Estado del arte

Ing. Felipe de Jesús Miramontes Romero

Centro de Investigación en Matemáticas A.C.,
Maestría en Ingeniería de Software,
Avenida Universidad 222, La Loma, 98068, Zacatecas, México.
felipemiramontesr@gmail.com
http://www.ingsoft.mx

1. Introducción

Como base fundamental de este estudio se ha realizado una revisión sistemática de la literatura acerca del desarrollo de aplicaciones en red con características enfocadas a la seguridad y las técnicas existentes para su correcta construcción, el resultado del análisis muestra que la literatura existente posee una clara tendencia hacia la generalización de los tipos de Software pues en su mayoría las técnicas estudiadas consideran a las aplicaciones en red como Software genérico, por otra parte y a manera de excepción existen muy pocas que tratan el tema de forma particular.

2. Protocolo de la revisión sistemática

El protocolo de la revisión sistemática es definido como una serie de pasos o etapas que pretenden ayudar al investigador a reunir el suficiente material de estudio sobre alguna temática de importancia, entre los principales beneficios obtenidos se encuentran el enriquecimiento de la base de conocimientos, las actividades a realizar y las decisiones tomadas a lo largo de la investigación, a continuación son mencionadas cada una de las etapas que lo conforman.

1. Planificación.

   En esta etapa es necesario establecer los objetivos y el rumbo que debe tomar la investigación. A continuación son mencionadas las actividades que se deben realizar.

   a) Realizar una adecuada elección del tema de investigación.
   b) Seleccionar cadenas y fuentes de búsqueda.
   c) Establecer criterios para la elección de estudios primarios y secundarios.

2. Revisión o ejecución.

   En esta etapa es necesario ejecutar ciertas actividades que garantizan un correcto desarrollo. Las actividades se mencionan a continuación.

   a) Ejecutar las búsquedas de información.
   b) Evaluar la calidad de la información.
   c) Revisar cada uno de los estudios seleccionados.
   d) Extraer la información relevante y necesaria.
   e) Documentar cada una de las interacciones para llevar un registro histórico que permita controlar el rumbo de la investigación.

3. Publicación.

   En esta etapa es necesario exponer de manera formal los resultados de nuestra investigación por medio de la redacción de un documento formal, en este caso la tesis, en la cual se deben incluir cada uno de los cálculos estadísticos y numéricos realizados.

3. Revisión sistemática para la tesis

El objetivo principal de la Revisión Sistemática de la Literatura (RSL) en la ingeniería de software es proporcionar los medios para suministrar la evidencia de mayor calidad y formalidad de la investigación actual e integrarla con la experiencia practica para lograr la mejor toma de decisiones en relación con el desarrollo y el mantenimiento de Software. La revisión sistemática sera realizada para resolver una problemática concreta, en este caso en particular, la temática que se pretende abordar es la construcción de una técnica para el desarrollo de aplicaciones seguras en red (Aplicaciones Web). La revisión sistemática se apega a las necesidades esta investigación pues sus principales metas son identificar, evaluar y interpretar la mayoría de los recursos literarios disponibles acerca de un tema, cuestión, tópico, área o fenómeno de interés, mismas que sirvieran como base para el desarrollo de la tesis y que además mostraran a los interesados el estado actual de la linea de investigación (Estado del Arte). Debido a la formalidad que la revisión sistemática posee y debido a su reconocimiento como protocolo en comparación con métodos tradicionales se espera que la construcción y redacción del estado del arte sea realizado en tiempo y forma.

Para la recolección del material de estudio utilizando la revisión sistemática se formularon las siguientes preguntas de investigación:

1. ¿Cuáles técnicas son usadas para desarrollar aplicaciones en red seguras?
2. ¿Cuáles son los principales beneficios que las técnicas para el desarrollo de aplicaciones en red seguras aportan a los involucrados en el desarrollo del producto?
3. ¿Cuáles son las principales deficiencias existentes en las técnicas para el desarrollo de aplicaciones en red seguras?

Una vez definidas las preguntas de investigación fueron creadas cadenas de palabras unidas por medio de operadores binarios y fueron usadas para optimizar la búsqueda e identificación del material de investigación apropiado. Dichas

cadenas fueron formadas por medio de palabras claves ligadas a la temática principal y las cuales a continuación son mencionadas:

1. Técnicas AND Desarrollo AND Aplicaciones en Red AND Seguras
2. Deficiencias OR Problemas AND Técnica AND Desarrollo AND Aplicaciones en Red AND Seguras
3. Aseguramiento AND Seguridad AND Aplicaciones en red
4. Desarrollo de Software AND Seguro

Una vez ejecutada la búsqueda de las cadenas anteriormente mencionadas los estudios obtenidos fueron analizados y evaluados para su inclusión en la literatura de estudio por medio de cumplimento de los siguientes criterios de aceptación:

1. ¿La referencia se encuentra publicada en idioma ingles o español?
2. ¿La referencia explícitamente ha sido publicada en años posteriores al 2009 o se ha actualizado en años posteriores al 2009?
3. ¿La referencia proporciona datos fiables y comprobables?
4. ¿La referencia explícitamente discute algún aspecto sobre técnicas para el desarrollo de aplicaciones en red seguras?

4. Literatura incluida en el estado del arte

La literatura que se ha incluido en el estado del arte ha cumplido las paramétricas establecidas a lo largo del desarrollo del proceso definido como revisión sistemática, se han incluido trabajos realizados por entidades académicas y de investigación así como trabajos desarrollados por entidades privadas, empresas, organizaciones gubernamentales y comunidades abiertas, todo esto con el fin de establecer una base confiable para el desarrollo de la nueva técnica para el desarrollo de aplicaciones seguras en red. A continuación son presentadas las técnicas recabadas en el estudio.

Glossary

Software es cualquier conjunto de instrucciones que dirige un sistema o equipo electrónico para llevar a cabo operaciones específicas. Las aplicaciones informáticas se compone de programas de ordenador, bibliotecas y datos no ejecutables relacionados (como la documentación en línea o los medios digitales). 1, 2

Acronyms

RSL Revisión Sistemática de la Literatura. 2

Referencias

1. Microsoft, "Microsoft security development adoption: Why and how," Septiembre 2013.
2. Microsoft, "Implementación simplificada del proceso sdl de microsoft," Febrero 2010.
3. C. S. Nuno Teodoro, "Web application security," Enero 2011.
4. S. L. Michael Howard, "Microsoft security development lifecicle," Junio 2015.
5. O. R. Ikram El rhaffari, "Benchmarking sdl and clasp lifecycle," Mayo 2014.
6. OWASP, "CLASP introduction." `https://www.owasp.org/index.php/CLASP`. Fecha de acceso: 25-11-2015.
7. OWASP, "CLASP concepts." `https://www.owasp.org/index.php/CLASP_Concepts`. Fecha de acceso: 25-11-2015.
8. OWASP, "Clasp activity-assessment view," Marzo 2006.
9. OWASP, "SAMM introduction." `https://www.owasp.org/index.php/Category:Software_Assurance_Maturity_Model`. Fecha de acceso: 30-11-2015.
10. OWASP, "OWASP introduction." `https://www.owasp.org/index.php/Category:OWASP_Project`. Fecha de acceso: 30-11-2015.
11. P. Amey, "CbyC cbyc." `https://buildsecurityin.us-cert.gov/articles/knowledge/sdlc-process/correctness-by-construction`. Fecha de acceso: 2-12-2015.
12. C. J. B. Abundis, "Metodologías para desarrollar software seguro," Diciembre 2013.
13. R. C. Anthony Hall, "Correctness by construction: Bettercan also be cheaper," Febrero 2002.
14. Praxis, "Praxis the foremost international specialist in critical systems engineering." `http://www.praxis-his.com/`. Fecha de acceso: 6-12-2015.
15. Praxis, "Praxis high integrity systems." `http://web.archive.org/web/20081114100215/http://www.praxis-his.com/services/software/approach.asp`. Fecha de acceso: 6-12-2015.
16. M. P. Daniel Mellado, Eduardo Fernandez-Medina, "Applying a security requirements engineering process," 2006.
17. MAP, "Metodología de análisis y gestión de riesgos de los sistemas de información (magerit - v 2)," 2005.
18. M. P. Daniel Mellado, Eduardo Fernandez-Medina, "A common criteria based security requirements engineering process for the development of secure information systems," 2007.
19. C. C. Org, "Introduction and general model," 2012.
20. C. C. Org, "Common Criteria certified products list - statistics." `http://www.commoncriteriaportal.org/products/stats/`. Fecha de acceso: 20-12-2015.
21. P. L. R. W. E. W. Christine Artelsmair, Wolfgang Essmayr, "Cosmo: An approach towards conceptual security modeling," 2002.
22. O. M. Group, "OMG about omg." `http://www.omg.org/gettingstarted/gettingstartedindex.htm`. Fecha de acceso: 2-1-2016.

23. J. Jürjens, "Umlsec: Extending uml for secure systems development," 2002.
24. J. Jürjens, *Secure Systems Development with UML*. Dep. of Informatics, Software and Systems Engineering, Technische Universität München, Boltzmannstr. 3, 85748 München/Garching: Springer, 1st ed., 2004.
25. J. Jürjens, "Using umlsec and goal trees for secure systems development," 2002.
26. P. S. M. ary McGraw and J. West, "Building security in maturity model bsimm-v," Octubre 2013.
27. P. S. M. ary McGraw and J. West, "Building security in maturity model bsimm-vi," Octubre 2013.
28. BSIMM, "BSIMM bsimm." `https://go.cigital.com/hubfs/Datasheets/building-secuirty-in-maturity-model-BSIMM-cigital.pdf`. Fecha de acceso: 12-1-2016.