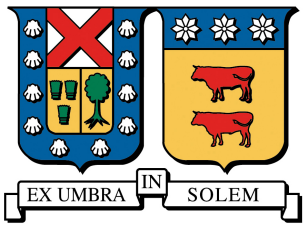
Universidad Técnica Federico Santa María
Departamento de Informática
Valparaíso, Chile



Una Arquitectura de Referencia para Web Browsers: Hacia una unificación de Conceptos de Seguridad

Paulina Andrea Silva Ghio

Memoria para optar al título de: Ingeniería Civil Informática

Profesor Guía: Raúl Monge
Profesor Correferente: Javier Cañas

6 de octubre de 2016

Si sta come
d'autunno
sugli alberi
le foglie
***Soldati** di Guiseppe Ungaretti (1918)*

Agradecimientos

Con esta Memoria voy a dar por finalizado los largos 6 años de la carrera, que terminaron por ser casí 7 y algo más por el Magister. No me arrepiento de mis decisiones en la parte académica, pero a veces en lo personal creo que pudo haber sido de otra manera. Tuve muchos desafíos que realizar al estudiar para este trabajo, partiendo por mi nulo conocimiento en Seguridad y a veces la falta de motivación. Sin embargo, estoy acá en este momento gracias a esas decisiones y experiencias que he ganado en el intertanto. Gracias a todas las personas que me motivaron, en especial, a mi profesor guía Raúl Monge (UTFSM) y el profesor Eduardo Fernandez (Florida Atlantic University), quienes me mostraron un camino interesante a seguir.

Quiero agradecer a todos mis amigos de la Universidad, que son muchos, y aquellos que la abandonaron por un camino mejor o más interesante. Gracias por haberse presentado en mi vida y hacerla entretenida. Sin la risa y diversión en mi vida, probablemente sería una persona amargada. Gracias a todos por soportar mi malhumor y comprenderme cuando estoy angustiada. Gracias también por haberme ayudado academicamente, que si bien todos creen que soy matea nada tengo de eso; solo estudio demasiado y a veces no de la mejor manera.

Gracias Mamá y Papá por darme educación. Se que no es fácil pagar tanto dinero todos los meses, pero en verdad se los agradezco siempre. Gracias a que he tenido la oportunidad de estudiar en una Universidad, se cuán importante es la educación y que debo aprovecharla al máximo. Se que muchas veces tuvimos varios problemas mientras yo crecía, pero quiero hacerles saber que estoy agradecida de ser su hija. Gracias por cuidar y confiar en mi.

Gracias Panchomon por todo, eres una existencia muy importante en mi vida y espero que lo sepas. Gracias Micchan, por ser mi manta cuando estoy triste. Ustedes dos han sido los pilares más grandes que he tenido en estos años de universidad. Gracias Fernando, Samuel, José Miguel, Francisco, Matías y Andrés, por ser mis *dudes* y soportarme siempre. Gracias Priscilla, Scarlet y Susana, por ser mis amigas más cercanas en la Universidad. Ko-chan, Yurie, Asumi, Geso y Motoki a ustedes también gracias por apoyarme siempre. Finalmente, ¡gracias a todos!, por tenerme una gran paciencia a lo largo de estos años, por levantarme el ánimo cuando no quiero

dar más pasos hacia adelante, por inspirarme a ser mejor, y por estar en mi vida de alguna que otra forma. También muchas gracias al que lee este documento, en especial, por darse el tiempo de hacerlo.

Resumen

El *Web Browser* es una de las aplicaciones más usadas - *killer app* - y también una de las primeras en aparecer en cuanto se creó el Internet (década de los 90). Por lo mismo, su nivel de madurez con respecto a otros desarrollos es significativo y permite asegurar ciertos niveles de confianza cuando otros usan un *Web Browser* como cliente para sus Sistemas.

Actualmente muchos desarrollos de software crean sistemas que están conectados a la Internet, pues permite agregar funcionalidades al sistema y facilidades para sus *Stakeholders*. Esto lleva a depender de un cliente web, cómo un *Web Browser*, que permite el acceso a los servicios, datos u operaciones que el sistema entrega. Sin embargo, la Internet influye en la superficie de ataque del nuevo sistema, y lamentablemente tanto Stakeholders como muchos desarrolladores no están al tanto de los riesgos a los que se exponen.

Al tener sistemas que se interconectan con el *Web Browser*, Stakeholder como Desarrolladores deben estar al tanto de los posibles riesgos que podrían enfrentar. La falta de educación de seguridad en los desarrolladores de software de un proyecto, la poca y dispersa documentación de cada navegador (así como su estandarización), podría llegar a ser un flanco débil en el desarrollo de grandes Architecturas que dependen del *Browser* para realizar sus servicios. Una Arquitectura de Referencia del *Web Browser*, utilizando Patrones Arquitecturales, podría ser una base para el entendimiento de los mecanismos de seguridad y su Arquitectura, que interactua con un sistema Web mayor. Ésto mismo, entregaría una unificación de ideas y terminología, al dar una mirada holística sin tener en cuenta detalles de implementación tanto del *Browser* como el sistema con el que interactua.

En esta memoria presentada al Departamento de Informática (DI) de la UTFSM[1] Casa Central, incursionará en el ámbito de la seguridad del *Web Browser*, tiene como objetivo el obtener documentos semi-formales que servirán como herramientas a personas que desarrollen Software y hagan un fuerte uso del navegador para las actividades del sistema desarrollado.

Abstract

The *Web Browser* is known as one of the most used applications - or *killer app* - and also was the first introduced when the Internet was created (1990s). Which is why, its significant maturity level is above in comparison with other developements and can assure a certain level of *trust* whenever it is used as a client with other systems.

[1] Universidad Técnica Federico Santa María

Currently a lot of software developments create systems that are connected to the Internet, which allows to add functionality within a system and facilities to their *Stakeholders*. This leads to depend in a *web client*, as the *Web Browser*, which allows access to services, data or operations that the system delivers. Nevertheless, the Internet influences the attack surface of the new system, and unfortunately many stakeholders and developers are not aware of the risks they are exposed.

Having systems which are interconnected with the *Web Browser*, Stakeholder and Developers should be aware of the potential risks they could face. The lack of Security Education in Software developers of a project, the low and scattered documentation of each browser (and standardization), could become a great flaw in big architectural developments which depends on the browser to do their services. A Reference Architecture of the *Web Browser*, using Architectural Patterns, could be a base for understanding the security mechanisms and its architecture, which interacts with a bigger web system. This would give an unification of ideas and terminology, giving a holistic view regardless the implementation details for both the browser and the system it communicates to.

This work presented to the Departamento de Informática (DI) of the UTFSM[2] Casa Central, will seek within the scope of *Web Browser* Security, has the objective or goal to obtain semi-formal documents that can help as tools to software developers who make a strong use of a web browser within the activities of the systems they are building.

[2]Universidad Técnica Federico Santa María

Índice general

Índice general VI

Índice de figuras VII

Índice de cuadros VIII

1. Introduction 1

2. Theoric Framework - Web Technologies 2

3. Browser's Threats 3

4. State of the Art 4

5. Towards a definition of a Security Reference Architecture 5

6. Misuse Patterns 6

7. Conclusions 7

8. Glossary 8

Bibliografía 9

Índice de figuras

Índice de cuadros

Capítulo 1

Introduction

Capítulo 2

Theoric Framework - Web Technologies

Capítulo 3

Browser's Threats

Capítulo 4

State of the Art

Capítulo 5

Towards a definition of a Security Reference Architecture

Capítulo 6

Misuse Patterns

Capítulo 7

Conclusions

Capítulo 8

Glossary

Bibliografía

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

[2] W. W. W. C. W3C, "About." [Online]. Available: http://www.w3.org/Consortium/

[3] "Sandbox - The Chromium Projects." [Online]. Available: http://www.chromium.org/developers/design-documents/sandbox

[4] M. V. Yason, "Diving into IE 10's Enhanced Protected Mode Sandbox."

[5] M. Crowley, *Pro Internet Explorer 8 & 9 Development: Developing Powerful Applications for The Next Generation of IE*, 1st ed. Berkely, CA, USA: Apress, 2010.

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

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

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

[9] "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

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

[11] ——, "Architecture and evolution of the modern web browser," uRL: `http://grosskurth.ca/papers.html#browser-archevol`. Note: submitted for publication.

[12] "How browsers work." [Online]. Available: http://taligarsiel.com/Projects/howbrowserswork1.htm

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

[14] K. M. Goertzel, T. Winograd, H. L. McKinley, L. J. Oh, M. Colon, T. McGibbon, E. Fedchak, and R. Vienneau, "Software security assurance: A state-of-art report (sar)," DTIC Document, Tech. Rep., 2007.

[15] J. Yoder, J. Yoder, J. Barcalow, and J. Barcalow, "Architectural patterns for enabling application security," *Proceedings of PLoP 1997*, vol. 51, p. 31, 1998. [Online]. Available: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Architectural+patterns+for+enabling+application+security#0

[16] E. B. Fernandez, "A methodology for secure software design." in *Software Engineering Research and Practice*, 2004, pp. 130–136.

[17] 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

[18] C. M. U. Computer Emergency Response Team, "Early identification reduces total cost (segment from cert's podcasts for bussiness leaders)." [Online]. Available: http://www.cert.org/podcasts/podcast_episode.cfm?episodeid=34820

[19] M. Hicks, "Interview to **Kevin Haley** (from **Symantec**)," 2014, mike Hicks (Profesor of Software Security course in Coursera.org).

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

[21] 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.

[22] E. B. Fernandez, M. VanHilst, M. M. L. Petrie, and S. Huang, "Defining security requirements through misuse actions," in *Advanced Software Engineering: Expanding the Frontiers of Software Technology*. Springer US, 2006, pp. 123–137.

[23] 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.

[24] E. B. Fernandez, N. Yoshioka, H. Washizaki, J. Jurjens, M. VanHilst, and G. Pernu, *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

[25] P. Avgeriou, "Describing, Instantiating and Evaluating a Reference Architecture: A Case Study," *Enterprise Architect Journal*, vol. 342, no. 1, p. 347, 2003. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/21213183

[26] M. Galster and P. Avgeriou, "Empirically-grounded Reference Architectures: A Proposal," pp. 153–157, 2011.

[27] F. Buschman, R. Meunier, H. Rohnert, P. Sommerlad, and M. Stal, "A system of patterns: pattern-oriented software architecture," 1996.

[28] W. Alcorn, C. Frichot, and M. Orrù, *The Browser Hacker's Handbook*. John Wiley & Sons, 2014.

[29] "HTML5 Web Messaging." [Online]. Available: http://www.w3.org/TR/webmessaging/

[30] . D. XMLHttpRequest Level 1, "Xmlhttprequest specification." [Online]. Available: http://www.w3.org/TR/2014/WD-XMLHttpRequest-20140130/

[31] T. W. API, "Websocket specification." [Online]. Available: http://www.w3.org/TR/2012/CR-websockets-20120920/

[32] W. . R. time Communication Between Browsers, "Webrtc specification." [Online]. Available: http://www.w3.org/TR/2015/WD-webrtc-20150210/

[33] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2." [Online]. Available: https://tools.ietf.org/html/rfc5246

[34] W. W. Group, "Html5 specification." [Online]. Available: http://www.w3.org/TR/html5/

[35] A. Barth, C. Jackson, and W. Li, "Attacks on javascript mashup communication," in *Proceedings of the Web*, vol. 2. Citeseer, 2009.

[36] A. Barth, J. Weinberger, and D. Song, "Cross-Origin JavaScript Capability Leaks : Detection , Exploitation , and Defense," *Opera*, vol. 147, pp. 187–198, 2009.

[37] A. Barth, A. P. Felt, P. Saxena, and A. Boodman, "Protecting Browsers from Extension Vulnerabilities," *Ndss*, vol. 147, pp. 1315–1329, 2010. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.154.5579&rep=rep1&type=pdf

[38] L. Liu, X. Zhang, G. Yan, and S. Chen, "Chrome extensions: Threat analysis and countermeasures," *... of the Network and Distributed Systems ...*, 2012. [Online]. Available: https://www.cs.gmu.edu/~sqchen/publications/NDSS-2012.pdf

[39] A. Singh and S. Sathappan, "A Survey on XSS web-attack and Defense Mechanisms," vol. 4, no. 3, pp. 1160–1164, 2014.

[40] A. Barth, C. Jackson, C. Reis, T. Team *et al.*, "The security architecture of the chromium browser," 2008.

[41] "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

[42] C. Reis and S. D. Gribble, "Isolating web programs in modern browser architectures," *Proceedings of the fourth ACM european conference on Computer systems EuroSys 09*, vol. 25, no. 1, p. 219, 2009. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1519065.1519090

[43] A. Barth, C. Jackson, and J. C. Mitchell, "Securing frame communication in browsers," *Communications of the ACM*, vol. 52, no. 6, pp. 83–91, 2009.

[44] A. Saini, M. S. Gaur, and V. Laxmi, "Privacy Leakage Attacks in Browsers," pp. 257–276, 2014.

[45] O. S. Architecture, "Definitions by osa." [Online]. Available: http://www.opensecurityarchitecture.org/cms/definitions

[46] L. Bass, P. Clements, and R. Kazman, *Software Architecture in Practice*, 3rd ed. Addison-Wesley Professional, 2012.

[47] O. Encina, "Towards a Security Reference Architecture for Federated Inter-Cloud Systems," 2014.

[48] K. Hashizume, E. B. Fernandez, and M. M. Larrondo-petrie, "A reference architecturefor cloud computing. Submitted for publication." 2014.

[49] E. B. Fernandez, H. Washizaki, N. Yoshioka, and M. VanHilst, "An approach to model-based development of secure and reliable systems," *Proceedings of the 2011 6th International Conference on Availability, Reliability and Security, ARES 2011*, pp. 260–265, 2011.

[50] E. Fernández and M. Larrondo, "Security Patterns and Secure Systems Design," no. June, pp. 1–12, 2006.

[51] E. Fernandez, J. Pelaez, and M. Larrondo-Petrie, "Attack patterns: A new forensic and design tool," in *Advances in digital forensics III*. Springer New York, 2007, pp. 345–357.

[52] E. Fernandez, N. Yoshioka, and H. Washizaki, "Modeling misuse patterns," in *Availability, Reliability and Security, 2009. ARES '09. International Conference on*, March 2009, pp. 566–571.

[53] N. Yoshioka, "A development method based on security patterns," *Presentation, NII, Tokyo*, 2006.

[54] ——, "Integration of attack patterns and protective patterns," in *1st International Workshop on Software Patterns and Quality (SPAQu'07)*, 2007, p. 45.

[55] J. C. Pelaez, E. B. Fernandez, and M. M. Larrondo-Petrie, "Misuse patterns in voip," *Security and Communication Networks*, vol. 2, no. 6, pp. 635–653, 2009.

[56] E. B. Fernandez, N. Yoshioka, and H. Washizaki, "A worm misuse pattern," in *Proceedings of the 1st Asian Conference on Pattern Languages of Programs*. ACM, 2010, p. 2.

[57] K. Hashizume, N. Yoshioka, and E. B. Fernandez, "Misuse patterns for cloud computing," in *Proceedings of the 2nd Asian Conference on Pattern Languages of Programs*. ACM, 2011, p. 12.

[58] J. Muñoz-Arteaga, E. B. Fernandez, and H. Caudel-García, "Misuse pattern: spoofing web services," in *Proceedings of the 2nd Asian Conference on Pattern Languages of Programs*. ACM, 2011, p. 11.

[59] E. B. Fernandez, E. Alder, R. Bagley, and S. Paghdar, "A misuse pattern for retrieving data from a database using sql injection," in *BioMedical Computing (BioMedCom), 2012 ASE/IEEE International Conference on*. IEEE, 2012, pp. 127–131.

[60] A. Alkazami and E. B. Fernandez, "Cipher suite rollback: A misuse pattern for the ssl/tls client/server authentication handshake protocol," 2014.

[61] O. Encina, E. B. Fernandez, and R. Monge, "A misuse pattern for denial-of-service in federated inter-clouds," 2014.

[62] J. Talamantes, "The social engineer's playbook." [Online]. Available: http://www.thesocialengineersplaybook.com/

[63] M. Rajab, L. Ballard, and N. Lutz, "CAMP: Content-agnostic malware protection," *Proceedings of Annual ...*, 2013. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.295.6192&rep=rep1&type=pdf

[64] N. S. S. Labs and A. R. Abrams, "Evolutions In Browser Security," no. October, pp. 1–20, 2013.

[65] "Top 10 2013 - OWASP." [Online]. Available: https://www.owasp.org/index.php/Top_10_2013

[66] "Security/ProcessIsolation/ThreatModel." [Online]. Available: https://wiki.mozilla.org/Security/ProcessIsolation/ThreatModel

[67] R. Abrams, J. Pathak, and O. Barrera, "Browser security comparative analysis: Phishing protection," 2013.

[68] ——, "Browser Security Comparative Analysis: Socially Engineered Malware Blocking," 2014.

[69] J. Drake, P. Mehta, C. Miller, S. Moyer, R. Smith, C. Valasek, and A. Q. Approach, "Browser Security Comparison," *Accuvant Labs*, 2011.

[70] N. Utakrit, "Review of Browser Extensions, a Man-in-the-Browser Phishing Techniques Targeting Bank Customers," *Proceedings of the 7th Australian Information Security Management Conference*, pp. 110–119, 2009. [Online]. Available: http://www.scopus.com/inward/record.url?eid=2-s2.0-84864552184&partnerID=40&md5=3d08a9c7c4ba9dbe5e04fb831ad5257b$\delimiter"026E30F$nhttp://ro.ecu.edu.au/ism/19/

[71] T. Dougan and K. Curran, "Man in the Browser Attacks," *International Journal of Ambient Computing and Intelligence*, vol. 4, no. 1, pp. 29–39, 2012.

[72] "DOM Based XSS - OWASP." [Online]. Available: https://www.owasp.org/index.php/DOM_Based_XSS

[73] "[DOM Based Cross Site Scripting or XSS of the Third Kind] Web Security Articles - Web Application Security Consortium." [Online]. Available: http://www.webappsec.org/projects/articles/071105.shtml

[74] "272620 – XSS vulnerability in internal error messages." [Online]. Available: https://bugzilla.mozilla.org/show_bug.cgi?id=272620

[75] S. D. Paola and G. Fedon, "Subverting Ajax," *23rd Chaos Communication Congress*, no. December, 2006. [Online]. Available: http://events.ccc.de/congress/2006/Fahrplan/attachments/1158-Subverting_Ajax.pdf

[76] A. B. <ietf@adambarth.com>, "The Web Origin Concept." [Online]. Available: http://tools.ietf.org/html/draft-abarth-origin-09

[77] M. Zalewsk, "Browser security handbook, part 2," Google, Web page, 2008. [Online]. Available: https://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy

[78] B. Sullivan and V. Liu, *Web application security.* McGraw-Hill, 2012.

[79] J. Hodges, C. Jackson, and A. Barth, "HTTP Strict Transport Security {(HSTS)}," Internet Engineering Task Force (IETF), RFC 6797, 2012.

[80] C. Reis, A. Barth, and C. Pizano, "Browser Security: Lessons from Google Chrome," *Commun. ACM*, vol. 52, no. 8, pp. 45–49, 2009. [Online]. Available: http://dl.acm.org/ft_gateway.cfm?id=1556050&type=html$\delimiter"026E30F$npapers3://publication/doi/10.1145/1538947.1556050

[81] "Necko: Electrolysis design and subprojects." [Online]. Available: https://wiki.mozilla.org/Necko:_Electrolysis_design_and_subprojects

[82] R. Colvin, "SmartScreen," 2010. [Online]. Available: http://blogs.msdn.com/b/ie/archive/2010/10/13/stranger-danger-introducing-smartscreen-application-reputation.aspx

[83] "Site Isolation - The Chromium Projects." [Online]. Available: https://www.chromium.org/developers/design-documents/site-isolation

[84] "The Future of Developing Firefox Add-ons | Mozilla Add-ons Blog." [Online]. Available: https://blog.mozilla.org/addons/2015/08/21/the-future-of-developing-firefox-add-ons/

[85] 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

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

[87] G. Team, "Evolution of the web." [Online]. Available: http://www.evolutionoftheweb.com/

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

[89] "Multiprocess Desktop Firefox | Air Mozilla | Mozilla, in Video." [Online]. Available: https://air.mozilla.org/inter-presentation-schuster/

[90] "Firefox Nightly Builds." [Online]. Available: https://nightly.mozilla.org/

[91] "Multiprocess Firefox | Bill McCloskey's Blog on WordPress.com." [Online]. Available: https://billmccloskey.wordpress.com/2013/12/05/multiprocess-firefox/#ipc

[92] "Inter-process Communication (IPC) - The Chromium Projects." [Online]. Available: https://www.chromium.org/developers/design-documents/inter-process-communication

[93] T. Vrbanec, "The evolution of web browser architecture," pp. 472–480, 2013.

[94] T. M. Coporation, "Common vulnerabilities and exposures." [Online]. Available: https://cve.mitre.org/about/terminology.html

[95] W3C, "Same Origin Policy," W3C, Web page, 2010. [Online]. Available: https://www.w3.org/Security/wiki/Same_Origin_Policy

[96] C. Jackson and A. Barth, "Beware of finer-grained origins," *Web 2.0 Security and Privacy*, 2008. [Online]. Available: http://seclab.stanford.edu/websec/origins/fgo.pdf

[97] M. Silic, J. Krolo, and G. Delac, "Security vulnerabilities in modern web browser architecture," *MIPRO, 2010 Proceedings of the 33rd International Convention*, 2010.

[98] E. B. Fernandez and R. Pan, "A pattern language for security models," *proceedings of PLOP*, vol. 1, pp. 1–13, 2001. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.90.5898

[99] E. B. Fernandez, R. Monge, and K. Hashizume, "Building a security reference architecture for cloud systems," in *Proceedings of the WICSA 2014 Companion Volume*. ACM, 2014, p. 3.

[100] I. C. Security, "Avoiding the top 10 security flaws." [Online]. Available: http://cybersecurity.ieee.org/center-for-secure-design/avoiding-the-top-10-security-flaws.html