Inicio de la Línea de Investigación "Ingeniería de Software y Defensa Cibernética"

Roberto Uzal[2], Jeroen van de Graaf[1], Germán Montejano[2,3], Daniel Riesco[2], Pablo García[3]

[1] Departamento de Ciencia da Computacao, Universidade Federal de Minas Gerais - Brasil
jvdg@dcc.ufmg.br –http://www.dcc.ufmg.br/~jvdg

[2] Facultad de Ciencias Físico-Matemáticas y Naturales, Universidad Nacional de San Luis – Argentina –
ruzl@uolsinectis.com.ar, gmonte@unsl.edu.ar, driesco@unsl.edu.ar - http://sel.unsl.edu.ar

[3] Facultad de Ciencias Exactas y Naturales, Facultad de Ingeniería, Universidad Nacional de La Pampa – Argentina -
pablogarcia@exactas.unlpam.edu.ar – http://www.unlpam.edu.ar

Resumen

Se presenta una nueva línea de investigación que estará inserta en el proyecto *"Ingeniería de Software: Aspectos de alta sensibilidad en el ejercicio de la profesión de Ingeniero de Software"* de la UNSL [1]. Esta línea estará incluida en trabajos realizados en cooperación con universidades de Brasil [2] y comprende a la prevención de la intrusión y/o mitigación de los efectos de software malicioso sofisticado destinado a causar daños a la infraestructura crítica del país, a paralizar el funcionamiento de los servicios esenciales o para acceder a información gubernamental de carácter secreto [3] …[14]. Están incluidos en esta línea: la prevención y detección de software malicioso sofisticado, la ingeniería reversa del malware detectado [15] [16] [17] [18], la identificación del emisor mediante "análisis de flujo de redes" [19] [20] y la neutralización de ataques provenientes desde otros estados naciones. Esta presentación incluye ejemplos reales de agresiones devastadoras entre países utilizando "malware" extremadamente complejo y la enumeración de los conceptos y habilidades a ser desarrollados en el contexto descripto. Se cita el consenso internacional que la UNSL ha logrado respecto de la necesidad de un "Nuevo Paradigma de Seguridad Informática" [21] y se describen los temas de investigación ya encarados. Finalmente se enumeran las referencias.

Palabras clave: Defensa Cibernética, Seguridad Informática, Análisis de Flujo de Redes, Nuevo Paradigma en Seguridad Informática

Contexto

El proyecto *"Ingeniería de Software: Aspectos de alta sensibilidad en el ejercicio de la profesión de Ingeniero de Software"* de la UNSL, con ligeras variantes en su denominación, viene desarrollándose, muy exitosamente, desde hace más de quince años. Tres de los integrantes de proyecto han alcanzado la Categoría I en el ámbito del Programa de Incentivo a la Investigación en Universidades Nacionales y los otros miembros del equipo han alcanzado diversas Categorizaciones en el mismo Programa. El proyecto está íntimamente asociado al desarrollo de la carrera de grado de Ingeniería Informática y de las carreras de post grado Doctorado en Ingeniería Informática, Maestría en Ingeniería de Software, Maestría en Calidad del Software y Especialización en Ingeniería de Software.

Este proyecto mantiene efectivos esquemas asociativos [1] con el Instituto de Tecnología del Software de las Naciones Unidas (Macao), con la Universidad Estatal de San Francisco (EEUU), con la Universidad Federal de Minas Gerais (Brasil), con la Universidad de Minho (Portugal) y con las Universidades de Castilla La Mancha, Vigo y Politécnica de Valencia (España). Asimismo el proyecto *"Ingeniería de Software: Aspectos de alta sensibilidad en el*

ejercicio de la profesión de Ingeniero de Software" trabaja en permanente contacto con el Parque Industrial del Software de San Luis, el de Córdoba y con centros de excelencia de elaboración de Software de Europa.
El financiamiento del proyecto proviene regularmente de la UNSL, de programas nacionales e internacionales específicos, de emprendimientos como el CAPG – BA [2] y de cada uno de las actividades que han venido realizándose como resultado de la interacción con el entorno social y productivo.

1. Introducción

En el contexto del proyecto "*Ingeniería de Software: Aspectos de alta sensibilidad en el ejercicio de la profesión de Ingeniero de Software"* de la UNSL se habían venido estudiando detenidamente los aspectos tecnológicos correspondientes a incidentes entre estados naciones del tipo:

- La masiva y devastadora agresión cibernética de Rusia a aeropuertos, sistemas ferroviarios, hospitales, sistema financiero y medios periodísticos de Estonia en el 2007. El ataque provocó la reacción de Alemania en ayuda de Estonia y luego la intervención de la NATO. A partir de este conflicto la NATO (Organización del Atlántico Norte) consolida su política y estructura de Defensa Cibernética [22].
- La alteración, mediante Armas Cibernéticas, del software de un Sistema de Radar de origen Ruso en el Norte de Siria, a orillas del Éufrates, en el 2007, impidiéndole detectar a cazas bombarderos de Israel que atacaron y destruyeron construcciones realizadas, aparentemente, por norcoreanos [3].
- La intrusión de China en sistemas satelitales de Estados Unidos [23].
- El prácticamente confirmado acceso, también por parte de China, a información del área Defensa altamente sensitiva, residente en la Intranet del Jet Propulsion Laboratory (California Institute of Technology – NASA) [24].
- La voladura, utilizando "virus de red" o "gusanos", de las baterías de centrífugas en la planta de enriquecimiento de uranio en Natanz, Irán [25] [26].
- La presencia de la ultra sofisticada Arma Cibernética, Flame, en las plataformas de explotación petrolera de Irán [27]
- La Guerra Cibernética de carácter "sine die" entre Pakistán e India [28 [29].

Asimismo, en el contexto del proyecto "Ingeniería de Software: Aspectos de alta sensibilidad en el ejercicio de la profesión de Ingeniero de Software" de la UNSL, en relación con lo expuesto más arriba, se habían venido encarando los aspectos antes de esta formalización de la nueva línea de investigación:

1.1. Acciones de Comunicación / Difusión realizadas por la UNSL:
  1.1.1. Conferencia en el Centro de Oficiales de las FFAA: "Nuevos escenarios, nuevos conflictos, nuevas armas, nuevos soldados: Cyber War"; 24 de abril de 2012
  1.1.2. Artículo de opinión sobre Cyber War en la Revista DEF de Agosto de 2012
  1.1.3. Reportaje al Dr. Roberto Uzal sobre Cyber War - Canal de TV C5N el 19 de agosto a las 23 horas.
  1.1.4. Reportaje al Dr. R. Uzal sobre Guerra Cibernética realizado por la Revista DEF ON LINE – Agosto de 2012 http://www.defonline.com.ar/?p=9064
  1.1.5. Consejo Profesional de Ingenieros Electrónicos y en Telecomunicaciones – COPITEC – "Guerra Cibernética" (conferencia), 4 de julio de 2012
  1.1.6. Consejo Argentino de Relaciones Internacionales, seminario sobre "Crimen Organizado Transnacional y

Ciberamenazas", 11 de noviembre de 2012

1.1.7. Sociedad Científica Argentina. Seminario sobre Guerra Cibernética dirigido a los Oficiales del Ejército de la Especialidad Informática; 21 de noviembre de 2012.

1.1.8. Exposición en la Universidad Nacional de San Luis en el contexto de las Jornadas por un Ciberespacio más seguro y confiable: "Ciberamenazas, escenarios y propuestas"; 18 de diciembre de 2012 http://webfmn.unsl.edu.ar/boletines/boletin418/boletin418.html

1.1.9. Artículo "Guerra Cibernética: ¿Un desafío para la Defensa Nacional", Revista Visión Conjunta (Escuela Superior de Guerra Conjunta – Ministerio de Defensa), Año 4, Nro 7, 2012

1.2. Tesis de Maestría de Walter Agüero: El alumno – graduado de la Maestría en Ingeniería de Software de la Universidad Nacional de San Luis Walter Agüero ha manifestado su interés en encarar su trabajo de tesis según el siguiente esquema general:

1.2.1. Desarrollo de un módulo adicional, para un determinado sistema operativo de computadora personal, tal que le posibilite a dicha PC, bajo determinadas condiciones, sustraerle / copiarle la lista de contactos a teléfonos celulares que se encuentren dentro de determinado distancia (de la PC).

1.2.2. Desarrollo de un módulo adicional, para determinados sistemas operativos de teléfonos celulares, tal que impida la sustracción / copia mencionada en el párrafo anterior.

1.2.3. Desarrollo de otro módulo adicional, para determinados sistemas operativos de teléfonos celulares, que, cuando se produzca un intento de sustracción / copia de la lista de contactos, le advierta tal anomalía al usuario indicando la URL de la computadora que realizó tal intento.

1.3. Tesis de Maestría de Pablo García: El alumno graduado de la Maestría en Ingeniería de Software de la Universidad Nacional de San Luis Pablo García desarrolló un enfoque algorítmico que incrementó significativamente las condiciones de confidencialidad del sistema de voto electrónico (extranjero). Los avances de Pablo García pueden ser utilizados en el contexto de la Defensa Cibernética.

1.4. Tesis Doctoral de Mario Berón: El Dr. Mario Berón ha realizado un muy valioso aporte a la Ingeniería Reversa a nivel programa y a la "comprensión" del funcionamiento y prestaciones de software del que se carece de su documentación de diseño

1.5. Convocatoria de ENIGMA: Integrantes del proyecto "*Ingeniería de Software: Aspectos de alta sensibilidad en el ejercicio de la profesión de Ingeniero de Software"* han sido invitados a desempeñarse como evaluadores de los trabajos que se presenten a "ENIGMA" The Brazilian Journal of Cryptography and Information Security, publicación científica auspiciada por el Ministerio de Defensa de Brasil

1.6. Un incidente en el Parque Industrial: Se contactó, a fines del año pasado, con el Gerente de una Planta de Tratamiento de Efluentes de una importante industria. De estudiado surgió que dicha Planta de Tratamientos de Efluentes había sido atacada (los PLC de la misma) mediante

un malware del mismo tipo del utilizado en el ataque a las instalaciones iraníes de Natanz. Esto no es extraño pues está casi verificada la existencia de un "mercado negro" de Ciberarmas. http://www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html

1.7. Posibilitar al LaCIS el Análisis de Flujos de Redes: El Laboratorio de Calidad e Ingeniería de Software del Área Metodologías y Programación del Departamento Informática de la UNSL tiene por objetivo promover la transferencia tecnológica y la asistencia técnica al entorno productivo. Un aspecto esencial que deberá encarar también el LaCIS es el de capacitar a Equipos de Respuesta a Incidentes en el Ciberespacio en lo que hace a la capacidad de detectar Botnet(s) y "Command and Control Servers" mediante "Análisis de Flujo de Redes". Se han adoptado previsiones en el sentido señalado.

1.8. Asistencia al Ministerio de Defensa – Estado Mayor Conjunto de las Fuerzas Armadas de Argentina en el Planeamiento Estratégico de la Defensa Cibernética de Argentina: Integrantes de esta línea de investigación están materializando esta asistencia en el momento de la elaboración de este documento. Marzo de 2013.

1.9. Una síntesis de la ideas desarrolladas en las actividades detalladas más arriba se plasmó en un "paper" titulado "Trust in Cyberspace: New Information Security Paradigm" el cual fue presentado en la Conferencia IEEE que se realizará los días 22 y 23 de marzo de 2013 en Hangzhou, China. El trabajo ya fue aceptado por el Comité de Programa (arbitraje internacional mediante)

2. Ejes de la nueva línea de investigación

Ingeniería Reversa a nivel programa, Criptografía y criptoanálisis, Detección de malware inmune a los productos "anti malware" de disponibilidad comercial, Análisis de Flujo de Redes, Enfoques innovadores en Auditoría de Seguridad Informática

3. Objetivos y resultados esperados

3.1. Ingeniería Reversa a nivel programa: Lograr la Ingeniería Reversa, partiendo de lenguaje de máquina, de productos de software elaborados con un enfoque multiparadigna.

3.2. Criptografía y criptoanálisis: Desarrollar herramientas de criptografía y criptoanálisis de alto rendimiento con "know how" propio.

3.3. Detección de malware inmune a los productos "anti malware" de disponibilidad comercial: Desarrollar los conceptos y herramientas correspondientes.

3.4. Análisis de Flujo de Redes: Desarrollar herramientas de alta efectividad.

3.5. Enfoques innovadores en Auditoría de Seguridad Informática: Proponer el perfeccionamiento de los estándares actualmente vigentes (del tipo ISO 27001 / 27002)

4. Formación de Recursos Humanos

Además de la Tesis doctoral de Mario Berón, la Tesis de Maestría de Pablo García y la Tesis de Maestría de Walter Agüero, está estudiándose la viabilidad de elaboración de nuevas tesis doctorales y nuevas tesis de maestría, abordando temas relacionados con la Defensa Cibernética, a ser encaradas en el futuro próximo. También se está poniendo un particular énfasis en el desarrollo de temas de Seguridad Informática en el contexto del Doctorado en Ingeniería Informática, de las Maestrías en Ingeniería de Software y Calidad del Software y en la Especialización en Ingeniería de Software. Asimismo se está

negociando la posibilidad de que la UNSL se haga cargo de la capacitación en Defensa Cibernética de personal del Ministerio de Defensa de Argentina. El equipo inicial de la línea de investigación que se inicia está constituido por el Dr. Roberto Uzal, el Dr. Jeroen van de Graaf1, el Dr. Germán Montejano, el Dr. Daniel Riesco, el Dr. Mario Berón y el Lic. Pablo García (tesis de maestría ya elaborada).

5. Referencias

[1]. http://www.sel.unsl.edu.ar/
[2]. http://webfmn.unsl.edu.ar/boletines/boletin416/noticia5-brasil.htm
[3]. Richard Clarke, “Cyber War”, Harper Collins, 2010
[4]. http://www.eluniverso.com/2009/11/12/1/1361/apagon-brasil-genera-temores.html
[5]. Wall Street Journal, June 15, 2011
[6]. http://www.youtube.com/watch?v=XgnRvcntfdo
[7]. http://www.nytimes.com/2012/06/06/books/confront-and-conceal-by-david-sanger.html?_r=0&adxnnl=1&adxnnlx=1362427401-0atlzUnTtJgjKOpj6e1Qvw
[8]. http://www.youtube.com/watch?v=EvP_x09cfU0
[9]. http://www.in.gov.br/visualiza/index.jsp?data=27/12/2012&jornal=1&pagina=11&totalArquivos=304
[10]. http://www.defesanet.com.br/cyberwar/noticia/5954/CDCiber---Centro-de-Defesa-Cibernetica-inicia-em-Junho-
[11]. http://revistaepoca.globo.com/Revista/Epoca/0,,EMI249428-15223,00-GENERAL+JOSE+CARLOS+DOS+SANTOS+PODEMOS+RECRUTAR+HACKERS.html
[12]. http://www.eluniverso.com/2009/11/12/1/1361/apagon-brasil-genera-temores.html
[13]. http://cespe.espe.edu.ec/2012/10/page/2/
[14]. http://sseguranca.blogspot.com.br/2012/12/politica-cibernetica-de-defesa.html
[15]. Berón M. y Henriques P. y Varanda Pereira M. y Uzal R.; “Comprensión de programas”; XI Workshop de Investigadores en Ciencias de la Computación., 1, 2009, ISBN: 978-950-605-570-7
[16]. R. Berón M. y Henriques P. y Varanda M. y Uzal R.” Inspección de código para relacionar los dominios del problema y programa para la comprensión de programas”. X Workshop de Investigadores en Ciencias de la Computación., 1:549–553, 2008
[17]. Beron M. y Cruz D. y Pereira M. y Henriques P. y Uzal R. “Evaluation criteria of software visualization system used for program comprehension”, 3a Conferencia Nacional em Interacção Pessoa-Máquina, 3:81–86, 2008. Estado: Publicado. Editorial: Universidade de Évora. ISBN: 972-9464-9-9.
[18]. Berón M. y Henriques P. y Varanda Pereira M. y Uzal R.; “Simplificando la comprensión de programas a través de la interconexión de dominios”. XIV Congreso Argentino de Ciencias de la Computación., 1, 2008. Estado: Publicado. Editorial: Universidad Nacional de la Rioja. ISBN: 978-987-24611-0-2.
[19]. http://www.sba-research.org/wp-content/uploads/publications/acsac12_disclosure.pdf
[20]. http://www.cert.org V. Krmícek, T. Plesník Detecting Botnets with NetFlow FloCon 2011, January 12, Salt Lake City, Utah
[21]. http://www.atlantis-press.com/publications/aisr/iccsee-13/index_iccsee-13.html?http%3A//www.atlantis-press.com/php/paper-details.php%3Fid%3D4471
[22]. http://news.bbc.co.uk/2/hi/europe/6665145.stm
[23]. http://www.defensenews.com/article/20111028/DEFSECT01/110280301/Report-Cyber-Attacks-Targeted-U-S-Satellites
[24]. http://www.foxnews.com/scitech/2012/03/01/chinese-hackers-nasa-jpl-lab/
[25]. http://www.dailymail.co.uk/news/article-2178781/Iran-nuclear-facilities-hit-cyber-attack-plays-AC-DCs-Thunderstruck-volume.html
[26]. http://www.reuters.com/article/2013/02/26/us-cyberwar-stuxnet-idUSBRE91P0PP20130226
[27]. http://www.youtube.com/watch?v=vrRj-kRofRg (documental de la TV Iraní)
[28]. http://cyberleaks.org/the-cyber-war-still-continues-between-india-and-pakistan-since-1954-a-report/
[29]. http://www.indianexpress.com/news/cyber-war-blaming-pakistan -is-not-enough/990637