickly and easily with a special share toolbar button.

Save Button for Pinterest™ will find and collect whole images in any web page and let you decide which to upload to **Pinterest™** as your **Pinterest** share.

Save Button for Pinterest™ can be found next to Location Bar of **Firefox** main interface.

You can also **right click** on any web page image and choose **Save Image for Pinterest** option from **context menu** to share an image easily and quickly.

Save Button for Pinterest™ is a helper tool for **Pinterest™** users. **Save Button for Pinterest™** is not officially affiliated with **Pinterest™** or any **Pinterest™** products. **Pinterest™** and **Pin™** are a registered trademark of **Pinterest Inc.**

Figure 5: Pinterest Save Button Extension

As we can see in Figures 5 – 6 this extension allows a user to add images directly into there Pinterest account. The user browses with a Firefox browser and if there is a image they like they can right click the mouse over the image and add it to there Pinterest account (Figure 6).

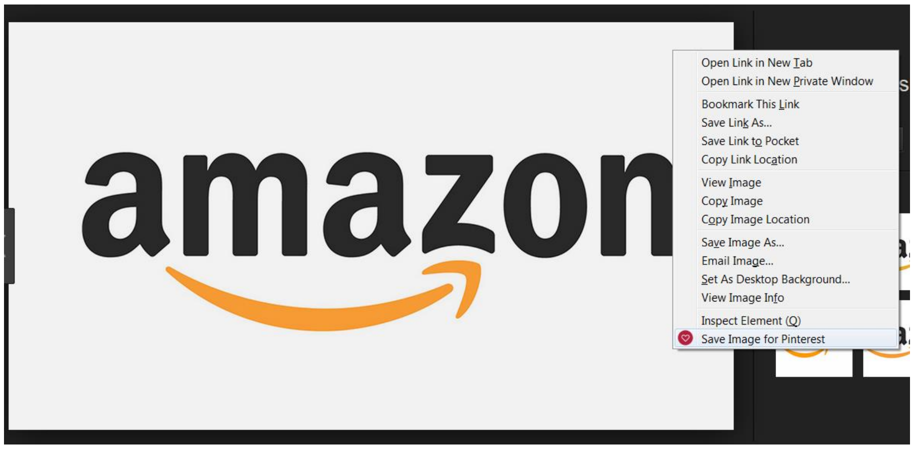
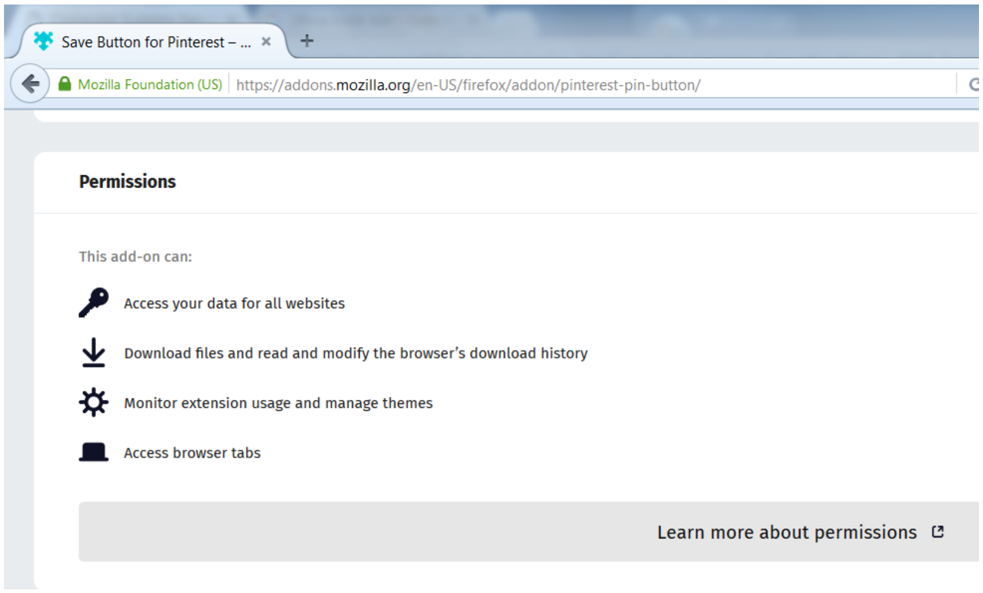


Figure 6: Pinterest Save Button Extension In use

5.2: What Permissions Does It Require?


Save Button for Pinterest – ...
Mozilla Foundation (US)
https://addons.mozilla.org/en-US/firefox/addon/pinterest-pin-button/

Permissions

This add-on can:

- Access your data for all websites
- Download files and read and modify the browser's download history
- Monitor extension usage and manage themes
- Access browser tabs

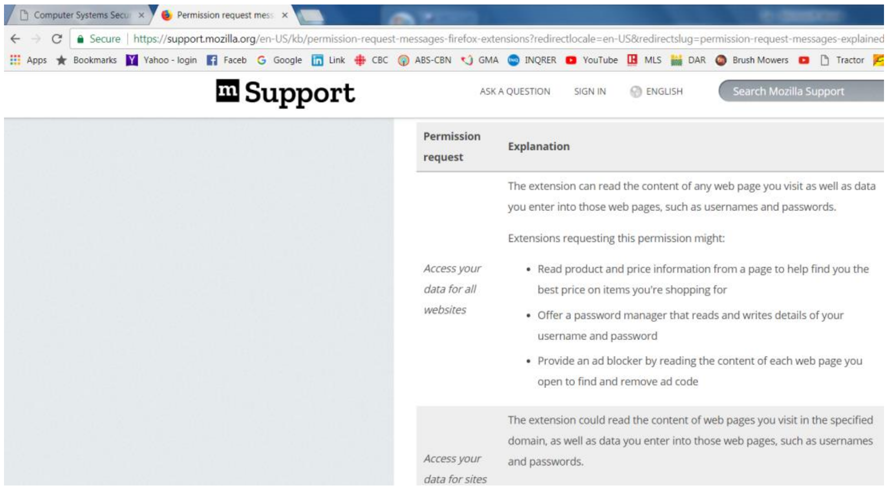
Learn more about permissions

Figure 7: Save Button For Pinterest

As can be seen in Figure 7 the Save Button For Pinterest extension requires permissions to:

1) Access data on all the websites.
2) Download Files and Read and Modify The Browser's Download History.
3) Monitor Extension Usage and Manage Themes.
4) Access Browser Tabs.

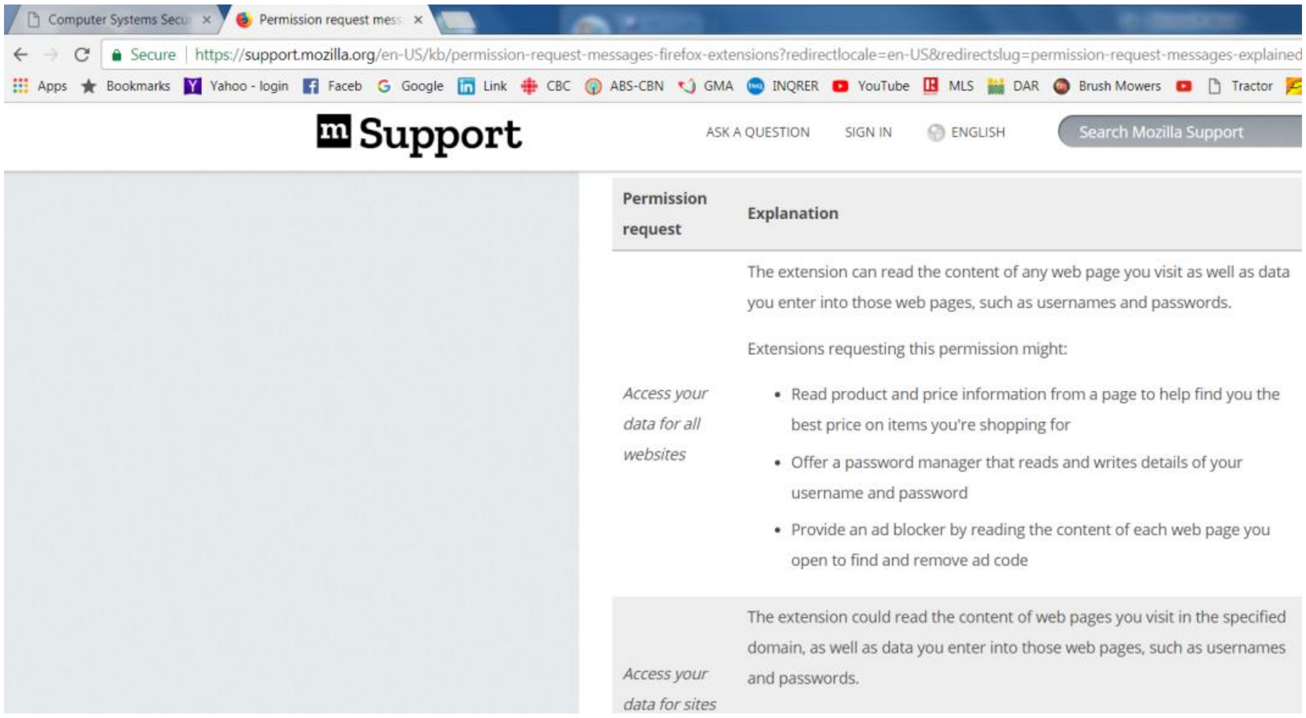
5.3: Why Does It Need These Permissions?



Permission request	Explanation
Access your data for all websites	The extension can read the content of any web page you visit as well as data you enter into those web pages, such as usernames and passwords. Extensions requesting this permission might: • Read product and price information from a page to help find you the best price on items you're shopping for • Offer a password manager that reads and writes details of your username and password • Provide an ad blocker by reading the content of each web page you open to find and remove ad code
Access your data for sites	The extension could read the content of web pages you visit in the specified domain, as well as data you enter into those web pages, such as usernames and passwords.

Figure 8: Firefox Extensions Explanation

5.3.1: Access Your Data For All Websites



Permission request	Explanation
Access your data for all websites	The extension can read the content of any web page you visit as well as data you enter into those web pages, such as usernames and passwords. Extensions requesting this permission might: • Read product and price information from a page to help find you the best price on items you're shopping for • Offer a password manager that reads and writes details of your username and password • Provide an ad blocker by reading the content of each web page you open to find and remove ad code
Access your data for sites	The extension could read the content of web pages you visit in the specified domain, as well as data you enter into those web pages, such as usernames and passwords.

Figure 9: Firefox - Access Your Data For All Websites

As we can see in Figure 9, Firefox provides a generic explanation why this extension needs access to your data.

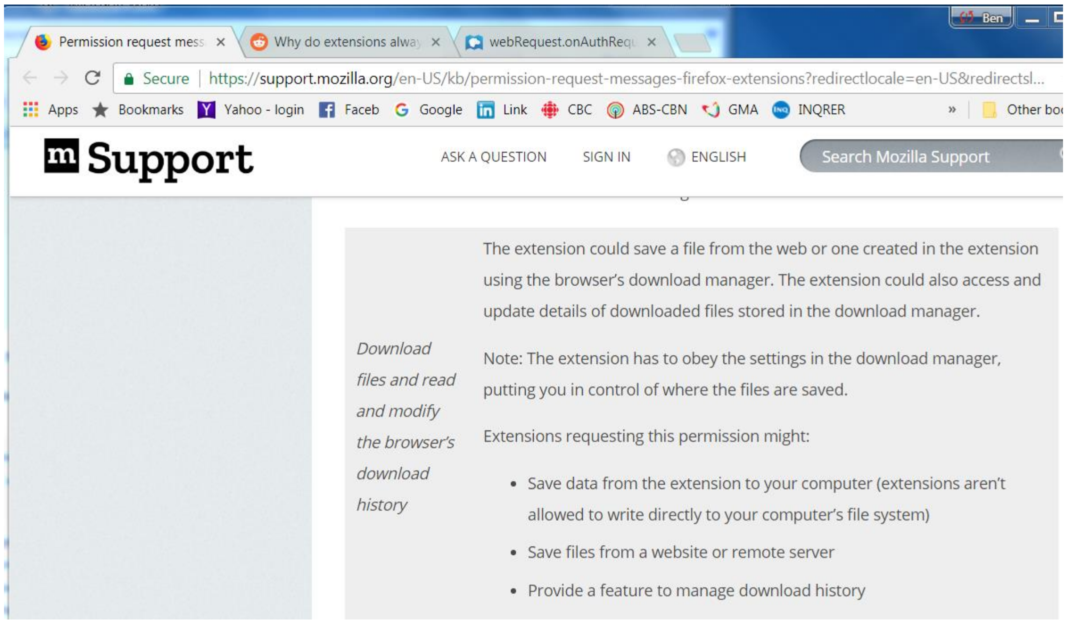
Disregarding the Firefox explanation the real reason why this extension needs permision to access your data is because whenever your viewing a website the web proxy will need to validate the users login credentials.

The proxy will call the function webRequest.onAuthRequired() which will then be used to validate the username and password.

If this extension did not have the users login credentials the user would be required to enter them with a popup every time the user needs to be validated, thus making it convenient for the user by having them saved.

The disadvantage is the users login credentials could be compromised, this disadvantage will be explained in the next section.

5.3.2: Download Files and Read and Modify the Browser's Download History



Download files and read and modify the browser's download history

The extension could save a file from the web or one created in the extension using the browser's download manager. The extension could also access and update details of downloaded files stored in the download manager.

Note: The extension has to obey the settings in the download manager, putting you in control of where the files are saved.

Extensions requesting this permission might:

- Save data from the extension to your computer (extensions aren't allowed to write directly to your computer's file system)
- Save files from a website or remote server
- Provide a feature to manage download history

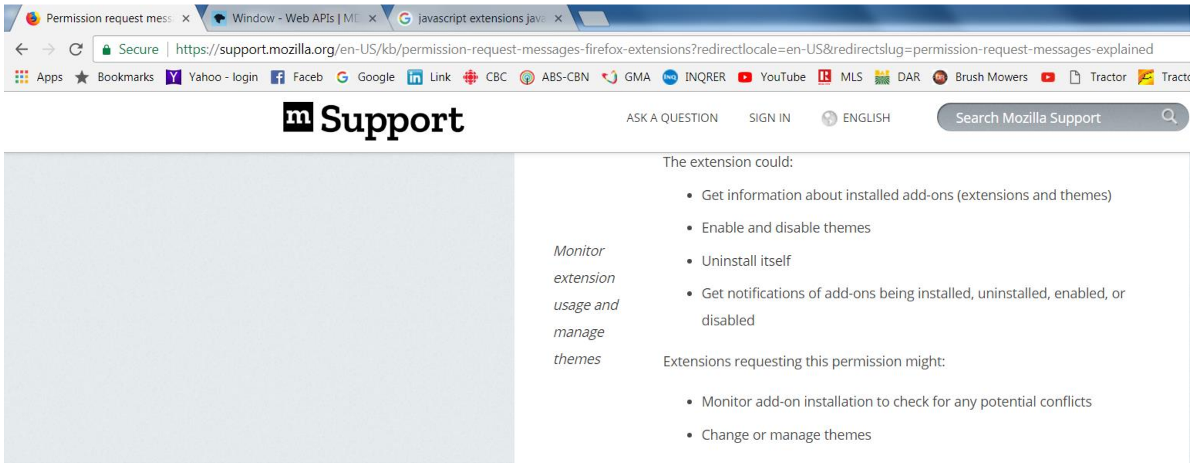
Figure 10: Firefox - Download Files and Read and Modify the Browser's Download History

Despite the explanation provided by Firefox in Figure 10 the extension most likely needs permissions to download and modify the browsers history.

It also needs these permissions to download image files which will then be added to the Pinterest account through the JavaScript function browser.downloads.download().

Next access privileges will be needed to execute the function Window.history() which will be used to modify the browsers history.

5.3.3: Monitor Extension Usage and Manage Themes



Monitor extension usage and manage themes

The extension could:

- Get information about installed add-ons (extensions and themes)
- Enable and disable themes
- Uninstall itself
- Get notifications of add-ons being installed, uninstalled, enabled, or disabled

Extensions requesting this permission might:

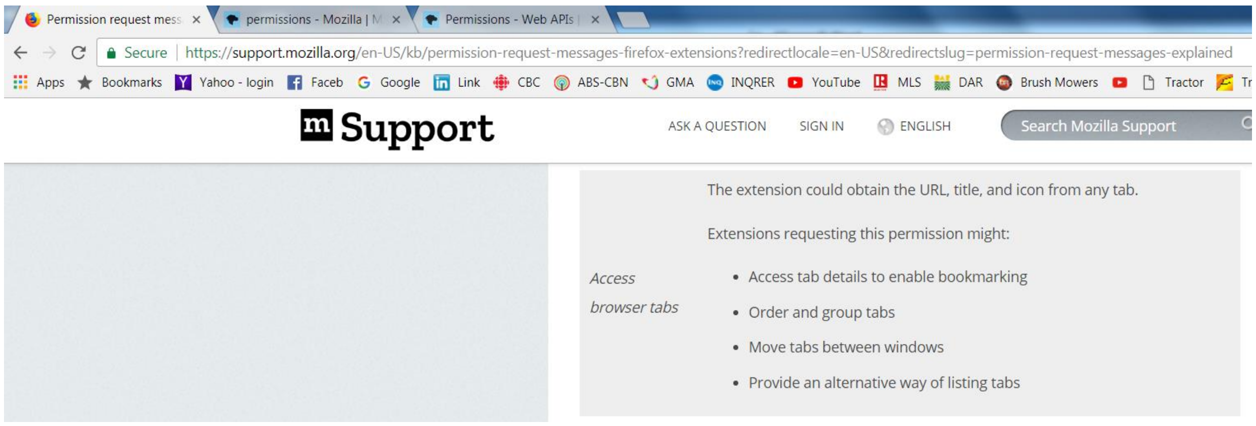
- Monitor add-on installation to check for any potential conflicts
- Change or manage themes

Figure 11: Firefox - Monitor Extension Usage and Manage Themes

Although Firefox provides us with an explaination why the extension needs this type of permission (Figure 11) we can determine that the primary purpose for this extension is to be able to manage all the extensions this includes updates, installation and the access privileges through enabling/disabling.

The Firefox API JavaScript function theme() and permissions() will be needed to be given permission to update the browser and to grant or revoke the extension(s) permissions to run.

5.3.4: Access Browser Tabs



Access browser tabs	The extension could obtain the URL, title, and icon from any tab. Extensions requesting this permission might: • Access tab details to enable bookmarking • Order and group tabs • Move tabs between windows • Provide an alternative way of listing tabs

Figure 12: Firefox – Access Browser Tabs

The assumption is the extension needs this level of permission (Figure 12) to get html and JavaScript information from the browser in order to modify the browser. The Firefox API functions browser.extension.getURL() and window() will need to have elevated permissions inorder to execute.

5.4: The Extension Performing Actions Unrelated to its Purpose with these Permissions

By allowing these permissions the JavaScript code now has more access privileges then it should have. An attacker can now take advantage of the elevated permissions and use the JavaScript beyond its original purpose and exploit a vulnerability called cross-site scripting.

Cross-Site Scripting or XSS is a JavaScript injection attack were an attacker uses a websites vulnerabilities to attack visitors that visit that site, XSS has three types of attacks these are:

1) Reflected.
2) Dom Based
3) Stored.

Since this extension now has greater privileges and involves adding images to a Pintrest account all of the three types of attacks are applicable since the JavaScript has elevated privileges and no control from the user.

5.4.1: Cross-Site Scripting – Reflected

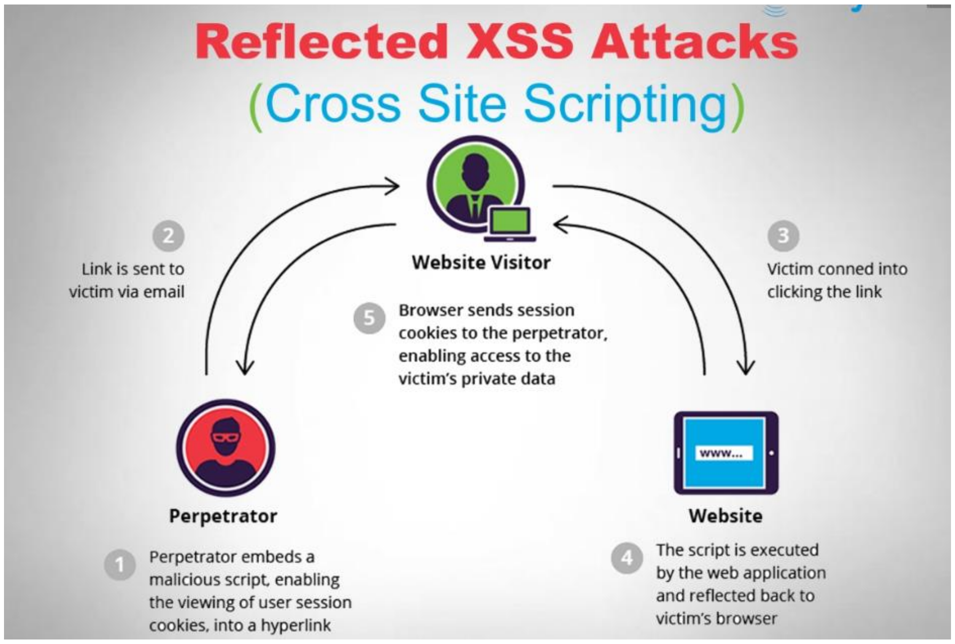

Reflected XSS Attacks
(Cross Site Scripting)
Website Visitor
2 Link is sent to victim via email
3 Victim conned into clicking the link
5 Browser sends session cookies to the perpetrator, enabling access to the victim's private data
Perpetrator
1 Perpetrator embeds a malicious script, enabling the viewing of user session cookies, into a hyperlink
www...
Website
4 The script is executed by the web application and reflected back to victim's browser

Figure 13: A Reflected Cross-Site Scripting (XSS) Attack

This type of attack occurs when a perpetrator/attacker sends malicious code to a server that replaces the content on a webpage. Whenever the user requests to access the website the server responses by displaying only the website changes made by the attacker.

This type of attack could impact the Pintrest user as they may be unaware of any changes on the main website were the image content was saved from.

5.4.2: Cross-Site Scripting – DOM Based

This type of attack differs as it only modifies the clients response and not the servers response as was done in the previous type of attack.

Instead of making website changes malicious JavaScript code is injected into text fields or the url input box. Since almost everything in JavaScript is an object the attacker can use the injected code to extract data. Whenever the user adds image links to there Pinetrest account there essentially adding more JavaScript objects that can access there data.

5.4.4: Cross-Site Scripting – Stored

This type of attack is similar to the previous DOM based attack the only difference is the malicious script gets permanently stored into the website, commonly this attack occurs in web forums or databases.

An excellent example on how this attack works is lets assume a web forum contains a user thread and a reply section which posts all users comments. Instead of posting a comment an attacker can inject code into a text field which will then get posted on the webpage if they click reply or add.

This extension can be susceptible to this type of attack if the image being saved is coming from a web forum with malicious code being saved.

6.0: IOS Runtime Security Vs. OS Virtualization

It can be argued that both iOS and OS Virtualization are conceptually similar since they both implement:

1) Containers/sandboxing.
2) Limited access to the physical hardware.
3) Access Privileges.

However both implement containers/sandboxing and the Physical hardware differently and are therefore not similar from an architectural perspective. We can then state that both iOS and OS Virtualization are conceptually similar but are architecturally different because of the differences in implementation.

6.1: Containers/Sandboxing IOS vs. OS Virtualization

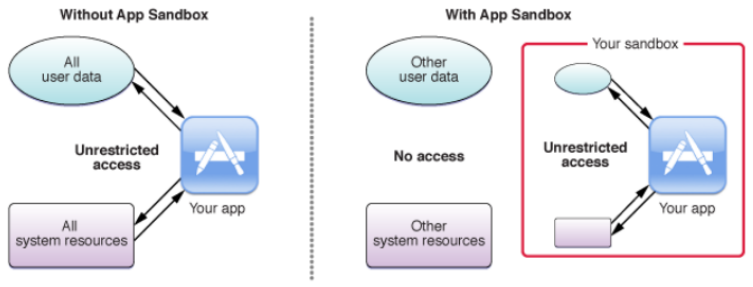
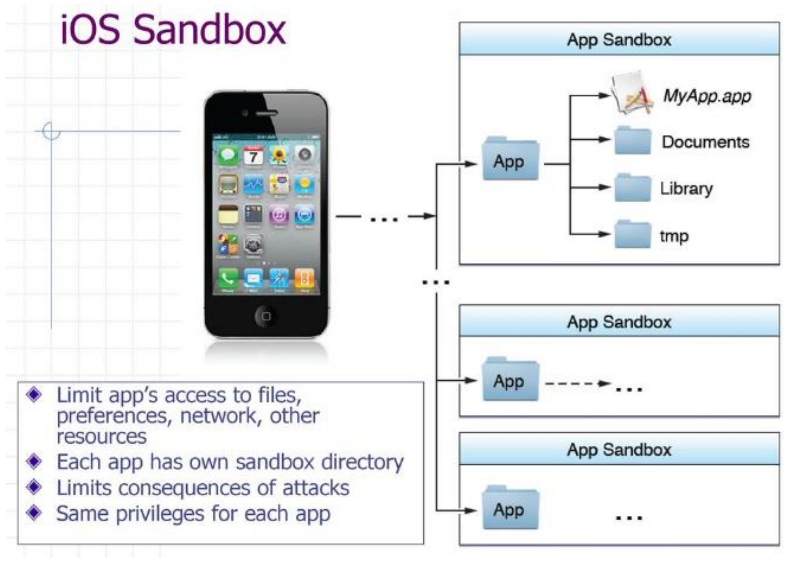


Figure 14: An Application With Sandboxing/Containers Implemented



Limit app's access to files, preferences, network, other resources
Each app has own sandbox directory
Limits consequences of attacks
Same privileges for each app

Figure 15: The IOS Security Model

As demonstrated in Figure 15 the iOS model implements sandboxing by making use of access privileges to isolate and maintain each application and process, it also isolates the home folder of every application (Figure 15).

In contrast OS Virtualization sets up the guest operating systems to operate as separate containers (Figure 16).

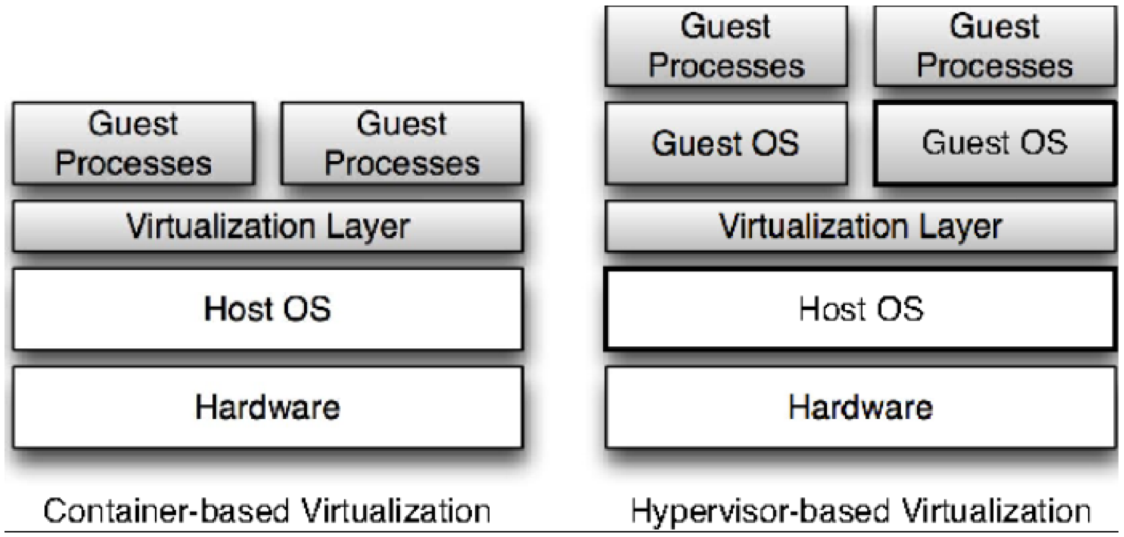


Figure 16: OS Virtualization Containers

Therefore both iOS and OS virtualization are similar for implementing containers as a security measure, but they differ with iOS sandboxing starting at the operating system level with each application and file being sandboxed within the OS, In contrast OS Virtualization only starts sandboxing with the guest OS.

6.2: Access To Hardware IOS vs. OS Virtualization

Since iOS operates at the read only mode and API's are prevented from escalating there own privileges access to the physical hardware becomes difficult.

Similarly access to the hardware is difficult in OS Virtualization but unlike iOS access is controlled by the hypervisor which manages the guest operating systems hardware allocation.

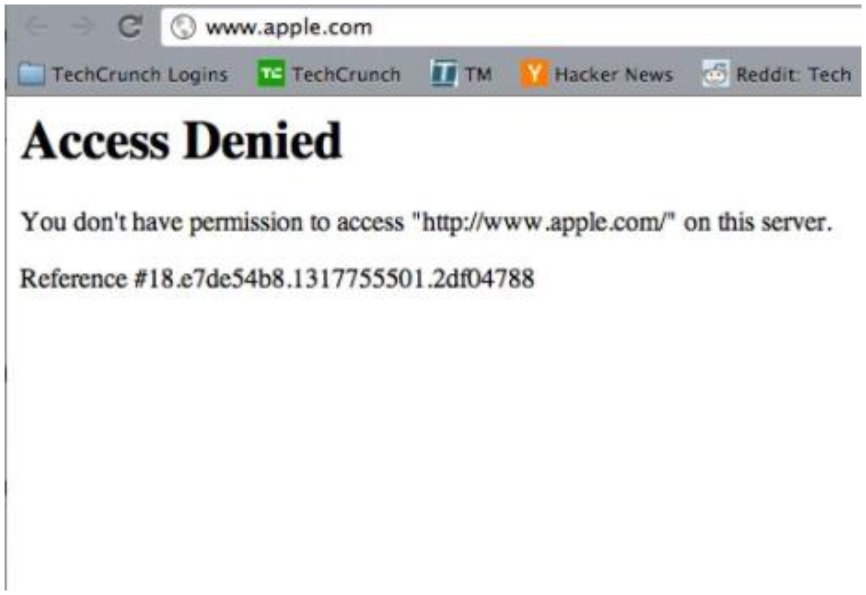
6.3: Access Privileges IOS vs. OS Virtualization

Assuming that the OS virtualization environment is Linux then the access privileges should be the same for both iOS and the OS Virtualization. This is because both Linux and iOS are Unix based operating systems with similar access privileges.

7.0: Definitions

7.1: Whitelists

A whitelist is defined as a list of allowable content into the network this include: websites, packets and etc all other content is subsequently blocked.



Access Denied

You don't have permission to access "http://www.apple.com/" on this server.

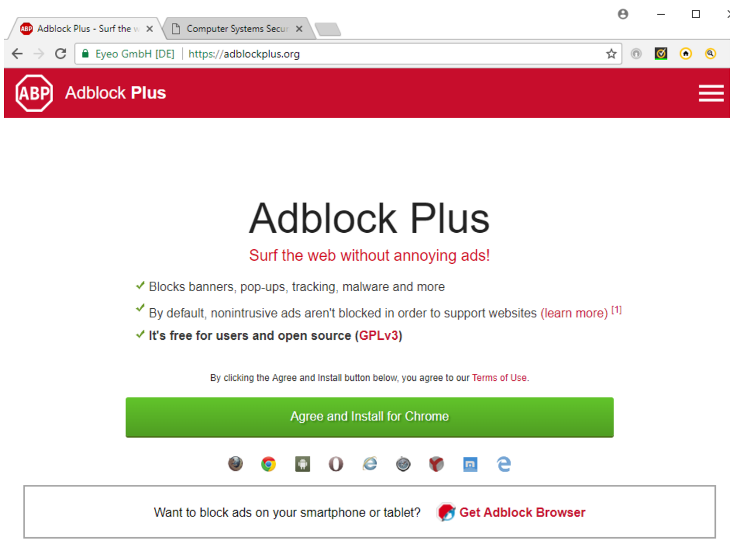
Reference #18.e7de54b8.1317755501.2df04788

Figure 17: Blocked Website As A Whitelist

A common security mechanism used to implement whitelists is a website blocker, the blocker can typical be found within large organizations where access is restricted to allowable websites only.

This strategy relates to the security mechanism as it prevents employees from accessing websites of rival corporations and/or it prevent rivals from accessing there network(s). It can also can be considered an effective security mechanism since it only allows packets that the administrator knows of into the network.

7.2: Blacklists


Adblock Plus - Surf the w

Computer Systems Secur

Eyeo GmbH [DE] | https://adblockplus.org

Adblock Plus

Adblock Plus

Surf the web without annoying ads!

✓ Blocks banners, pop-ups, tracking, malware and more

✓ By default, nonintrusive ads aren't blocked in order to support websites (learn more) [1]

✓ **It's free for users and open source (GPLv3)**

By clicking the Agree and Install button below, you agree to our Terms of Use.

Agree and Install for Chrome

Want to block ads on your smartphone or tablet? **Get Adblock Browser**

Figure 18: Adblock Plus As A Blacklist

A blacklist is the opposite of a whitelist were all content is allowed into the network and only web content on the blacklist will be blocked.

The security mechanism used to implement this type of strategy is an adblock where malicious content is filtered from entering the users browser.

This strategy relates to the mechanism as the user has unrestricted web access which improves efficiency but the organization can still block malicious content out.

7.3: Anomaly Detection

Anomaly detection is a misunderstood and underappreciated aspect of computer security its main strategy is to monitor network traffic for strange and unusually network behaviors.

The type of security mechanism used to detect anomalies are auditing software such as wireshark and a security officer that monitors the network for unusually network traffic.

This strategy relates to the security mechanism as the security officer looks for drops in network bandwidth or unusually user activity which would be considered strange and indicate some type of intrusion could be occurring.

7.4: Virtualization

Virtualization is a level of abstraction between a physical resource that exists and an artificial resource that is perceived to exist.

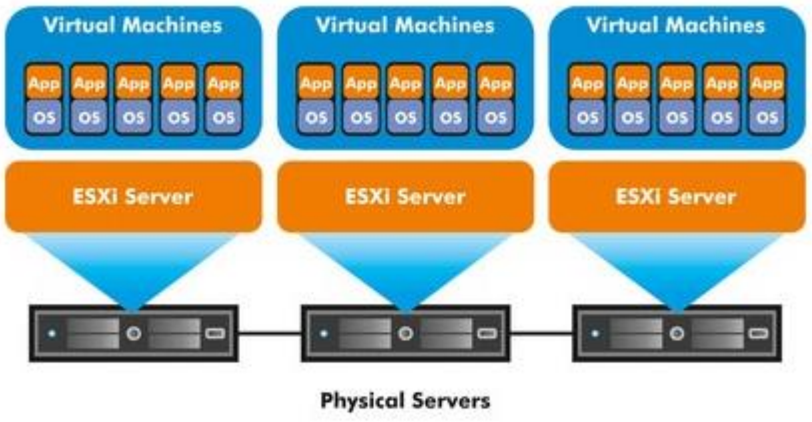


Figure 19: An Example Of Virtualization With Servers

The security mechanism for this type of implementation is a layer of abstraction that creates the illusion that the guest operating system(s) actually exists when it doesn't.

This strategy relates to the security mechanism as an attacker may perceive that each guest OS exists while also being unable to get control of the actual OS environment.

8.0: Bibliography

Section 3.0 – 4.0

1.12. System Calls." *1.12. System Calls - Operating Systems Study Guide*, Kansas Polytechnic , 2009, faculty.salina.k-state.edu/tim/ossg/Introduction/sys_calls.html.

"Coding Horror." *Understanding User and Kernel Mode*, Jan. 2008, https://blog.codinghorror.com/understanding-user-and-kernel-mode/.

Section 5.0

"Save Button For Pineterest." *Save Button For Pineterest*, Brian Derin, Feb. 17. 2018, https://addons.mozilla.org/en-US/firefox/addon/pinterest-pin-button/

What Is Cross-Site Scripting." *What Is Cross-Site Scripting*, David Evana, Aug.12. 2015, https://www.youtube.com/watch?v=ddcQ688eO7U

Section 6.0 – 7.0

"SystemsSec 2018W Lecture 20", SystemsSec 2018W Lecture 20, Anil Somayaji, Mar. 29 2018. https://homeostasis.scs.carleton.ca/wiki/index.php/SystemsSec_2018W_Lecture_20