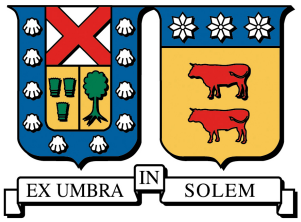
Universidad Técnica Federico Santa María
Departamento de Informática
Valparaíso, Chile



Estado del Arte: Web browsers bajo ataques y sus mecanismos de Seguridad.

Paulina Andrea Silva Ghio

Memoria para obtar al título de: Ingeniera Civil Informática

Profesor Guía: Raúl Monges
Profesor Correferente: Javier Cañas

24 de marzo de 2015

Resumen

El uso del Internet en la vida cotidiana ya es parte de la mayoría del mundo. Para cada necesidad de información el usuario puede buscar en Internet aquello que lo aqueja, desde comprar tickets para una película, realizar reuniones por videoconferencia y muchas otras tareas que en el pasado no eran necesarias, pero que hoy en día su uso es imperante; como las redes sociales. La Web 2.0 ha sido gran colaboradora de éste éxito en la vida de las personas, entregando las herramientas para que los contenidos que los usuarios necesiten estén disponibles de diversas formas y en tiempo real.

Junto con éste desarrollo en la forma de interactuar con la Internet, parte de la responsabilidad de que existan la tienen los desarrolladores que crean Software de acuerdo a los requerimientos de sus clientes. Dentro de las necesidades de los clientes, algunos equipos de Desarrollo de Software tienen casi siempre en cuenta ciertos requerimientos no funcionales que permiten conservar ciertos atributos en el Sistema a crear, como: Confidencialidad, Integridad, No Repudio y Disponibilidad. Sin embargo, muchas veces por los costos y poco tiempo que poseen, los atributos mencionados no son salvaguardados. En consecuencia el producto final, podría llegar a tener serias consecuencias tanto en el Cliente como en los Usuarios que podrían llegar a usar el Sistema.

El Objetivo de esta Memoria es concretar un Estado del Arte que analice el funcionamiento y estructura (componentes) del Web Browser, e investigar los peligros en que se puede encontrar un usuario al usar la aplicación *killer*[1]. Además se desea construir una Arquitectura de Referencia que permita comprender los componentes que interactúan en el browser y desarrollar patrones de mal uso de estos artefactos; mencionando los componentes utilizados para que los ataques se lleven a cabo. Finalmente se desea clasificar los riesgos y mecanismos de defensa (mitigación) de los navegadores Web, para poder obtener un panorama general de cómo los Web Browser protegen al usuario.

Abstract

[1] Web Browsers

Índice

1. **Motivación: ¿Por que estudiar el Browser?**
2. **Contribuciones**
3. **Estructura del Documento**

12. Conclusiones

13. Trabajo Futuro

Bibliografía

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

A. Anexos