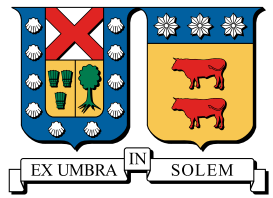
Hacia una unificación de Conceptos de Seguridad

Paulina Silva Ghio

Departamento de Informática - UTFSM

pasilva@alumnos.inf.utfsm.cl

24-11-2015.



UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Indice

Contexto

- La guerra de los Navegadores: construir y parchar.
- El navegador web: herramienta de uso cotidiano.
- El usuario común utiliza servicios.
- Distintos tipos, distintas implementaciones.
- Web 2.0 y 3.0: AJAX (Asynchronous Javascript and XML).

Browser en la Actualidad

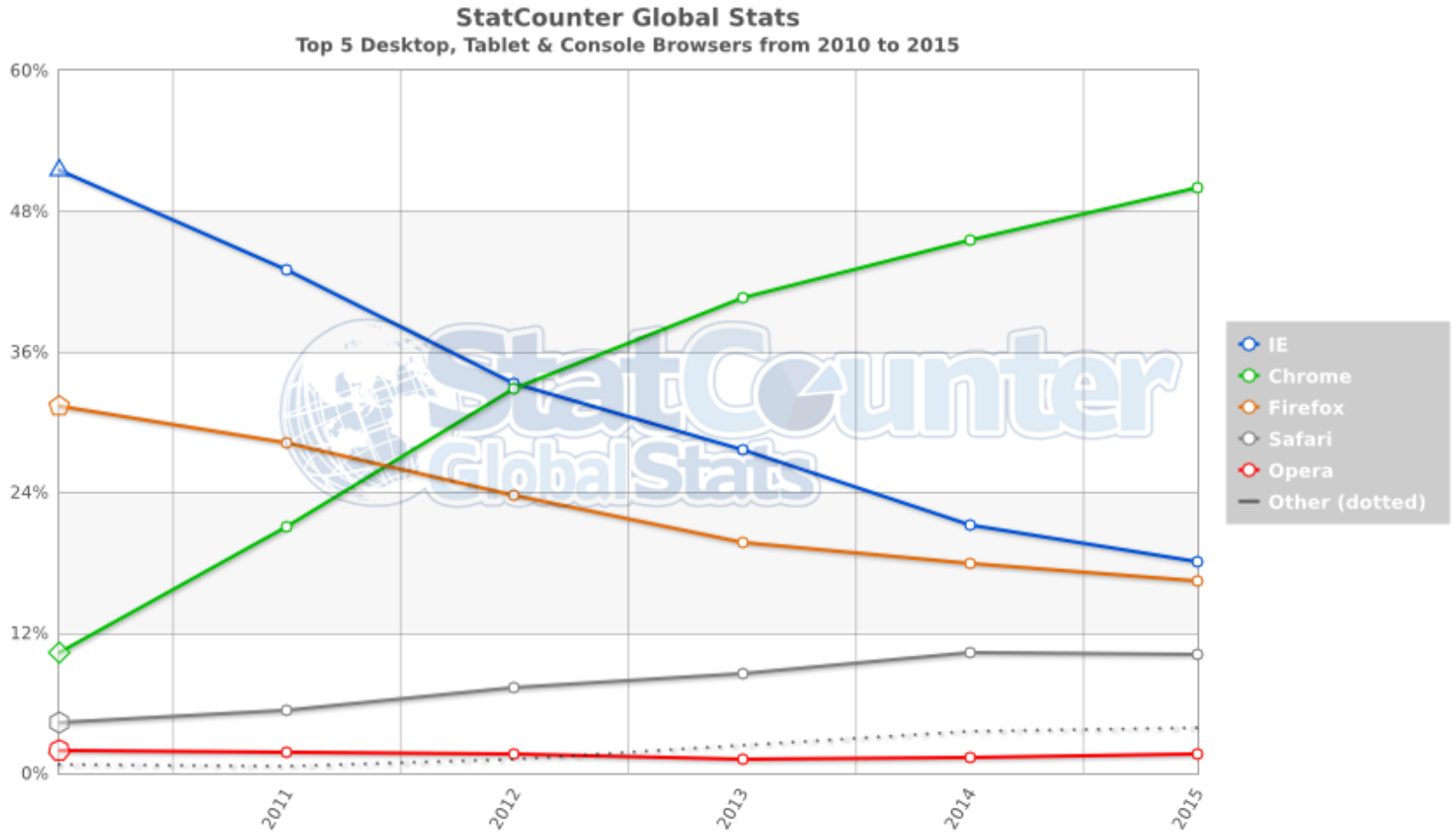


Figura: Porcentaje de uso de Navegadores. Fuente: [1]

Seguridad...

Desde la perspectiva de seguridad [2]:

- Qué realizan las universidades o la industria respecto a estas preocupaciones?
- Projectos de desarrollo de software, cuanto se le dedica a la seguridad?

Qué conceptos de seguridad sabe en promedio un estudiante graduado de carrera relacionada a Computer Science?

- La gente es autodidacta? o aprende por necesidad?
- La malla curricular es suficiente?
- La industria asegura que los sistemas a construir, sean seguros?

Desarrollo de Software y Seguridad

- Qué tanto se diferencian las preocupaciones del usuario común y el desarrollador que crea los sistemas?
- Cómo desarrollar software seguro?

Construcción de Software Seguro...

- Los que participan en la construcción: deben entender los problemas de seguridad.
- No basta saber como está construido.
- Considerar la Seguridad desde el inicio del Proyecto.
- Seguridad como una Propiedad Sistémica.

Motivación

- Nuevas formas de interactuar.
- Permite disminuir los costos de construir un programa Cliente (desde cero) para el usuario del sistema.
- Seguridad implementada que los Web Browser es bastante buena.
- El browser es una herramienta indispensable.

Las preocupaciones principales

- Los sistemas, a los que un usuario hace referencia, son llamados desde un Web Browser.
- El stakeholder afectado: el usuario del Browser, el Host del usuario y hasta el Servicio externo usado.
- Falta de conocimientos de seguridad con respecto al Browser, podría afectar de forma directa el desarrollo de aplicaciones que lo utilizan.

Contribuciones

Objetivo General

- Generar un cuerpo organizado de información sobre el Web Browser y su seguridad, de tal manera que se pueda sistematizar, organizar y clasificar el conocimiento adquirido en un documento, con formato semi-formal, tanto para Profesionales como Estudiantes del área Informática que estén insertos en el área de Desarrollo de Software.

Contribuciones

Objetivos Específicos

- Comprender los conceptos relacionados al navegador web, sus componentes, interacciones o formas de comunicación, amenazas y ataques a los que puede estar sometido, como también los mecanismos de defensa. Esto se realizará a través del desarrollo de un Estado del Arte sobre el Browser.
- Identificar actores, componentes, funciones, relaciones, requerimientos y restricciones del navegador, para lograr abstraer una Arquitectura de Referencia (AR) a partir de documentación disponible en Internet, blogs de desarrolladores, papers e iniciar un pequeo catálogo de Patrones de Mal Uso. Esto permitirá condensar el conocimiento obtenido en el punto anterior a través de documentos semi-formales, lo que permitirá generar una guía para comunicar los conceptos relevantes que pudieran afectar la relación existente entre un desarrollo de software y el navegador.
- Profundizar el conocimiento en ataques relacionados con métodos de Ingeniería Social

Marco Teórico de un Browser

- Arquitectura cliente/servidor
- Comunicación e Información de estado: HTTP y canales.
- SSL/TLS
- HTML5 y XML (Markup Languages)
- CSS
- DOM
- Javascript (ECMAScript)
- Geolocalización, WebWorkers y otros...

Desafíos del navegador

- Contenido y compatibilidad
- Navegación personalizada
- Navegación sin inconvenientes
- Seguridad

Arquitectura de Referencia (AR) y Patrones de Mal Uso

AR

- Especifica la decomposición del sistema en subsistemas, las interacciones entre estas partes y la distribución de funcionalidad entre ellas.
- Capturar la esencia de la arquitectura a través de una colección de sistemas similares, por medio del reuso arquitectónico
- Ayudar a los implementors o desarrolladores del software, a entender los trade-off cuando se disean nuevos sistemas
- Ayudar a los mantenedores de estos sistemas a entender el código legacy usado.
- Comparar las diferencias en decisiones de diseo y poder entender los cambios realizados a lo largo del Desarrollo de un sistema.
- Mirada holística del Sistema.

Patrones del Mal Uso

- Permitirán ensear y comunicar las posibles formas en que tal sistema puede ser usado inapropiadamente.

Arquitectura de Referencia (AR)

- Describir los Stakeholders que interactuan con el sistema y que poseen preocu paciones/concerns de éste.
- Patrones de Arquitectura.
- Atributos de calidad deseables que el sistema debe garantizar. Es importante solo destacar aquellos realmente necesarios, dado que un sistema sobrecargado con ellos tampoco es conveniente.

Ventajas

- Comprender la estructura subyacente de un Web Browser y las interacciones que tendrá con otros sistemas.
- Proveer una base tecnológica modular y flexible. Al tener los subsistemas compartimentalizados es posible quitar y sacar piezas, que poseen interfaces similares, y de esa manera reusar lo otro sin tener que construir un sistema nuevo.
- Entrega una base para el desarrollo de otros Navegadores Web, sin explicar detalles de implementación.

Ataques y Amenazas

- Social Engineering Attacks o Ataques de Ingeniería Social: Phishing
- Instalación de Malware o extensiones malignas
- Extensiones Vulnerables
- Ejecución de código Javascript
- XSS-DOM
- Man-in-the-Browser

Ataques y Amenazas

- SOP o Same Origin Policy
- CORS o Cross-Origin Resource Sharing
- HTTP Fields o Campos HTTP
- Sandboxing: Google Chrome/Chromium e Internet Explorer
- Aislación de Contenido
- Blacklist y Whitelist
- Sistema de Reputación
- Actualizaciones periódicas en background

Estado del Arte

- No se encontró información actualizada sobre una Arquitectura de Referencia del Browser. Hay una [3], pero es muy antigua.
- Poca documentación y no hay conceptos unificados.

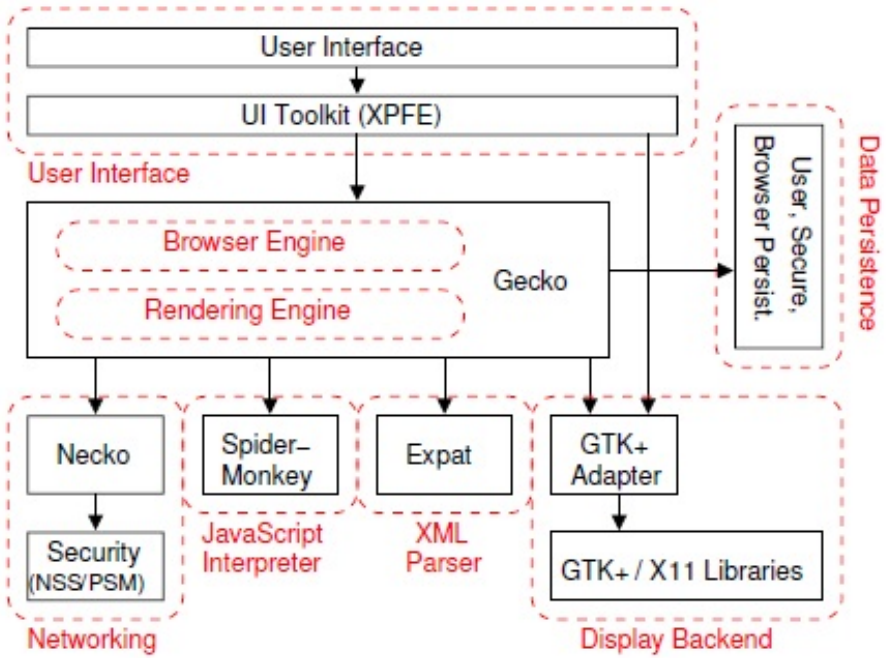


Figura: Arquitectura de Browser monoproceso. Fuente: [3]

Google Chrome y Chromium

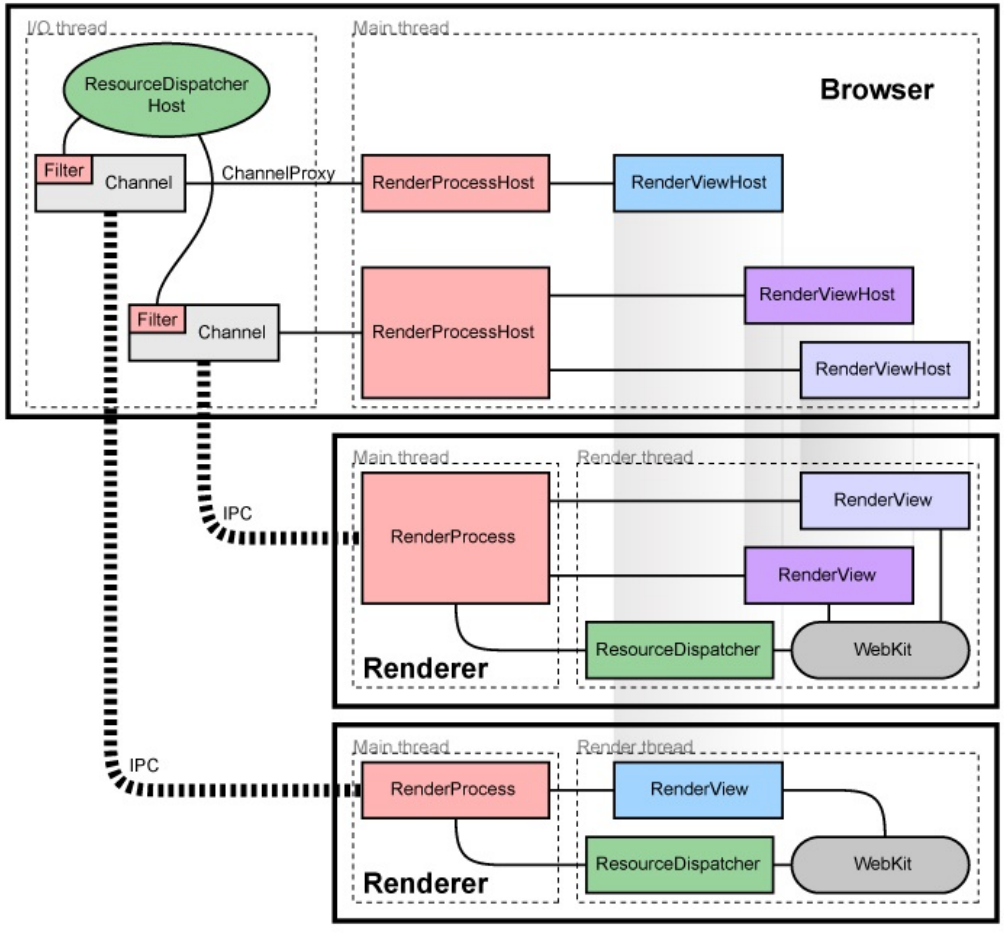


Figura: Architectura Multiprocesos de Google Chrome. Fuente: [4]

Google Chrome y Chromium

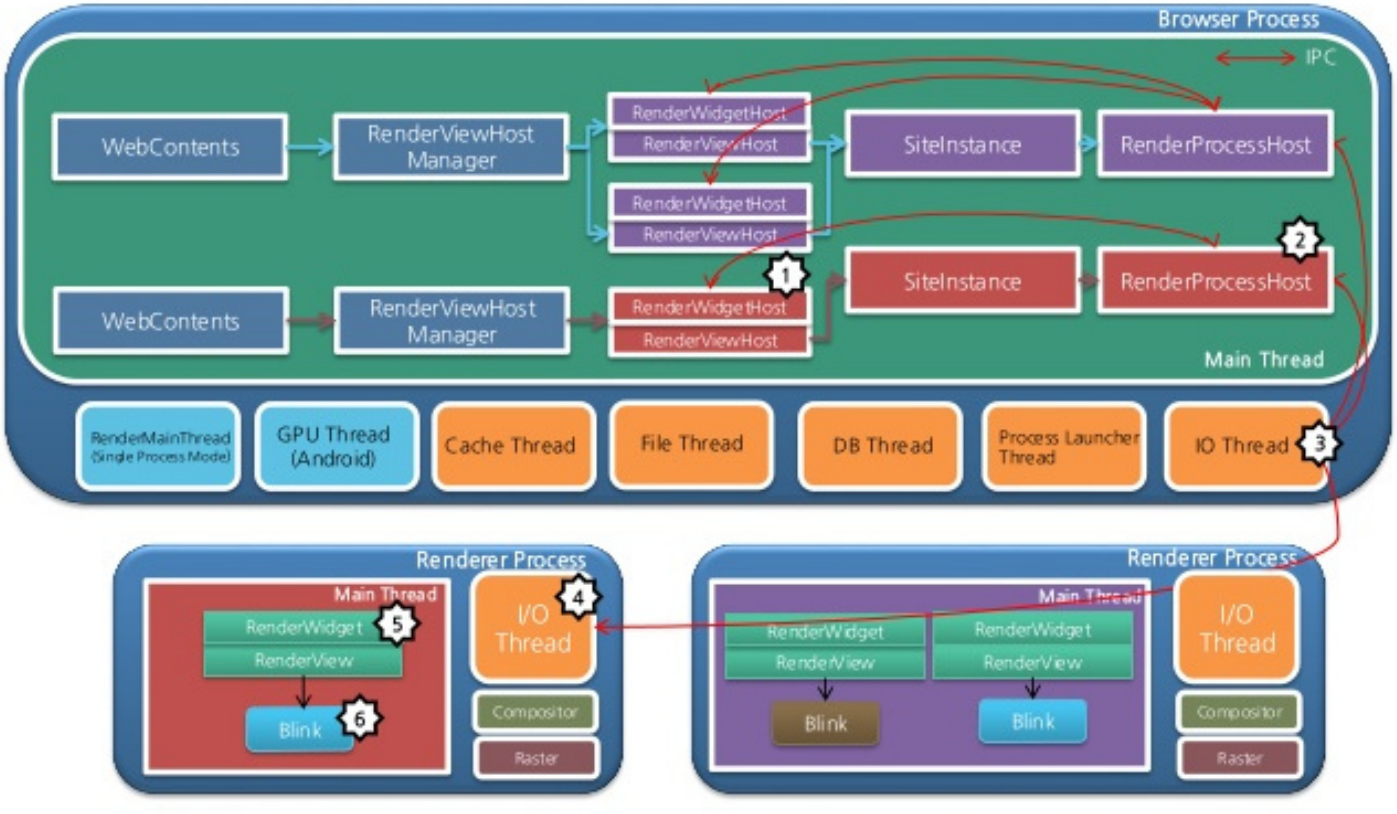


Figura: Architectura de Chromium en detalle. Fuente: [5]

Internet Explorer

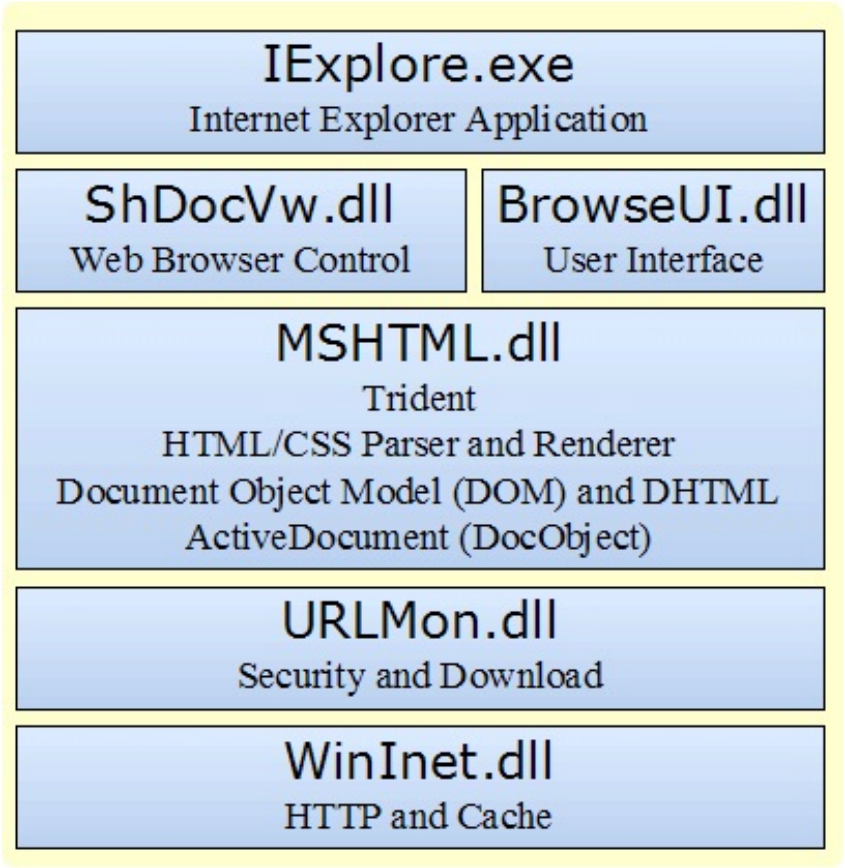


Figura: Arquitectura de Internet Explorer. Fuente: [6]

Internet Explorer

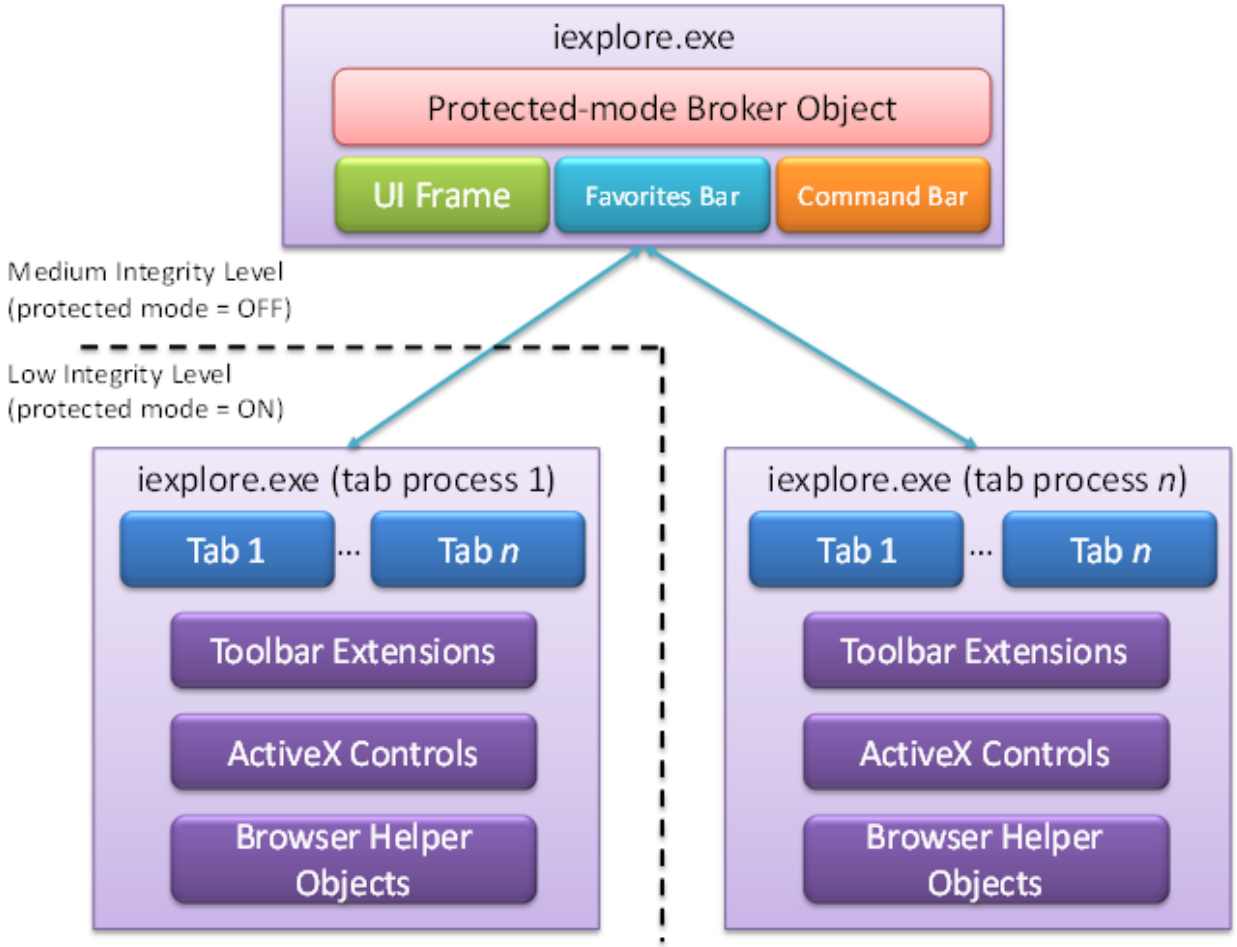


Figura: Arquitectura de Internet Explorer más detallada. Fuente: [7]

Firefox - Electrolysis

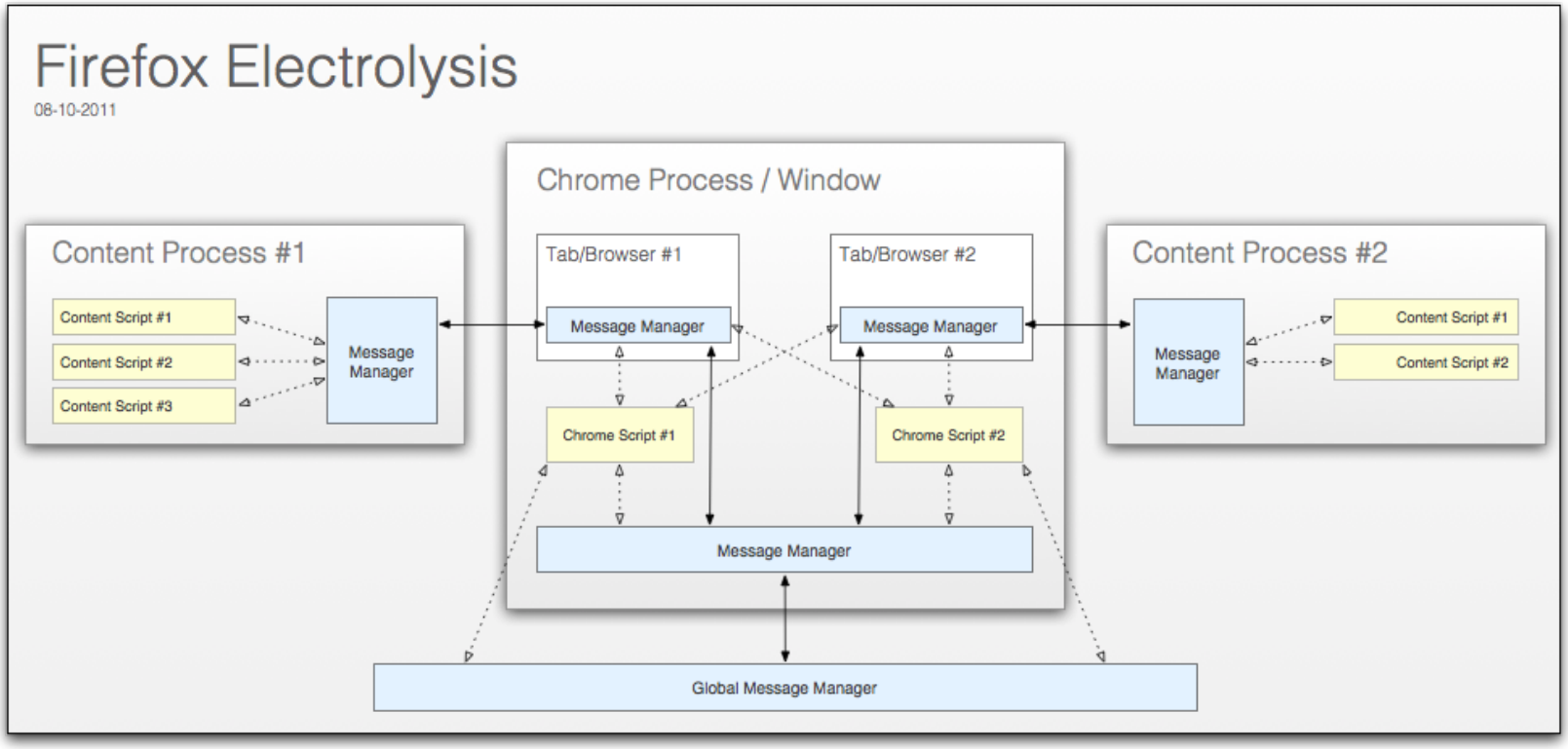


Figura: Firefox Electrolysis, Comunicación de procesos 1. Fuente: [8]

Firefox - Electrolysis

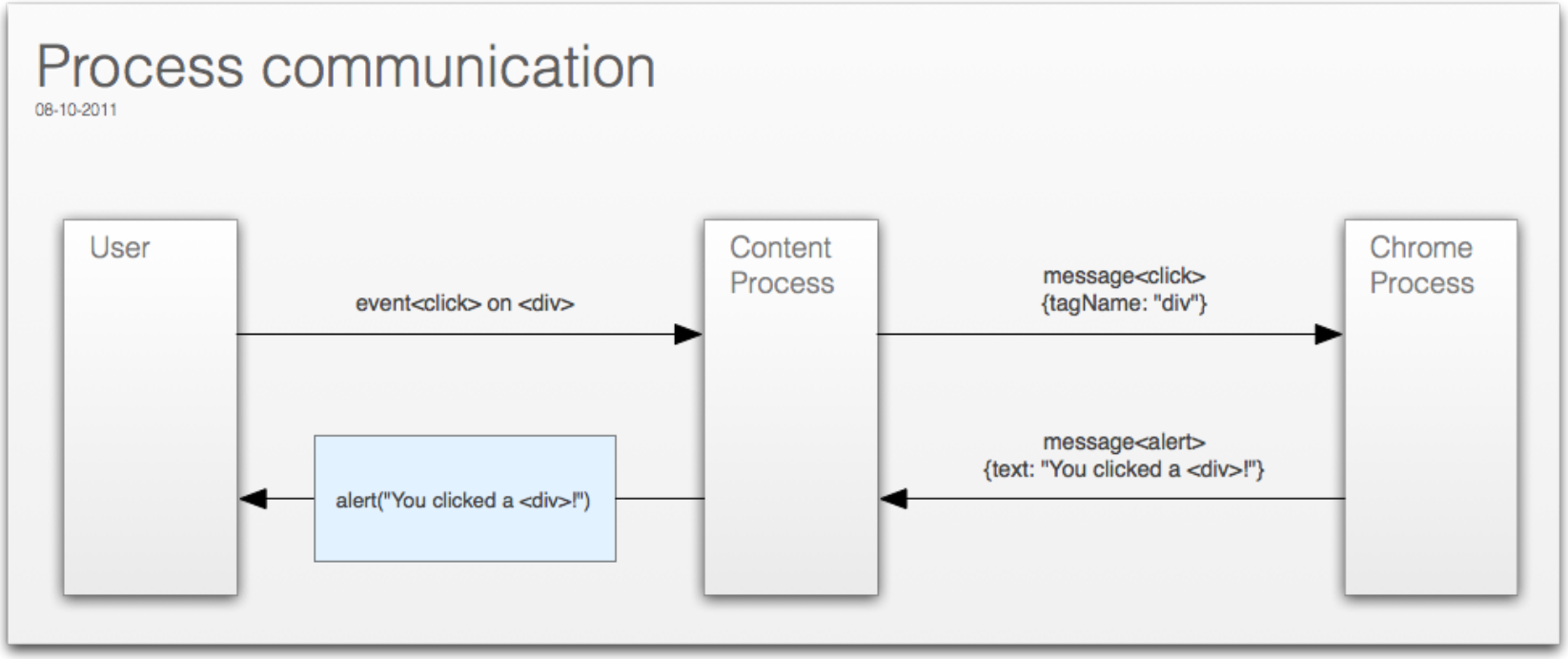


Figura: Firefox Electrolysis, Comunicación de procesos 2. Fuente: [8]

Casos de Uso

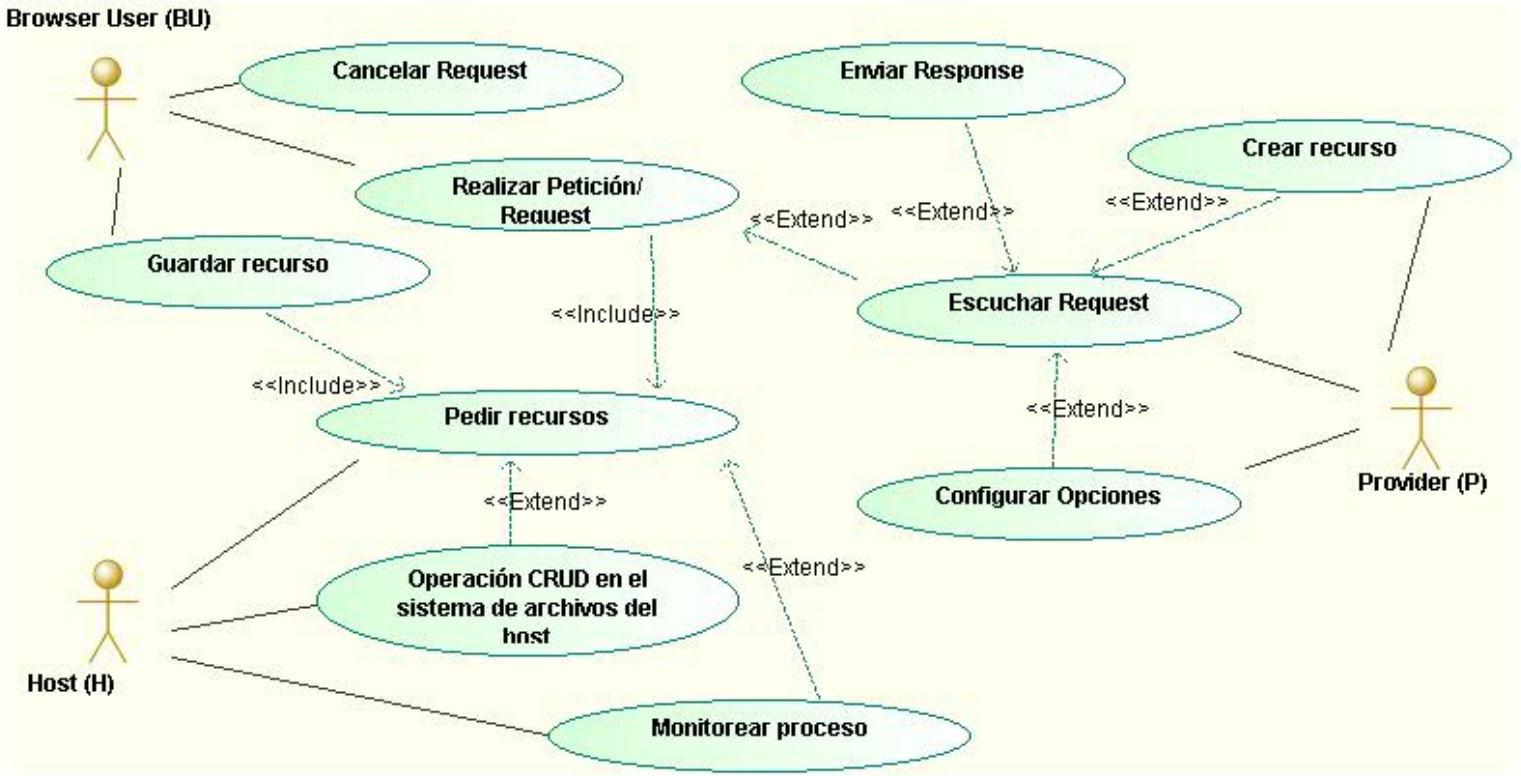


Figura: Diagrama de Caso de Uso del *Web Browser*.

Patrn Browser Infrastructure

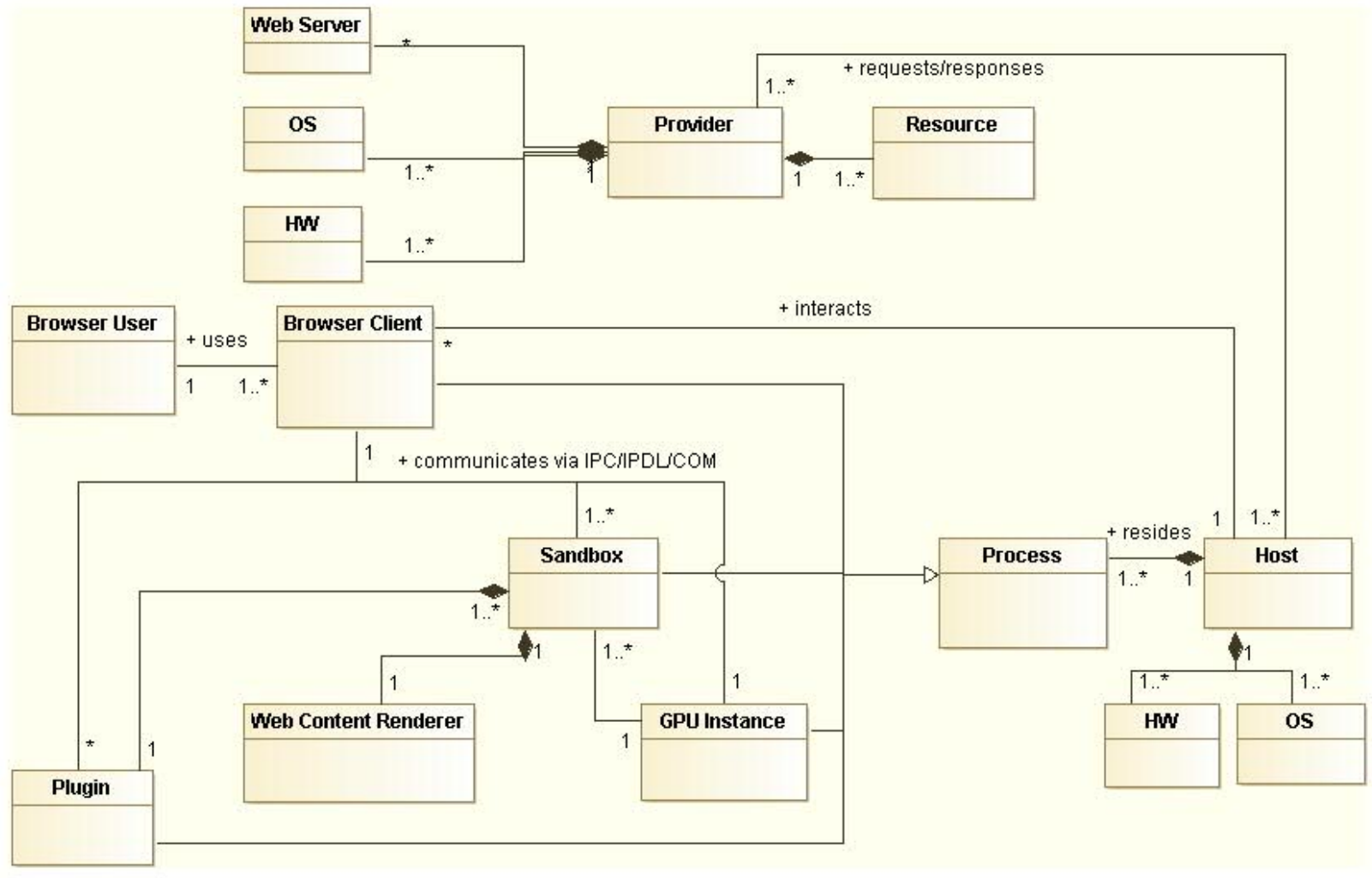


Figura: Componentes de alto nivel del *Browser*.

Dinmica: Realizar Request

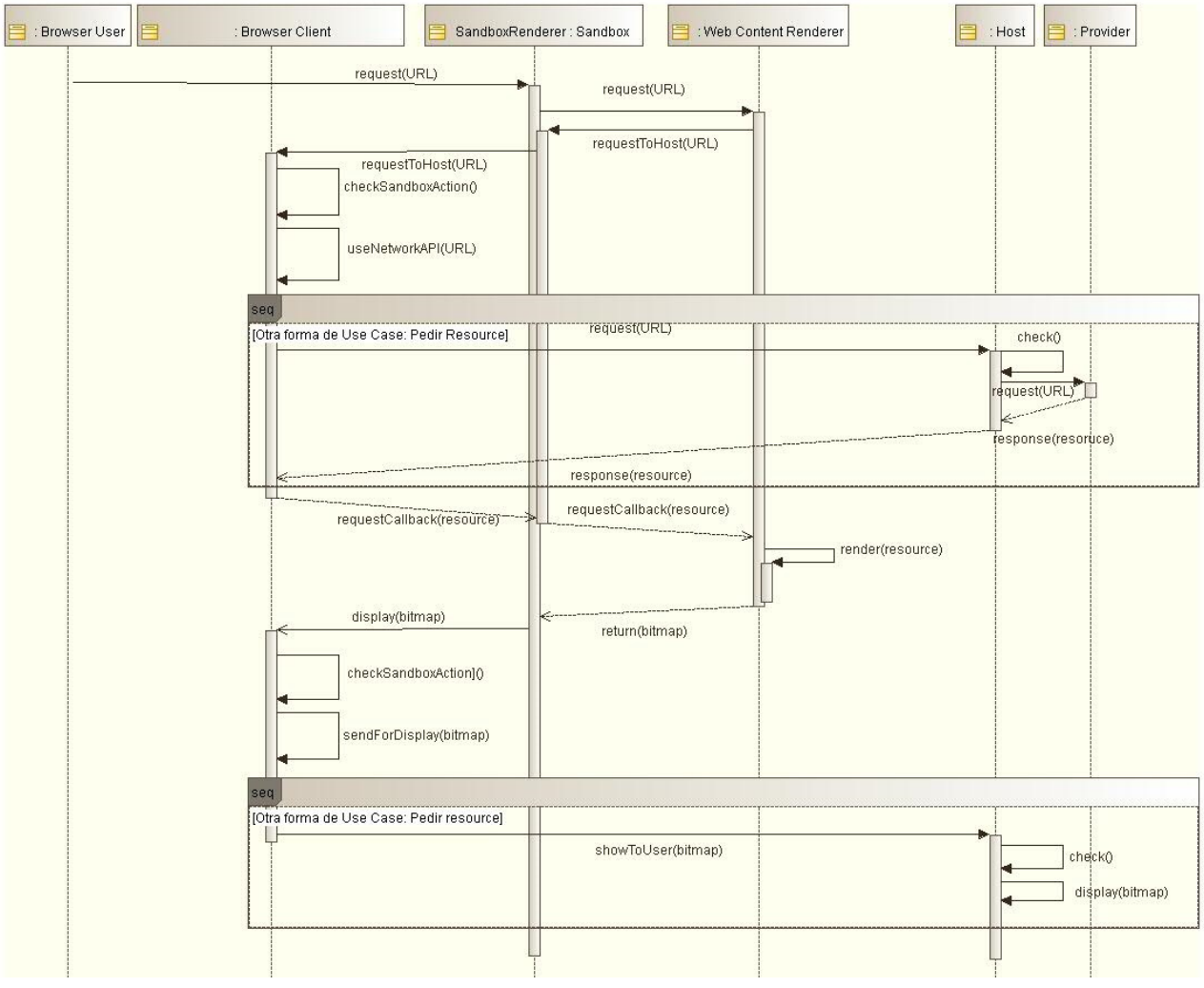


Figura: Diagrama de Secuencia: Realizar Request.

Diagrama de Actividad

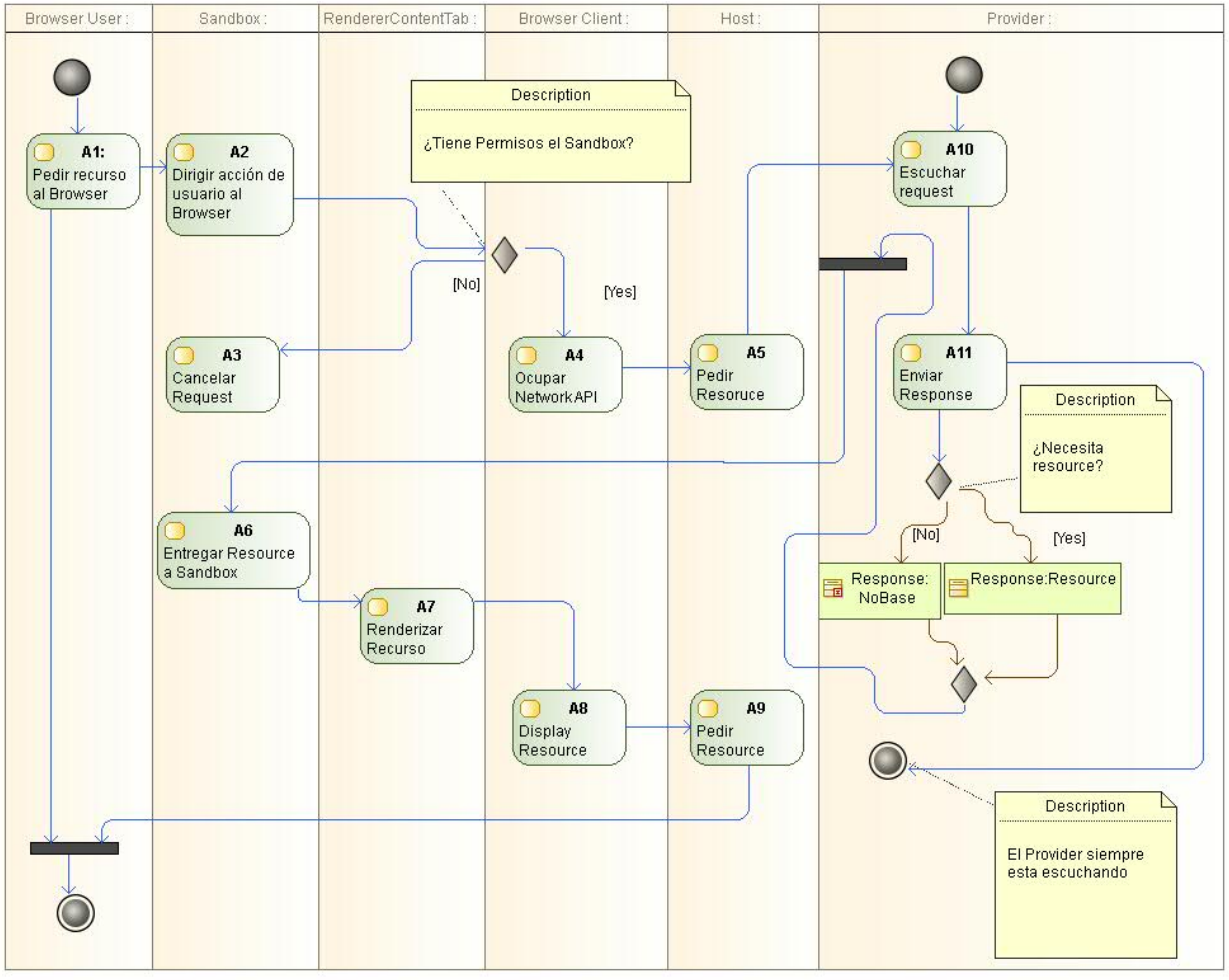


Figura: Diagrama de Actividad Compuesto para los casos de uso **Realizar Request** y **Recibir Request**.

Diagrama de Clases para el patrn de Mal Uso.

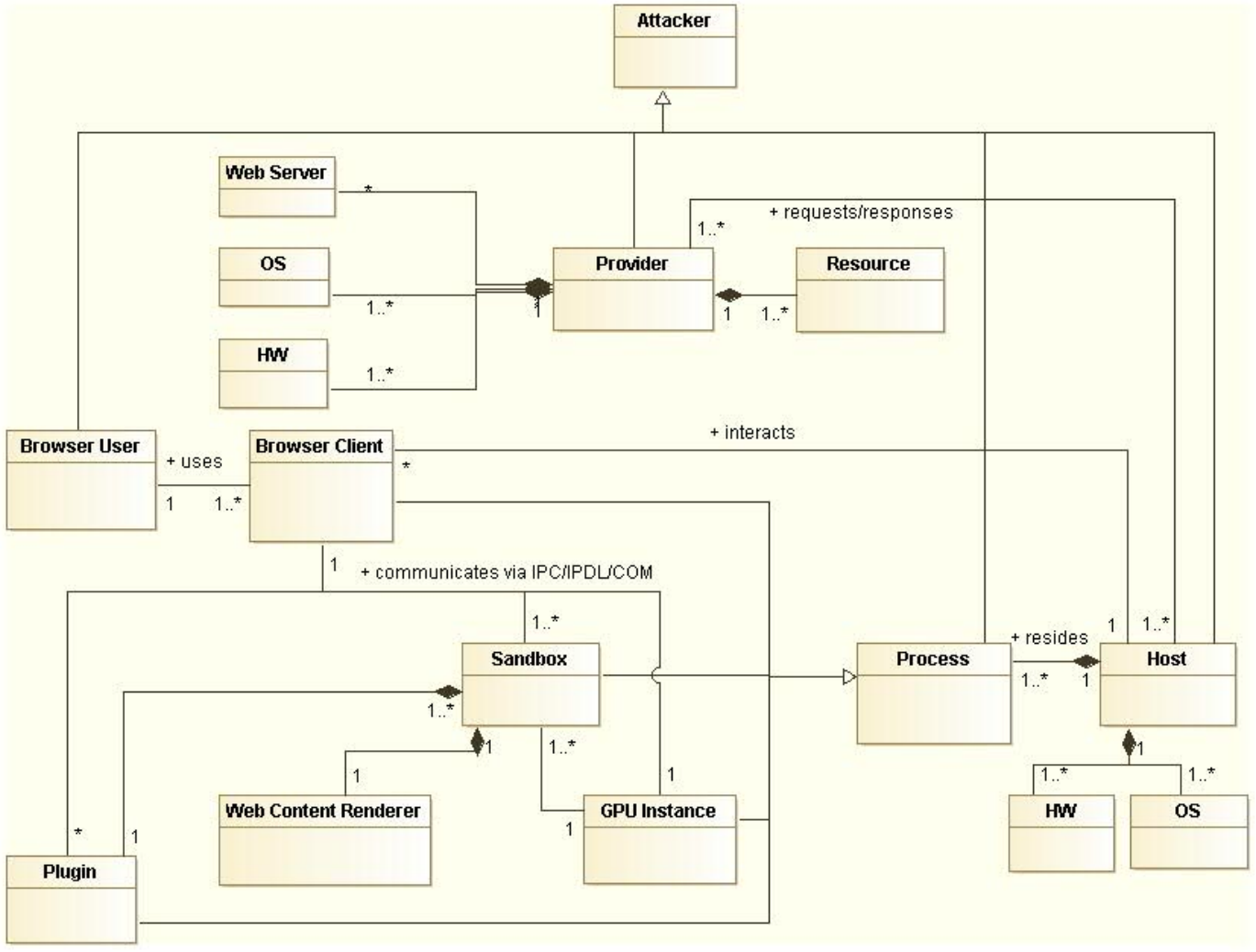


Figura: Diagrama de Clases para el patrn de Misuse.

Diagrama de Clases para el patrn de Mal Uso.

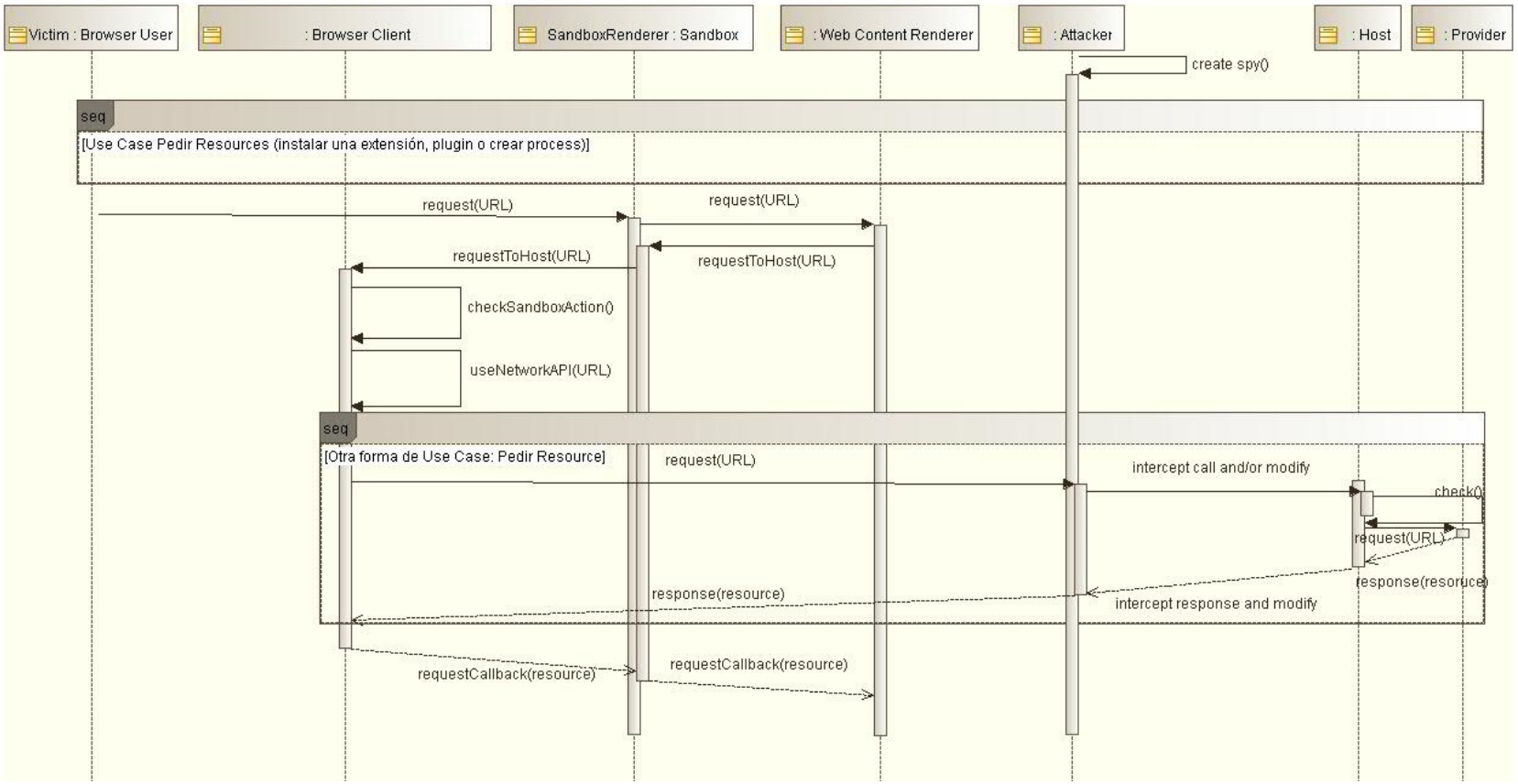


Figura: Diagrama de Secuencia para el Mal uso: Modificacin de trfico en el *Web Browser*.

Conclusiones


G. S. StatCounter, "Top 5 desktop, tablet and console browsers," 2015. [Online]. Available: http://gs.statcounter.com/


B. Whyte and J. Harrison, "State of Practice in Secure Software: Experts Views on Best Ways Ahead." IGI Global. [Online]. Available: http://www.igi-global.com/chapter/state-practice-secure-software/48404


A. Grosskurth and M. W. Godfrey, "Architecture and evolution of the modern web browser," uRL: `http://grosskurth.ca/papers.html#browser-archevol`. Note: submitted for publication.


"Multi-process Architecture - The Chromium Projects." [Online]. Available: https://www.chromium.org/developers/design-documents/multi-process-architecture


"Chromium Rendering Pipeline." [Online]. Available: http://www.slideshare.net/HyungwookLee/android-chromium-rendering-pipeline


"Internet Explorer Architecture (Internet Explorer)." [Online]. Available: https://msdn.microsoft.com/en-us/library/aa741312(v=vs.85).aspx


"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


"Firefox Electrolysis 101." [Online]. Available: https://timtaubert.de/blog/2011/08/firefox-electrolysis-101/