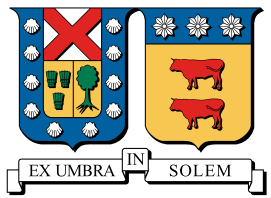
Presentación de Seminario de Tesis I
Hacia una Arquitectura de Referencia de Seguridad del Web Browser

Paulina Silva Ghio

pasilva@alumnos.inf.utfsm.cl

15-01-2016.



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).

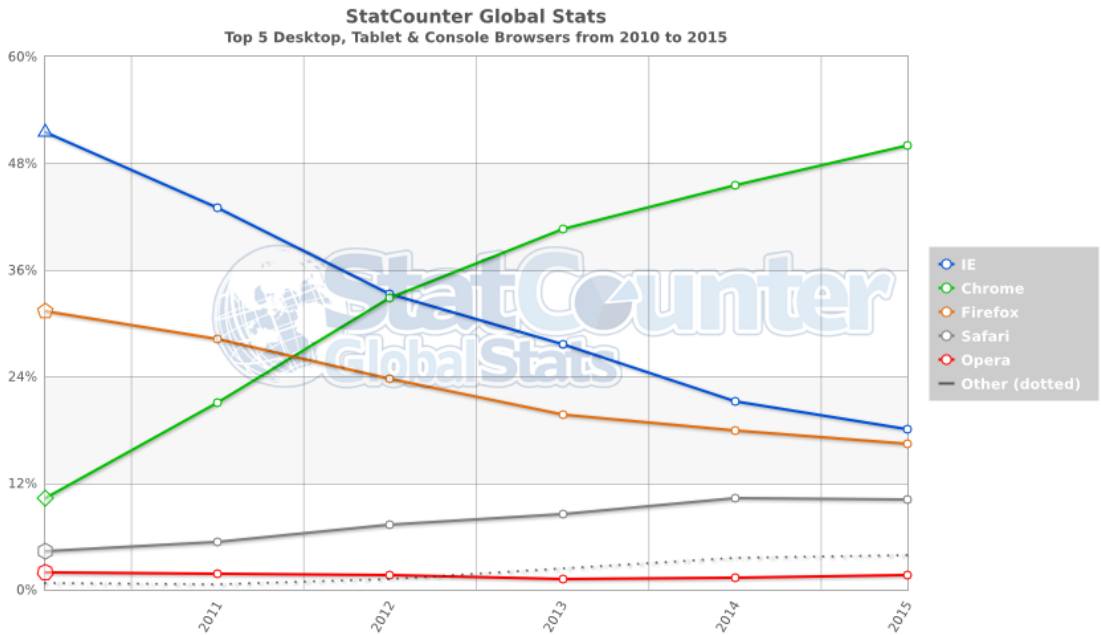


Figura: Porcentaje de uso de Navegadores. Fuente: [1]

Motivación para estudiar el Browser

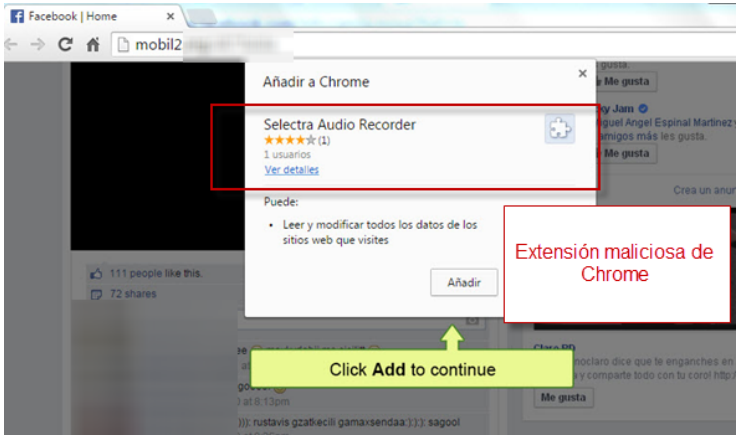
El browser es una herramienta indispensable, éste permite:

- 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.

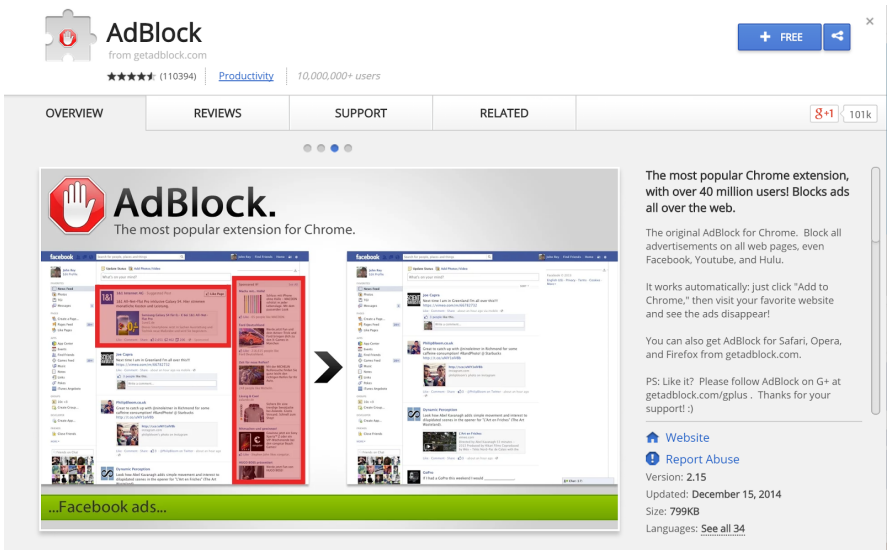
Las preocupaciones principales

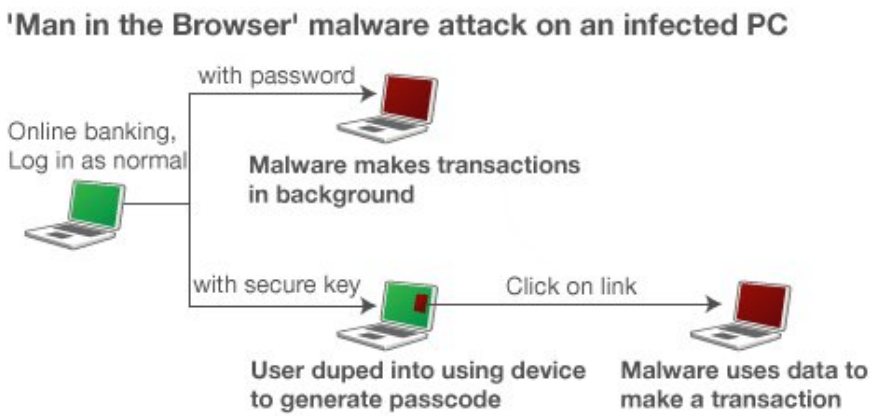
- Los sistemas, a los que un usuario hace referencia, son llamados desde un Web Browser.
- Los stakeholders afectados: el usuario del Browser, el Host del usuario y hasta el Servicio externo usado.

Amenazas y Vulnerabilidades



1. Instalación de Malware o extensiones maliciosas.
2. Extensiones Vulnerables.
3. Man in the Browser.





Problemas

- Falta de conocimientos de seguridad con respecto al Browser, podría afectar de forma directa el desarrollo de aplicaciones que lo utilizan y Stakeholders.
- Poca documentación y no hay conceptos unificados. No se ve que existan descripciones formales para los conceptos relacionados al browser.

Arquitectura de Referencia (AR) para el browser

- Actualmente no hay un consenso de cómo definir una AR, lo que debería contener y cómo debería de construirse. En este trabajo usaremos patrones arquitecturales para su construcción.
- Especifica la decomposición del sistema en subsistemas, las interacciones entre estas partes y la distribución de funcionalidad entre ellas.
- Describir los Stakeholders que interactuan con el sistema y que poseen preocupaciones/concerns de éste, así como los atributos de calidad deseables que el sistema debe garantizar.
- Capturar la esencia de la arquitectura a través de una colección de sistemas similares, por medio del reuso arquitectónico
- Ayuda: 1) a los implementores o desarrolladores del software, a entender los trade-off cuando se diseñan nuevos sistemas, 2) a los mantenedores de estos sistemas a entender el código legacy usado.
- Comparar las diferencias en decisiones de diseño y poder entender los cambios realizados a lo largo del Desarrollo de un sistema.
- Mirada holística del Sistema.

Desventajas

Incluso realizar los casos de uso más importantes del sistema toma tiempo.

Arquitectura de Referencia de Seguridad (ARS) para el browser

- Abtracción de los mecanismos de defensa en forma de patrones de seguridad
- Se enseña en que lugares de la Arquitectura de Referencia son necesitados.
- Una forma de entender y descomponener un sistema complejo con mecanismos de defensa que aumentan esa complejidad.
- Una vista holística de la seguridad, teniendo en cuenta las interacciones con otros sistemas que pueden generar vulnerabilidades.
- Unifica la terminología. Esto permite comparar diferentes implementaciones bajo las mismas definiciones de conceptos.
- Evaluación de la seguridad del browser
- Selección de un browser basado en los requerimientos de seguridad.
- Referencia para funciones de monitoreo y forense.

Desventajas

- Se necesita invertir mucho tiempo en la construcción, al menos de los componenentes más importantes.

Patrones del Mal Uso

- Describen desde el punto de vista del atacante, como un tipo de ataque es realizado (que unidades usa y cómo), analiza las formas de detener el ataque enumerando los posibles patrones de seguridad qu pueden ser utilizados, y describe como rastrear el ataque una vez ocurrido con la recolección y observación de datos forenses.
- Permitirán enseñar y comunicar las posibles formas en que tal sistema puede ser usado inapropiadamente.
- Normalmente explicado a traves de un diagrama de secuencia o colaboración: es posible relacionar los mensajes con los componentes que los reciben.

Estado del Arte

- No se encontró información actualizada sobre una Arquitectura de Referencia del Browser. Hay una [2], pero es muy antigua.
- Trabajos encontrados: Larrondo et al. [3], Grosskurth et al. [4, 2], Godfrey et al. [5], Lwin [6].
- Poca documentación y no hay conceptos unificados.
- Queda por buscar si existe algo parecido a una Arquitectura de Referencia de Seguridad del Browser.

Objetivo General y Específicos

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.
- Lograr una mejor comprensión sobre la seguridad en el web browser.

Objetivos Específicos

- Una guía para comunicar los conceptos relevantes que pudieran afectar la relación existente entre un desarrollo de software y el navegador.
- Mejorar la Arquitectura de Referencia (AR) obtenida en la memoria de Pregrado para agregar más patrones a ésta y continuar el catálogo de Patrones de Mal Uso.
- Construir un modelo conceptual de la seguridad del web browser a través de una Arquitectura de Referencia de Seguridad, identificando patrones de seguridad en el navegador.
- Profundizar el conocimiento en ataques relacionados con métodos de Ingeniería Social.
- Utilizar técnicas de Ingeniería de Software Experimental.

Hipótesis

Hipótesis Principal

H1: La definición de una Arquitectura de Referencia de Seguridad para web browsers permite abstraer y capturar los principales aspectos estructurales y de comportamiento de éstos, facilitando la expresión de los patrones más conocidos de mal uso y seguridad relacionados con los navegadores.

Formas de Validación

- Las Arquitecturas de Referencias (AR/RA) y Arquitecturas de Referencias de Seguridad (ARS/SRA) no son implementables. Éstos son modelos abstractos y no pueden ser evaluados con respecto a la seguridad o desempeño por medio de testing o experimentación.
- La validación de los artefactos generados en este trabajo será a través de la revisión realizada por expertos en el área de computer science y patrones, por medio de la asistencia de conferencias.
- Al ser aceptados, presentados, mejorados y publicados en conferencias *PLoP, tendremos un respaldo de la utilidad de estos patrones. Los patrones antes de ser publicados, son refinados a través del proceso llamado “Shepherding”. Para esta tesis se espera ir a las conferencias: AsianPLoP y EuroPLoP.
- Se utilizarán conocimientos en ingeniería de software experimental para probar nuestra hipótesis.

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".

Metodología y Plan de Trabajo

- Marco teórico y Estado del Arte: Revisión de conceptos relevantes del navegador, seguridad y Arquitecturas de Referencias existentes.
- 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), la siguiente más próxima es el EuroPLoP.
- Documentar la tesis a partir de la compilación de papers obtenidos y el trabajo adelantado.

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 - Mayo 2016
Documentar la tesis	Enero - Mayo 2016

Cuadro: Plan de Trabajo

Aportes y Resultados Esperados

- Se espera poder obtener una documentación semi-formal que permita comprender mejor la seguridad y estructura del browser. Para así entender que éste tiene una superficie de ataque muy usada por los atacantes de los sistemas con los que se conecta el usuario, utilizando frecuentemente ataques de ingeniería social.
- Crear un catálogo de patrones de mal uso que permitan instruir a personas en el área de IT pero carecen de conocimientos de seguridad, sobre los tipos de ataques existentes.
- Arquitecturas de Referencia (AR) de su infraestructura como de los mecanismos de defensa existentes (ARS). Incluyendo 2 nuevos patrones arquitecturales: el Browser Kernel y el Web Content Renderer. Patrones de Seguridad existentes o nuevos y aún no documentados.
- Experimentación del modelo utilizando técnicas de ingeniería de software experimental.

¿Preguntas?

¡Muchas Gracias!


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


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.


M. Larrondo-Petrie, K. Nair, and G. Raghavan, "A domain analysis of web browser architectures, languages and features," in *Southcon/96. Conference Record*, Jun 1996, pp. 168–174.


A. Grosskurth and M. W. Godfrey, "A reference architecture for web browsers," 2005, pp. 661–664, uRL: `http://grosskurth.ca/papers.html#browser-refarch`.


M. W. Godfrey and E. H. S. Lee, "Secrets from the Monster: Extracting Mozilla's Software Architecture," *In Proc. of 2000 Intl. Symposium on Constructing software engineering tools (CoSET 2000*, pp. 15–23, 2000. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.42.9211


A. Systems and N. Lwin, "Agent Based Web Browser," *2009 Fifth International Conference on Autonomic and Autonomous Systems*, 2009.