

A pattern for Web Browser Infrastructure

Paulina Silva
Departamento de Informática
Universidad Técnica Federico
Santa María
Valparaíso, Chile
pasilva@alumnos.inf.utfsm.cl

Raúl Monge
Departamento de Informática
Universidad Técnica Federico
Santa María
Valparaíso, Chile
rmonge@inf.utfsm.cl

Eduardo B. Fernandez
Department of Computer &
Electrical Engineering and
Computer Science
Florida Atlantic University
Boca Raton, FL, USA
fernande@fau.edu

ABSTRACT

Currently, most software development is focused in creating systems connected to the Internet, which allows to add functionality within a system and facilities to their *Stakeholders*. This leads to depend on a *web client*, such as *Web Browser*, which allows access to services, data or operations that the system delivers. However, the Internet influences the attack surface of the system, and unfortunately many stakeholders and developers are not aware of the risks to which they are exposed. The lack of security education among software developers and the scarce and scattered documentation for browsers (and standardization) could become a big problem in large architectural developments that depend on browsers to perform their services. A Reference Architecture of the *Web Browser*, using Architectural Patterns, could be a starting point for understanding its security mechanisms and architecture, which interacts with a bigger web system. This would unify ideas and terminology, giving a holistic view of independent implementation details for both the browser and the system it communicates with. We developed a Browser Infrastructure pattern that describes the infrastructure to allow the communication between a Web Client and a Server in the Internet. With this work we propose an architectural pattern as the first piece of our Reference Architecture for Web Browsers and security concerns.

Keywords

Browser, Web Client, Browser Architecture, Reference Architecture, Pattern

Introduction

Patterns are encapsulated solutions to recurrent problems and define a way to express requirements and solutions concisely, as well as providing a communication vocabulary for designers [1]. The description of architectures using patterns makes them easier to understand, provides guidelines

for design and analysis, and can define a way of making their structure more secure.

Security patterns describe solutions to problems that arise from controlling (stopping or mitigating) a set of specific threats through security mechanisms, defined in a given context. The most common use of security patterns is to help application developers -who are not security experts- to add security in their designs. Patterns of this kind are also used to reinforce a legacy system.

The aim of a Reference Architecture is to provide a guide for developers, who are not security experts, to develop architectures for concrete versions of the system or to extend such system. With the use of architectural patterns we describe the Browser Architecture as a Reference Architecture (RA). An RA is created by capturing the essentials of existing architectures and by taking into account future needs and opportunities, ranging from specific technologies, patterns and business models. It can also be derived from domain models.

A Security Reference Architecture is a Reference Architecture where security services have been added in appropriate places to provide some degree of security for a specific system. The basic approach we will use to build a Security Reference Architecture is the application of a systematic methodology from [2, 3, 4], which can be used as a guideline to build secure web browser systems and/or evaluate their security levels. The first step was to build a Reference Architecture in a student work, and now we are trying to improve it using security patterns and misuse patterns. By checking if a threat, expressed as a misuse pattern, can be stopped or mitigated in the security reference architecture, we can evaluate its level of security.

In this work, a Browser Infrastructure Pattern is presented as a first step in to the process of developing a Reference Architecture (RA) and Security Reference Architecture (SRA) for the Web Browser. The audience to which our paper is focused are Browser developers, Web Application developers and even normal users. Being the first two the most important, since they are the responsables for the implementation and correct use of secure mechanisms while a user is browsing in the Internet. Secure communication is an important matter, but in this work the focus will be on how to control the responses a Browser receives. Threat analysis and security patterns were done in a previous work, we will improve the architecture in the construction of the SRA.

Browser Infrastructure Pattern

Intent

The Browser Infrastructure describes the architecture for the processing of a user request for web resources in the Internet.

Example

Within the Host is possible that resources are needed to fulfill the user needs are limited. The request of external services or resources is the main reason of the Internet existence. If a user needs to make a bank transaction, such as deposit money to another party, the Browser User will type an URL in the browser to access the online banking service of the bank the user belongs to.

Context

Users need to access services or information in the Internet, for which they use browsers. A browser starts by accepting a URL from a user and sending it to the corresponding IP address. It also receives the answers that the users want.

Problem

Internet users need resources from Providers, but they may need them in a specific format, for example to be visualized the screen of computer. In this case, if appropriate tools are not available, the resource could not be helpful and it cannot be used correctly. How can the Host and Provider provide these functions? The solution to this problem must resolve the following forces:

- *Transparency*: the user should not be concern about how his request is performed.
- *Stability*: The browser must be capable of working, even if a web page can not be displayed properly or there is an internal problem in the server.
- *Isolation*: Each *request* must not interrupt others.
- *Heterogeneity*: It does not matter the type of Provider with which the browser communicates, it should be possible to interact with whatever type, and it should be capable of showing the content of the obtained resource adequately.

Solution

Provide a device, the Web Browser, with the functions needed to understand user requests and send them to the Provider. A web browser satisfies a request of a Browser User of the Host.

Structure

In Figure 1 the **Browser Kernel** is an entity that represents the main process of a Web Browser, which is constantly communicating with the host of the browser. A user who makes a **Request** to a Internet resources using a Web Browser, will be called **Browser User**. At the same time, a **Provider** is responsible for receiving external requests. According to the request, a **Provider** will send the **Service** (or resource) the **Browser User** needs in a **Response** message. Most Browsers use a central component to do operations that need to affect the Host of the Browser, a **Browser Kernel**. Figure 1 shows the Class diagram for

the Browser Infrastructure Pattern. For each new resource a **Browser Kernel** request a created or reused **Web Content Renderer** instance is used; this will inherit the **Controlled Process** properties and its methods. A **Plugin** and an **Extension** are elements that extend the functionality of the browser; the extender being for the exclusive use of the browser while the plugin can be used in other systems, such as the Adobe Reader Plugin. A **Sandbox** is a Controlled Execution Domain [5] created for a single **Controlled Process** instance. The **Sandbox** allows the process memory isolation and the access control of each communication between processes, such as an instance of a **Controlled Process** with the **Browser Kernel**; this applies to a **Web Content Renderer**, a **Plugin** and an **Extension** as well. To communicate with the **Browser Kernel**, a **Proxy** created within a **Controlled Process** forwards a **Local Request** to the **Reference Monitor** inside the **Browser Kernel**. For every message sent from a **Controlled Process**, the **Reference Monitor** will check the **Domain's Rights** to permit the access. The access control which the **Sandbox** delivers to each **Controlled Process** allows the isolation between different **Domains**. Depending on the manufacturer, a **Plugin** could not be Sandboxed.

Dynamics

Some use cases are the following:

- Make Request (actor: Browser User)
- Save Resource (actor: Browser User)
- Ask for Resources (actor: Host)

We show in detail Make Request below. (Figure 2):

Summary

A Browser User needs an URL resource which can be obtained by using the HTTP protocol, as required by the Provider. The Browser Kernel will be used by a User Browser to perform the display of the URL resource.

Actor

Browser User

Preconditions

The Host must have one or more Browser Kernel for the Host user. In addition to being connected to a network or the Internet. The Provider you want to contact must also be available.

Description

Note: Messages between Browser Kernel and Sandbox can be both synchronous and asynchronous [6, 7]. We do not explain in this work synchronization details, because it is out of our scope. We are interested only in specifying who interacts with whom.

1. A Browser User requires a browser to access a URL for some resource in a Provider, this is done by using a Browser Kernel already instanced in the Host. A Browser Kernel also has a Reference Monitor to receive incoming messages from Controlled Process instances.

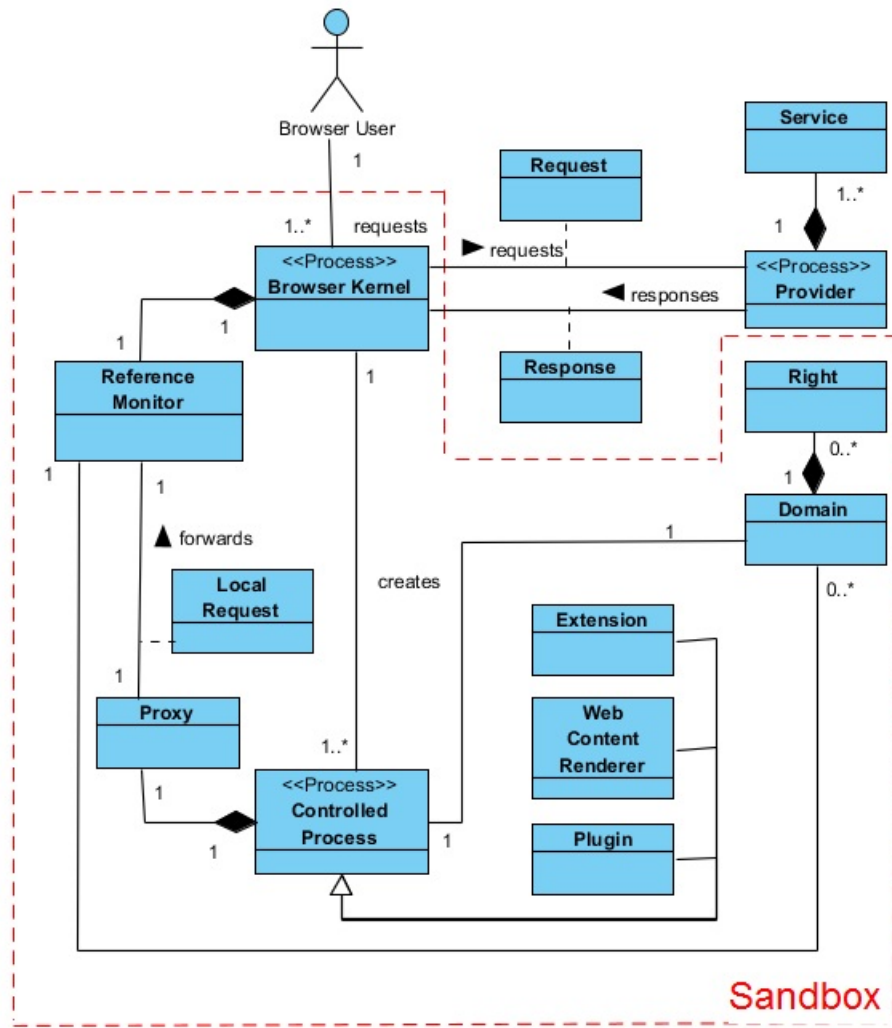


Figure 1: High-level Components of the Browser Infrastructure.

- The Browser Kernel creates an instance of a Web Content Renderer (a Controlled Process subclass), and sets the Domain and Rights. A Proxy is created in each Controlled Process instance as a mean to communicate with the Browser Kernel.
- Once the Controlled Process is ready, the Browser Kernel creates a Request which is sent to the Provider.
- The Provider will send a *Response* to the *Request* received. Depending on how it is implemented the Browser Kernel, it may or may not have to wait for the response (synchronous or asynchronous) of the Provider.
- The Response is sent by a communication channel to the Controlled Process of origin, realized it as a Web Content Renderer. If a Response was received to a Request, the Controlled Process is ready to prepare the parsing of the content or use it in a plugin or extension to support the display of the resources obtained by the URL. Otherwise, the Web Content Renderer will create an error page.
- The Web Content Renderer obtains a bitmap to be sent to the Browser Kernel, so the Browser User can see it. Before doing this, the Controlled Process sends through its Proxy a Local Request to the Reference Monitor within the Browser Kernel.
- If the permissions are sufficient (Domain and Rights the Controlled Process has), the Reference Monitor lets the message with the bitmap go to the Browser Kernel.

Alternative flow

- The Provider is not available.
- The resource pointed by the URL does not exists.
- The request is cancelled.

Postconditions

The *Browser* receives the resource indicated by the URL and it is displayed by the peripheral device output for the Browser User.

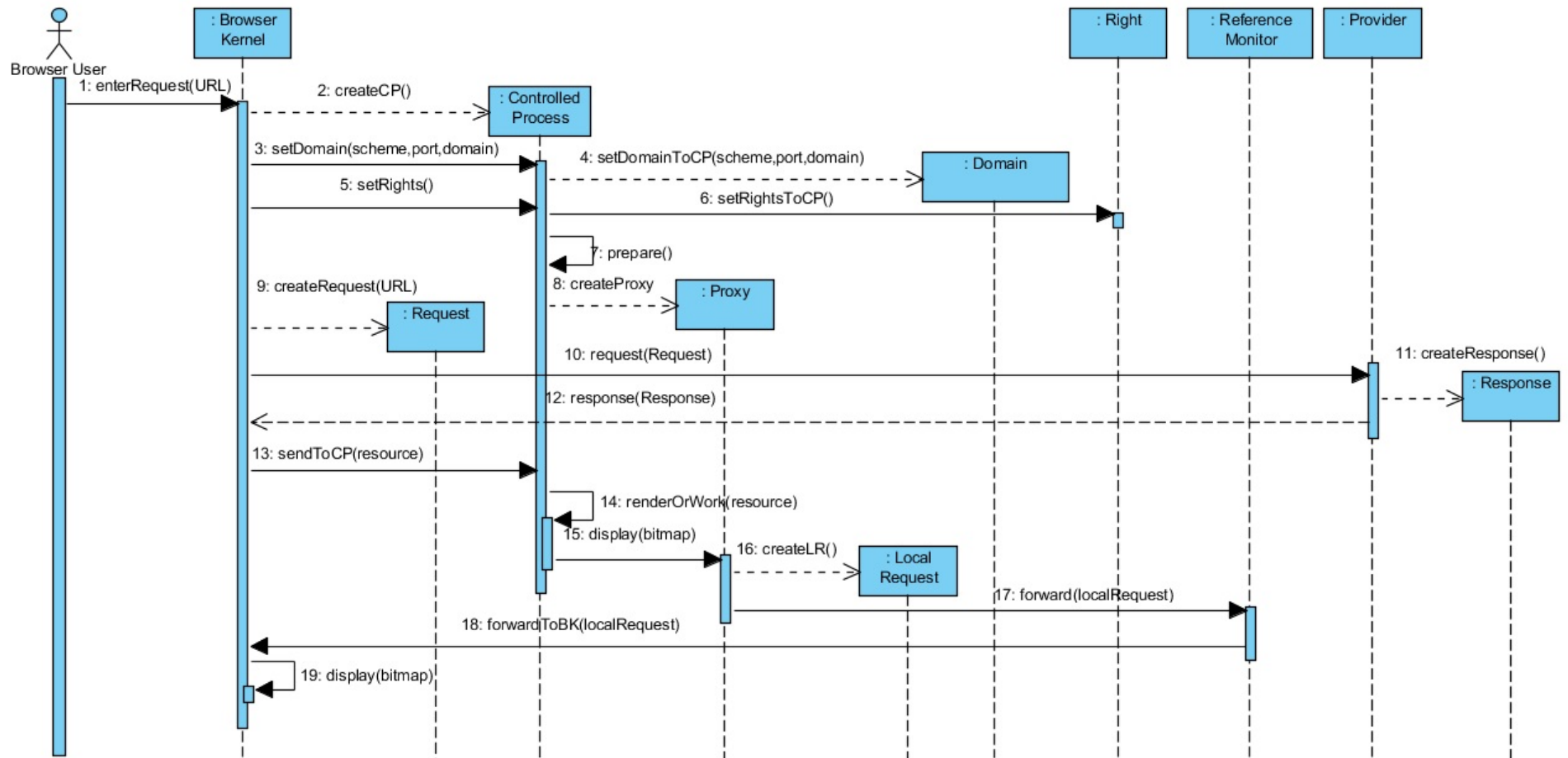


Figure 2: Sequence Diagram: Make Request.

Implementation

- While it is true that a **Browser Kernel** does not need sandboxing and only creates sandboxed processes or **Controlled Process**, the concept called **Sandbox** is defined here as in [5]; in which the **Browser Kernel** acts as the User that is related to the isolated process.
- The sandbox may be implemented in various ways. Google Chrome [8] is based on not reinventing the wheel and use the protection mechanisms provided by the OS (e.g, Windows or Linux) of the Host to protect the user. This prevents any process to access the file system, and having a restrictive API in the web Content Renderer. Google Chrome, Firefox and Internet Explorer affirm that Sandboxes are an important piece to the Browser because it realizes the principle of least privilege [9, 8, 10]. Some Operating Systems provide tools for creating Sandbox or in other cases a special library is used as Google Chromium. To create a Sandbox, the minimum configuration includes 2 processes: The privileged process or Broker represented by the Browser Kernel and the processes hosted in Sandboxes or Targets.
- To enforce the Same Origin Policy, Google Chrome, Firefox and Internet Explorer use different schemes; for example Google Chrome leaves pages/resources isolated with the help of the Renderer (Web Content Renderer in this case).
- The TLS protocol complements our pattern while giving security to the browser's communication channels.

Consequences

The Browser Infrastructure pattern provides the following benefits:

- **Transparency:** The user navigation is done almost automatically, only in rare cases the user will have to make a decision on the resource asked.
- **Stability:** Because the Browser Kernel, Sandbox, and GPU Plugin are independent Host processes, the failure of one will not generate problems in other (crash, memory corruption, etc.).
- **Isolation:** Depending on the type of isolation you can separate the different request, so they do not interfere with each other, unless it is desired.
- **Heterogeneity:** Because each Browser Kernel tries to follow the standards of the W3C [11], every page that follows these guidelines can be viewed, as well as other resources.

At the same time, this pattern has the following liabilities:

- Since independent processes are used to browse a resource (depending on the scheme using the browser), it is possible that a lot of the host's resources are used to keep everything open.
- Resources from Providers which do not comply the specifications of the W3C, will be displayed incorrectly by the Web Browser.

Example Resolved

With the given pattern it is now possible to navigate smoothly to all resources on the Internet we want. It is possible to provide through the isolation of the components: speed, security and stability. The Browser User will only concern about the navigation, unless it is required for its explicit permission to enter certain Host resources that are privileged (e.g, the file system). Each Host user can use the Browser Kernel they want, because each one is isolated by using separate processes.

Known Uses

- Currently, the separation of the components of the *Browser* in various processes, with different levels of access, is called as Modular Architecture [12]. This enables the separation of concerns in the browser, which gives greater stability, isolation, safety and speed.
- Google Chrome is based on the modular architecture, where each Renderer Process communicates with the Browser Kernel [13]. This proposal is used as a reference in the Mozilla project Electrolysis, as you can see in [14, 15], specially in the development of the sandbox and architecture.
- Internet Explorer, a proprietary browser, does not give much information about its structure or details of its implementation; [16] addresses Loosely-Coupled architecture [17] and its components, but without giving further details.
- Firefox, meanwhile has two implementations: mono-process and multiprocess/modular. Electrolysis is the name of the modular architecture being implemented, but it has not yet been fully completed.

Related Patterns

- The Web Content Renderer pattern, which is under development, represents the subsystem hosted by a Sandbox that allows the parsing of a resource obtained through a request.
- The Browser Kernel pattern, a pattern we are developing, represents the subsystem that represents the Web browser central component. This acts as a Reified Reference Monitor [5], which describes how to enforce authorization rights when a subject requests access to a protected object or service and returns a decision (response).
- The Sandbox is another name for the pattern Controlled Execution Domain [5].
- The TLS pattern in [5] complements our pattern, for adding security to communications between Client and Server.

Conclusions and Future Work

A Web browser appears to be a medium complexity software for users and developers without security experience, but unfortunately this piece of software allows a variety of attack vectors, to the user using it as well as the system with which interacts. Therefore it is important to understand its

structure and how it interacts with internal and/or external Stakeholders.

A part of our Reference Architecture has been built through the abstraction of documentation through the Browser Infrastructure pattern. We created our first architectural pattern for the infrastructure of *Web Browser* to help others understand, holistically, the components, interactions and relationships of this system. Furthermore, it has been possible to characterize the Stakeholders and one of the most important use case. From what we have known, this is the second Reference Architecture for the *Browser* built. The reference model obtained in [18] express the type of architecture used in the nineties until 2009 (approximately). However, our proposal represents the current implementation used in browsers, usually called a **Modular Architecture**. The proposed work allows a better understanding of this system called Web Browser by using our partially Reference Architecture, this is also helpful to understand existing threats. Also, as it is not subject to specific implementations, it is possible to generalize certain results in other browsers.

Future work to do is finishing the Reference Architecture for *Web Browsers*. Other patterns related to Browser Infrastructure pattern will be obtained in order to complete the Reference Architecture, such as the Web Content Renderer and Browser Kernel pattern.

We plan to build more Misuse Patterns for the Browser Infrastructure Pattern, to continue the study of the possible threats in the *Browser*, as a way to educate Developers and Stakeholders. At the same time, these patterns will allow the construction of the Security Reference Architecture for the browser. In the same line, in addition to finding potential threats existing in the system, we need to find countermeasures or security defenses to prevent or foresee such threats through security patterns on the reference architecture built. An example of the type of work to be carried out can be seen in [4].

1. REFERENCES

- [1] E. Gamma, R. Helm, R. Johnson, and J. Vlissides, *Design patterns: elements of reusable object-oriented software*. Pearson Education, 1994.
- [2] E. B. Fernandez, M. Larrondo-Petrie, T. Sorgente, and M. VanHilst, "A methodology to develop secure systems using patterns," *Chapter 5 in "Integrating security and software engineering: Advances and future vision"*, pp. 107–126, 2006.
- [3] E. B. Fernandez, N. Yoshioka, H. Washizaki, J. Jurjens, M. VanHilst, and G. Pernul, *Using Security Patterns to Develop Secure Systems*, H. Mouratidis, Ed. IGI Global, 2011. [Online]. Available: <http://www.igi-global.com/chapter/using-security-patterns-develop-secure/48405>
- [4] E. B. Fernandez, R. Monge, and K. Hashizume, "Building a security reference architecture for cloud systems," *Requirements Engineering*, Jan 2015. [Online]. Available: <http://link.springer.com/10.1007/s00766-014-0218-7>
- [5] E. B. Fernandez, *Security patterns in practice: designing secure architectures using software patterns*. John Wiley & Sons, 2013.
- [6] B. McCloskey, "Multiprocess Firefox." [Online]. Available: <https://billmccloskey.wordpress.com/2013/12/05/multiprocess-firefox/#ipc>
- [7] Google Chromium, "Inter-process Communication (IPC)." [Online]. Available: <https://www.chromium.org/developers/design-documents/inter-process-communication>
- [8] "Sandbox - The Chromium Projects." [Online]. Available: <http://www.chromium.org/developers/design-documents/sandbox>
- [9] M. V. Yason, "Diving into IE 10's Enhanced Protected Mode Sandbox."
- [10] "Security/Sandbox - MozillaWiki." [Online]. Available: <https://wiki.mozilla.org/Security/Sandbox>
- [11] World Wide Web Consortium - W3C, "About." [Online]. Available: <http://www.w3.org/Consortium/>
- [12] T. Vrbanc, "The evolution of web browser architecture," pp. 472–480, 2013.
- [13] "Multi-process Architecture - The Chromium Projects." [Online]. Available: <https://www.chromium.org/developers/design-documents/multi-process-architecture>
- [14] "Security/ProcessIsolation/ThreatModel." [Online]. Available: <https://wiki.mozilla.org/Security/ProcessIsolation/ThreatModel>
- [15] "Features/Security/Low rights Firefox - MozillaWiki." [Online]. Available: [https://wiki.mozilla.org/Features/Security/Low{ }rights{ }Firefox](https://wiki.mozilla.org/Features/Security/Low%7B%7Drights%7B%7DFirefox)
- [16] M. Crowley, *Pro Internet Explorer 8 & 9 Development: Developing Powerful Applications for The Next Generation of IE*, 1st ed. Berkely, CA, USA: Apress, 2010.
- [17] "IE8 and Loosely-Coupled IE (LCIE) - IEBlog - Site Home." [Online]. Available: <http://blogs.msdn.com/b/ie/archive/2008/03/11/ie8-and-loosely-coupled-ie-lcie.aspx>
- [18] A. Grosskurth and M. W. Godfrey, "A reference architecture for web browsers," 2005, pp. 661–664.