

## Presentación de Seminario de Tesis

pasilva@alumnos.inf.utfsm.cl

15-01-2016.



UNIVERSIDAD TECNICA  
FEDERICO SANTA MARIA

# Indice

- ➊ Introducción
  - Contexto
  - Seguridad...
  - Desarrollo de Software y Seguridad
  - Motivación para estudiar el Browser
  - Contribuciones
- ➋ Marco Teórico de un Browser
- ➌ Estado del Arte
  - Google Chrome y Chromium
  - Internet Explorer
  - Firefox - Electrolysis
- ➍ Metodología
- ➎ Plan de Trabajo
- ➏ Trabajo Adelantado
- ➐ Conclusiones

# 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

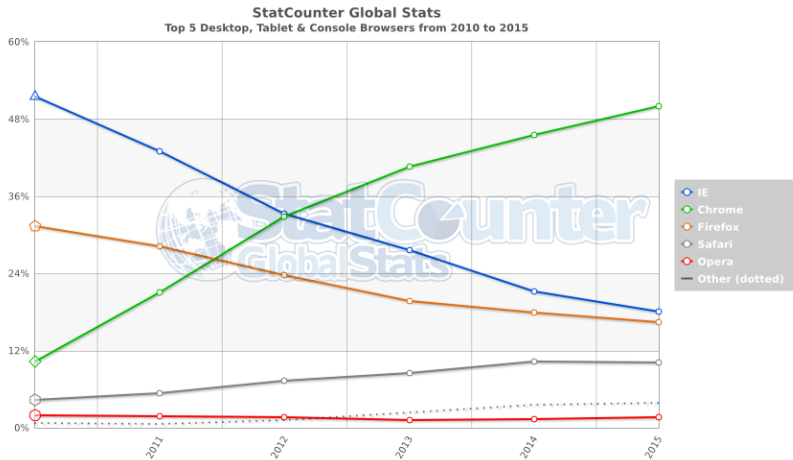


Figura: Porcentaje de uso de Navegadores. Fuente: [1]

# El Problema...

- Sistemas actuales son muy complejos.
- Es necesario utilizar metodologías que aseguren: Requerimientos Funcionales y No-Funcionales.
- Defectos y errores en el Software generan vulnerabilidades.
- La Seguridad es un costo “extra”, a veces no considerado.

## Las vulnerabilidades...

Ocurren por que no se ha tomado en cuenta la seguridad en el desarrollo.

# Seguridad...

Desde la perspectiva de seguridad [2]:

- ¿Qué realizan las universidades o la industria?
- Proyectos de desarrollo de software, ¿cuanto se le dedica a la seguridad?
- ¿La industria asegura que los sistemas a construir, sean seguros?

¿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?

# 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 para estudiar el Browser

El browser es una herramienta indispensable, éste permite:

- Nuevas formas de interactuar.
- Disminuir los costos de construir un programa Cliente (desde cero) para el usuario del sistema.
- Seguridad (la que está implementada en los Web Browser es bastante buena).
- Es una herramienta indispensable, por lo tanto el reuso es lógico.

## Las preocupaciones principales

- Los sistemas, a los que un usuario hace referencia, son llamados desde un Web Browser.
- Los stakeholders afectados: 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 y Stakeholders.



# Contribuciones

## Objetivo General

- Generar un cuerpo organizado de información sobre el Web Browser y su seguridad.
- Sistematizar, organizar y clasificar el conocimiento adquirido en un documento, con formato semi-formal. Dado que hay conceptos poco claros y poca documentación formal.
- 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 pequeño catálogo de Patrones de Mal Uso.
- Condensar el conocimiento obtenido en el punto anterior a través de documentos semi-formales.
- 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)

- Describir los Stakeholders que interactúan con el sistema y que poseen preocupaciones/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.
- Actualmente no hay un consenso de cómo definir una AR, lo que debería contener y cómo debería de construirse.

### 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.

# Arquitectura de Referencia de Seguridad (ARS)

- asdf

## Ventajas

- asdf

# Estado del Arte

- No se encontró información actualizada sobre una Arquitectura de Referencia del Browser. Hay una [5], pero es muy antigua.
- Poca documentación y no hay conceptos unificados.
- Queda por buscar si existe algo parecido a una ARquitectura de Referencia de Seguridad del Browser.

# Google Chrome y Chromium

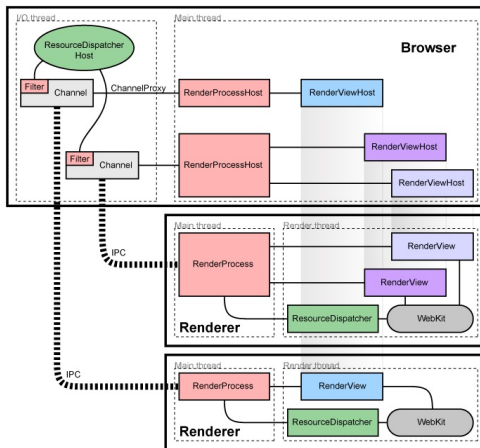
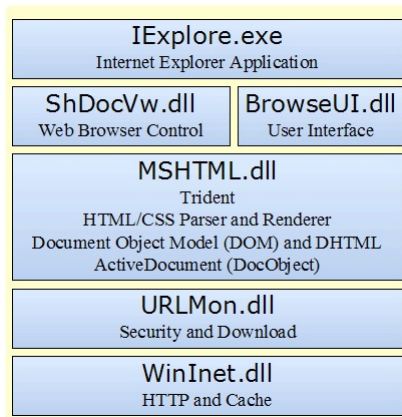


Figura: Arquitectura Multiprocesos de Google Chrome. Fuente: [6]



A set of small navigation icons typically found in Beamer presentations, including symbols for back, forward, search, and other slide controls.





# Internet Explorer

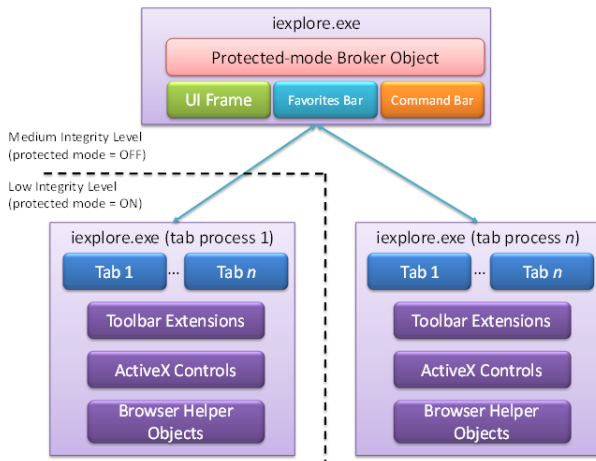


Figura: Arquitectura de Internet Explorer más detallada. Fuente: [9]

# Firefox - Electrolysis

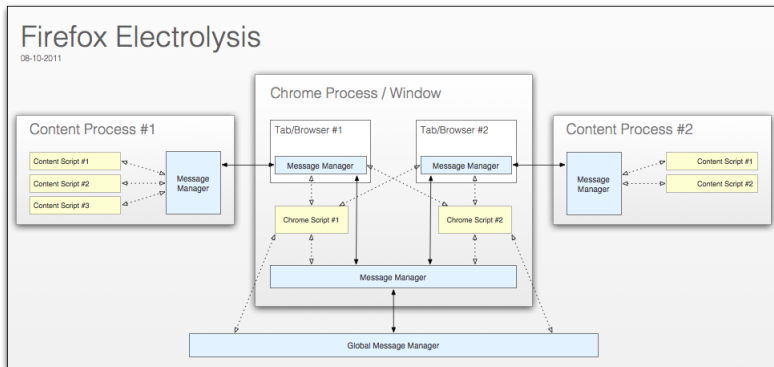


Figura: Firefox Electrolysis, Comunicación de procesos 1. Fuente: [10]

# Firefox - Electrolysis

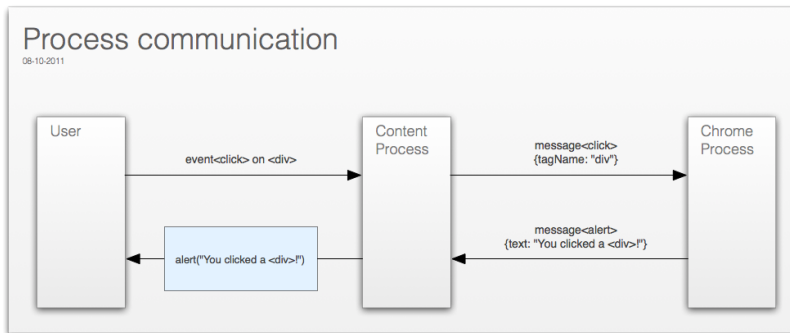


Figura: Firefox Electrolysis, Comunicación de procesos 2. Fuente: [10]

# Metodología

- Marco teórico y Estado del Arte: Revisión de conceptos relevantes del navegador, seguridad y Arquitecturas de Referencias existentes. Se examinarán artículos científicos, blogs o proyectos de investigación relacionados al tema.
- Evaluación de Resultados Intermedios: a) Envío de papers a Asian PLoP, b) Depurar el modelo obtenido en la memoria de pregrado.
- Agregar nuevos patrones y adecuar modelo para especificar semi-formalmente estos patrones. Creación de la Arquitectura de Referencia de Seguridad.
- Producir segunda versión de publicaciones: Se enviarán más trabajos a conferencias de tipo PLoP (Pattern Languages of Programs).
- Documentar la tesis a partir de la compilación de papers obtenidos y el trabajo adelantado.

### Plan de Trabajo

Actividad	Fecha
Marco teórico y Estado del Arte	Noviembre 2015 - Enero 2016
Evaluación de Resultados Intermedios	Noviembre 2015 - Febrero 2016
Agregar nuevos patrones y adecuar modelo	Enero - Abril 2016
Producir segunda versión de publicaciones	Enero - Abril 2016
Documentar la tesis	Enero - Abril 2016

Cuadro: Plan de Trabajo

# Trabajo Adelantado

- En la memoria de Pregrado se obtuvo un Estado del Arte sobre el Browser y documentación sobre Arquitecturas de Referencias existntes. Falta averiguar sobre Arquitecturas de Referencia de Seguridad.
- Se han enviado 2 papers a la conferencia AsianPLoP con lo obtenido en la memoria de pregrado. El proceso llamado “shepherding” permite evaluar el paper enviado, al mismo tiempo que provee al autor la mejora del trabajo a través del intercambio continuo de sugerencias entre el autor/autores con el “shepherd”.

# Conclusiones

asasas



# Contribuciones


- asadsd


# Resumen


- asasa

## ¿Preguntas?


¡Muchas Gracias!

 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>

 F. A. Braz, E. B. Fernandez, and M. VanHilst, “Eliciting security requirements through misuse activities,” in *Database and Expert Systems Application, 2008. DEXA’08. 19th International Workshop on*. IEEE, 2008, pp. 328–333.

 E. Fernandez-Buglioni, *Security patterns in practice: designing secure architectures using software patterns*. John Wiley & Sons, 2013.

 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](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/>