Andorra La Vella, 7 de julio 2015
ISBN: 978-99920-70-09-3

La enseñanza de la Ciberseguridad en el Grado en Ingeniería Informática

José Ant. Gómez Hernández
Departamento de Lenguajes y Sistemas Informáticos
Universidad de Granada
Granada
jagomez@ugr.es

Resumen

La Ciberseguridad es un bien a proteger dado su impacto a nivel político, social, económico e individual. Una parte importante la misma descansa en la construcción y usos seguros de los sistemas informáticos.

Sería necesario que todos nuestros graduados adquieran unos conocimientos básicos relativos a seguridad para abordar su trabajo profesional con la responsabilidad necesaria y bajo los estándares reconocidos.

El posicionamiento de la ponencia es que para prevenir los problemas más frecuentes de seguridad es necesario ligar la enseñanza de la tecnología junto con la forma segura de uso. Esto significaría que debemos, no solo incluir aspectos de seguridad informática en materias específicas, si no que además debemos incluir conocimientos de seguridad en otras materias básicas de cara a construir sistemas seguros que generen confianza en los consumidores.

Por supuesto, el punto más conflictivo es establecer un equilibrio entre los contenidos propios de una materia y su uso de forma segura.

Abstract

Cybersecurity is an asset to protect given their impact on the political, social, economic and individual levels. An important part of it rests on the construction and secure use of computer systems.

It's important that all our graduates acquire basic knowledge on security to address their professional work with the necessary responsibility and under recognized standards..

This paper states that to prevent the most common security issues is necessary to link the teaching of technology along with the secure use. This would mean that we should not only include aspects of security in specific subjects, but it also must include security elements in other basic subjects in order to build secure systems that generate consumer confidence.

Of course, the most controversial point is to establish a balance between the own contents of a subject and the secure elements inserted.

Palabras clave

Ciberseguridad, cibercrímenes, enseñanza.

1. Motivación

La Ciberseguridad es un bien a proteger dado su impacto a nivel político, social, económico tanto a nivel de estados u organizaciones como individual. Gran parte de nuestro mundo descansa en la construcción y usos seguros de los sistemas informáticos sobre los que realiza una amplia variedad de actividades cotidianas, especialmente en países desarrollados tecnológicamente.

En este sentido, comentar algunas cifras para ver la magnitud del problema. En [10] para 2014 se estima el coste del cibercrimen en 400.000 millones de dolares, lo que supone entre un 15% y un 20% del dinero que se mueve en Internet. Las principales causas de esta brutales perdidas provienen de [9]: el 68,32 % debido a *phishing*, un 66,48% a *malware*, el 50.14% por intentos de hacking, un 43,54% por ingeniería social, un 43,89% por perdida de dispositivos móviles, 25,28% de los trabajadores (*insiders*), 21,88% de Inyección SQL, etc.

No solo hay que tener en consideración los aspectos económico, sino también sociales y personales. Por ejemplo, va en aumento delitos como el ciberacoso o el *sexting*, que afectan especialmente a nuestros jóvenes, parte de cuya solución pasa por una educación en seguridad, la construcción de sistemas y herramientas destinadas a evitarlos. Sin dejar de mencionar aspectos estratégicos relacionados con ataques a infraestructuras críticas, o que afectan a la privacidad como las brechas de datos (últimamente crecientes en número y volumen).

En España este fenómeno también es creciente tal como podemos ver el primer informe sobre Cibercri-

Andorra La Vella, 7 de julio 2015
ISBN: 978-99920-70-09-3

minalidad presentado por el Ministerio del Interior [11]. Además, hay que resaltar que el número de ataques sufridos por España en 2014 fue de 70.000 lo que nos posiciona en tercer lugar tras EEUU y Reino Unido [6] . Debemos resaltar que un 95% de estos delitos [5] quedan impunes por diferentes causas: no son denunciados, o encuentra problemas tecnológicos y/o legales.

Como podemos ver, el incremento y volumen del cibercrimen son lo suficientemente grandes como para no abordar el problema con rapidez y contundencia. En especial, si deseamos consolidar el uso de las Nuevas Tecnología por la mayoría de la población. Como se indica en [4], solo un 53% de los usuarios de Internet declaran que compran bienes o servicios *online*, un 48% realiza operaciones bancarias en línea, y el 20% vende bienes o servicios. Este aspecto también esta reconocido por su importancia en la Estrategia de Ciberseguridad Nacional [12].

La estructura de la ponencia aborda en el Apartado 2 cómo ha quedado la enseñanza de la Seguridad en los Grados de Ingeniería Informática en España y, especialmente, en la Universidad de Granada. En el Apartado 3, se presenta y justifica una propuesta de mejora para solucionar algunos problemas. En el Apartado 4, se verán algunos ejemplos concretos de asignaturas afectadas por la propuesta. Para terminar con un resumen de la propuesta realiza en la ponencia.

2. La enseñanza de la seguridad

2.1. La seguridad en los Grados en Informática

Todos leímos en su momento multitud de veces el BOE 187/2009 [2] que establece la recomendaciones para la solicitud de títulos de Ingeniería Informática. En el Apartado 3 del Anexo I, se relacionan las competencias que todos los estudiantes deben adquirir, entre las que aparece " Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y **seguridad** de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan". Volviendo a aparecer el término "seguridad" tanto en el módulo de rama como en los de especialización.

He marcado en negrita el elemento que desde mi punto de vista se ha reflejado de manera insuficiente en el plan de estudios de Grado en Ingeniería Informática en la Universidad de Granada, y posiblemente en otros, como trataré de justificar en breve.

Para la adquisición de competencias relacionadas con la Ciberseguridad se ha optado por incluir cierto número de asignaturas dedicadas al tema en todos los planes de estudio, tal como se puede ver el en magnífico trabajo de Ramió [14] a través del proyecto MESI.

Si bien la situación de la enseñanza de la Seguridad ha mejorado respecto de los planes de estudios anteriores, es actualmente a todas luces insuficiente, máxime cuando en algunos casos estas asignaturas son bien optativas, bien troncales pero solo se cursan en alguna mención concreta y, por tanto, no es vista por todos los alumnos del título.

En [13] se propone la creación de una titulación propia en seguridad para la formación de profesionales en esta materia. Desde mi punto de vista esta propuesta es muy interesante pero solo cubre una parte del problema. La seguridad informática no es solo cuestión de profesionales de la seguridad, es algo que nos afecta a todos los que usamos y/o construimos software. Por tanto, debemos buscar una solución que permita cubrir unas competencias básicas en seguridad a todos los alumnos de nuestros grados.

2.2. La docencia de la seguridad en el Grado de Ingeniería Informática de Granada

En el caso concreto del Grado en Ingeniería Informática de la Universidad de Granada, se pasa a comentar que asignaturas específicas sobre Seguridad se establecieron así como una breve descripción de sus contenidos.

Seguridad y Protección de Sistemas Informáticos obligatoria en la mención de Tecnologías de la Información. Esta dedicada en gran parte a la criptografía, si bien cubre algunos aspectos de seguridad en redes y comunicaciones, identidad digital, privacidad en Internet y comercio electrónico.

Seguridad en Sistemas Operativos optativa de la mención de Ingeniería del Software. Asignatura que imparto, se diseño para completar la parte de seguridad vista en la asignatura de Sistemas Operativos de segundo curso. Además, trata cubrir otros aspectos de la seguridad que los estudiante de la mención de Ingeniería del Software no ha visto, como son: desarrollo de software seguro, *malware*, informática forense.

Criptografía y Computación optativa en la mención de Computación y Sistemas Inteligentes. Como su propio nombre indica aborda los aspectos de cifrado de la información

Además, también deben incluirse los contenidos de seguridad de la asignatura de *Sistemas Operativos* que suelen incluirse en cursos básicos sobre la materia, como son básicamente autorización y control de acceso.

A la luz de lo indicado, es notorio que no hay una asignatura específica de seguridad básica que cursen todos los estudiantes del Grado y que exponga la complejidad y amplitud del tema.

A continuación trataré de esbozar una propuesta que cubra de manera razonable estas deficiencias en

Andorra La Vella, 7 de julio 2015
ISBN: 978-99920-70-09-3

seguridad y que tenga una implementación flexible dentro de los diferentes marcos curriculares establecidos.

3. Una propuesta de mejora

La propuesta que se presenta esta destinada, como comentábamos en los párrafos anteriores, a que todos nuestros estudiantes alcancen una competencias básicas de seguridad necesarias para construir sistemas software seguros tal como demanda la sociedad.

Esta propuesta trata de alcanzar este objetivo sin necesidad de hacer una reforma del plan de estudios para incluir nuevas asignaturas. Reforma que sería costosa, compleja y tardaría en poder aplicarse. Además esta propuesta no es incompatible, al contrario complementaria, de la situación actual donde hay asignaturas específicas de seguridad en las diferentes menciones, o con la implantación de un título propio en seguridad.

Se trata de plantear una serie de competencias básicas de seguridad como competencias transversales de forma que se cubran en asignaturas ya existentes (en lugar de pretender crear nuevas asignaturas). Es decir, dedicar parte los contenidos de asignaturas ya existentes a abordar aspectos básicos de seguridad. Esto el algo que en algunos caso ya se hace parcialmente pero que habría que potenciar y coordinar.

Es evidente que esto presenta un problema en el que ya habrá pensado el lector: cómo incluyo competencias nuevas en asignaturas que ya de por sí esta sobrecargadas. Las respuesta no es ni sencilla, ni única. Es evidente que supone un gran esfuerzo de coordinación a nivel de título en que debemos valorar que equilibrio en la formación de nuestro estudiantes damos a dos aspectos contrapuestos en muchos casos: inclusión de conceptos/tecnologías avanzados frente a conceptos/tecnologías que hagan más seguros los sistemas que pretendemos construir.

Como es evidente y pretendía dejar manifiesto en la Introducción de la ponencia, mi postura es que en general considero necesario sacrificar la inclusión de algunos avances tecnológicos para facilitar la inclusión de elementos de seguridad. A menudo vemos como las empresas en una veloz carrera por ofrecer nuevas soluciones tecnológicas de cara a abarcar cuotas de mercado dejan atrás aspectos de seguridad, lo que tiene consecuencias nefastas. El grado de penetración de competencias de seguridad en las asignaturas dependerá del grado de sensibilización del profesorado hacia el tema sin dejar atrás las competencias legales establecidas para las asignaturas que en la mayoría de los casos hemos aumentado para cubrir la carga crediticia.

Evidentemente, no se trata de que todos los alumnos sean profesionales de la Seguridad Informática, pero si que conozcan, se sensibilicen y sean capaces de abordar los problemas que se producen al no tenerla en cuenta. Esto les permitirá eliminar de entrada determinados defectos de sus construcciones software y facilitar la comunicación en equipos multidisciplinares con profesionales de la seguridad.

La propuesta que podemos resumir como “debemos ligar la enseñanza de la tecnología con su uso de forma segura”. Este lema ser extrapolable a todos los niveles docentes donde se enseñe tecnología. Por ejemplo, deberíamos enseñar a nuestros adolescentes no solo a utilizar un navegador, sino a utilizar *de forma segura* un navegador. Lo mismo sería aplicable al uso seguro de redes sociales, dispositivos móviles, etc.

A nivel universitario, esta propuesta se alinea con trabajos previos como [7, 8, 16], donde se realizan diferentes propuestas de integrar la Seguridad en el currículum, pero que desgraciadamente no son muy numerosas ni parecen haber arraigado lo suficiente.

Otro elemento importante, una vez concienciados de la necesidad de incluir competencias de seguridad en nuestras asignaturas, es: en qué sentido debo modificar mi asignatura para incluir dichas competencias.

Para responder a esta cuestión, tendríamos dos líneas de actuación. La primera enfocada al desarrollo y construcción de software seguro, que afectaría a las asignaturas relacionadas con la programación e Ingeniería del Software. La segunda, desde el punto de vista de hacking, ver cuales son las amenazas más frecuentes y estudiar las soluciones para paliar o anular dichas amenazas. Vamos a dar, en el Apartado siguiente, ejemplos concretos de contenidos que debería abordarse en asignaturas ya establecidas y que actualmente se hacen de manera baja o nula, al menos en el Grado de la Universidad de Granada.

4. Asignaturas afectadas por la propuesta

Vaya por adelantado la aclaración de que algunos elementos de seguridad ya se ven el algunas asignaturas pero a veces no están sistematizados y dependen de la concienciación del profesor correspondiente. Por lo que la propuesta presentada va más en la línea de sistematizar contenidos y distribuir competencias.

Para ayudarnos en [3] podemos encontrar la lista de las 25 errores software más usuales que los programadores deberían mitigar o eliminar. Estos errores están agrupados en tres categorías (interacción insegura entre componentes, gestión arriesgada de recursos, y defensas porosas) que vamos a despiezar en función de las asignaturas en los que se podrían incluir.

Las primeras asignaturas sería las relacionadas con la Ingeniería del Software (como Fundamentos de Ingeniería del Software, de 2º curso), donde no se cubre

Andorra La Vella, 7 de julio 2015
ISBN: 978-99920-70-09-3

una metodología de desarrollo software que tenga en cuenta la seguridad como un requisito no funcional. En múltiples conversaciones con mis compañeros reconocen la necesidad pero me indican que no se materializa por falta de tiempo.

Las asignaturas básicas de programación (Fundamentos de Programación y Metodología de la Programación, de primer curso) son las candidatas naturales para introducir conceptos fundamentales de programación segura (o defensiva) destinados a eliminar vulnerabilidades en la etapa de codificación, como por ejemplo, desbordamiento de búfer.

Otras asignaturas afectadas derivadas de las principales amenazas en sistemas, son las asignaturas de programación web. Los sistemas web están expuestos a un elevado número de amenazas que el alumno debe conocer y saber paliar bien manualmente bien utilizando algún *framework* de desarrollo que lo haga.

Estas consideraciones pueden extenderse como ejemplos de prácticas a otras asignaturas, por ejemplo, de *Big Data* que nos pueden ayudar a procesar grandes volúmenes de información dispar con los algoritmos adecuado.

En los subapartados siguientes, vamos a desarrollar algunos de los aspectos anteriormente mencionados solo en las asignaturas que creo directamente afectadas.

4.1. Asignaturas de programación

En las asignaturas de programación se incluirían muchos de los elementos que caen en el segundo grupo de errores etiquetado con el nombre de "Gestión arriesgada de recursos" que incluiría los ítems: copia de búferes sin comprobar las entradas (*Buffer Overflow*), limitación inadecuada de un nombre de camino a un directorio restringido (Path traversal), uso de funciones potencialmente peligrosas, cálculo incorrecto del tamaño de un búfer, cadenas con formato incontrolado o desbordamiento de enteros.

Muchos de estos elementos se ven en las programación básicas por lo cual lo único que deberíamos hacer es darles consistencia y ligarlas con la seguridad del programa/sistema en construcción.

Quizás un elemento que debería incluirse es la utilización de alguna herramienta para el análisis estático del código resultante en los supuestos de programación. Esto se puede hacer como parte de las prácticas y no debería ser muy costoso en recursos.

4.2. Asignaturas de Ingeniería de Software

La mejor forma de evitar ataques (que no hacen más que aprovechar vulnerabilidades) es el desarrollo de software seguro desde sus inicios. Para ello es necesario el uso de una metodología de desarrollo software que contemple la seguridad desde sus inicios. Esta necesidad se recoge en [16], donde se describe la asignatura de Seguridad de Sistemas Software enmarcada dentro de la especialidad de Ingeniería del Software.

La propuesta citada es perfectamente válida para una especialización en desarrollo de software, pero responde a un enfoque diferente a adoptado en mi propuesta: no beneficiaría a todos los estudiantes del Grado y duplica una asignatura. Por tanto, la propuesta presentada, va en la dirección de tener la seguridad inmersa en las asignaturas básicas de Ingeniería del Software. Valga como ejemplo de la importancia de la construcción de software seguro el reciente y luctuoso accidente de un Airbus A400M debido a un problema de integración software.

Entre los contenidos básicos a incluir tendríamos el uso de una metodología segura y el uso de herramientas de análisis, verificación y prueba de software seguro. En estas asignaturas sería más costosa la integración pues supondría en muchos casos el cambio completo de metodología software utilizada y al que puedo imaginar mas reticencias por parte del profesorado. Creo que sin duda los beneficios en la seguridad del software que produzcan nuestros futuros estudiantes lo merece.

Se pueden incluir contenidos del grupo de "defensas porosas" de los 25 errores comunes del software entre los que se incluirían: perdida de autenticación en funciones críticas, perdida de autorización, falta de cifrado de datos sensibles, o asignación incorrecta de permisos para recursos críticos.

4.3. Asignaturas de desarrollo web

El grupo de "interacción insegura entre componentes" incluye mayoritariamente aspectos relacionados con el desarrollo web, a saber: neutralización inadecuada de elementos especiales en las órdenes SQL (*SQL injection*), neutralización inadecuada de entradas en la generación de páginas web (*Cross-site scripting*), carga sin restricciones de archivos con tipos peligrosos, falsificación de solicitudes cruzadas (*Cross-Site Request Forgecy* - CSRF), redirección de URLs a sitios no confiables, o exposición de información a través de mensajes de error.

También serían elementos potenciales a incluir, algunos de segundo grupo "gestión arriesgada de recursos", a saber, la descarga de código sin comprobación de integridad, y la inclusión de funcionalidad desde una esfera de control no confiable, por ejemplo, código móvil.

Es evidente la dificultad de incluir en dos o tres asignaturas de 6 créditos la descripción de todos los elementos citados, pero sería aconsejable que los alumnos al menos conociesen de que tratan y, al menos, cómo evitarlos en los casos más comunes. Ademas de tener presente que debería que trabajar con profesionales del tema cuando desarrolla aplicacio-

Andorra La Vella, 7 de julio 2015
ISBN: 978-99920-70-09-3

nes/sitio web de forma profesional. Desgraciadamente me he encontrado con algún alumno en la asignatura de Seguridad que imparto en cuarto curso, que estaba haciendo el desarrollo de sitio web con acceso a una base de datos para una organización y estos términos tan siquiera le sonaban.

Aquí es también posible una distribución de contenidos entres las numerosas asignaturas sobre desarrollo web incluidas en los nuevos planes. Por otro lado, en las prácticas de estas asignaturas se pueden plantear proyectos conjuntos con otras asignatura, como la que imparto de Seguridad en Sistemas Operativos, para realizar teste de penetración de sitios web, por ejemplo.

4.4. Asignaturas de sistemas operativos

Tradicionalmente, las asignaturas generales de sistemas operativos suelen incluir algún tema teórico de seguridad, que incluye una introducción a la misma, y suele centrarse generalmente en aspectos de autentificación y control de acceso.

A esto puntos, habría que añadir algunos elementos fundamentales y que no son muy difíciles de alcanzar ya que se pueden incluir de manera natural en las prácticas de la asignatura. Me refiero a la gestión de actualizaciones del sistema operativo y las aplicaciones, la gestión de listas blancas (*white lists*), y restricción de privilegios de administrador a los usuarios que lo necesitan. Estos elementos aseguran una reducción del orden del 70% en la presencia de amenazas, tal como se indica en [1].

Estos elementos pueden completarse, en la medida que el temario práctico lo permita en la parte de administración del sistema con gestión de copias de seguridad (una medida contra el *ransomware*), y endurecimiento del sistema operativo (*OS hardening* como medida para reducir el frontera de ataque).

5. Conclusiones

Puesta de manifiesto la importancia creciente de la construcción de sistemas informáticos seguros de cara a satisfacer las necesidades presentes y futuras de la Sociedad de la Información, se ha pretendido concienciar la necesidad de una formación básica en materia de ciberseguridad para todos los estudiantes del Grado en Informática.

Además, se propone un modelo que permitiría incluir competencias de seguridad en los actuales planes de estudios de forma transversal sin necesidad de una modificación estructural de los mismos, sino que afecta al diseño de contenido de asignaturas ya existente.

También se ha puesto de manifiesto como este modelo depende de una coordinación transversal de los contenidos que si bien exige esfuerzo por parte del profesorado es fácilmente modularizable para separar dichas competencias en asignaturas y cuyo resultado sería la formación profesionales concienciados con la construcción de sistemas seguros.

Referencias

[1] Australian Defence Signals Directorate (DSD), *Strategies to Mitigate Targeted Cyber Instrusions – Mitigation Details*, Oct. 2012.

[2] BOE, resolución de 8 de junio de 2009 de la Secretaría General de Universidades, nº 187 de 2009, 4 Agosto de 2009.

[3] Steve Chistey (Ed.), *CWE/SANS Top 25 Most Dangerous Software Errors*, Common Weakness Enumeration, Sep. 2011.

[4] Comisión Europea, "Ciberdelincuencia: Los ciudadanos de la UE, preocupados por la seguridad de la información personal y los pagos en línea". Bruselas 9/6/2012. http://europa.eu/rapid/press-release_IP-12-751_es.htm?locale=en.

[5] Jesús Duva, "El 95% de los ciberdelitos cometidos quedan impunes", El País, 4/5/2014. http://politica.elpais.com/politica/2014/05/03/actualidad/1399117342_852720.html.

[6] Europa Press, "España sufrió más de 70000 ataques cibernéticos, la cifras más alta tras EEUU y Reino Unido", Madrid, 5/2/2014. http://www.europapress.es/nacional/noticia-espana-sufrio-2014-mas-70000-ataques-ciberneticos-cifra-mas-alta-eeuu-re-20150205115531.html.

[7] Trudy Howles, Carol Romanowski, Sumita Mishra y Rajendra K. Raj, "A Holistic, Modular Approach to Infuse Cyber Security into Undergraduate Computing Degree Programs", *Annual Symposium on Information Assurance (ASIA 2011)*, Albany NY, June 2011.

[8] Cynthia E. Irvine, Shiu-Kai Chin, y Deborah Frincke, "Integrating Security into the Curriculum" (1998). Electrical Engineering and Computer Science. Paper 84. http://surface.syr.edu/eecs/84.

[9] ISACA, State of Cybersecurity: Implications for 2015. An ISACA and RSA Conference Survey, RSA Conference, 2015. http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf.

[10] McAfee, Net Losses: Estimating the Global Cost of Cybercrime. Economic impact of cybercrime II , McAfee, Junio de 2014. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

[11] Ministerio del Interior, "Avance de los datos estadísticos de 2013 relativos a la cibercriminalidad" , 2013.

Andorra La Vella, 7 de julio 2015
ISBN: 978-99920-70-09-3

http://www.interior.gob.es/prensa/balances-e-informes/2013.

[12] Presidencia de Gobierno, *Esquema de Ciberseguridad Nacional*, Gobieno de España 2013. http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf.

[13] Jorge Ramió, "Introducción de las Enseñanzas de Seguridad Informática en los Planes de Estudio de las Ingenierías del Siglo XXI", JENUI 2001.

[14] Jorge Ramió, Informe gráfico de la tesis doctoral "La enseñanza universitaria en seguridad TIC como elemento dinamizador de la cultura y la aportación de confianza en la sociedad de la información en España". León, 12 de diciembre de 2013. http://www.criptored.upm.es/guiateoria/gt_m001i1.htm.

[15] David G. Rosado, Carlos Blanco, Luis Enrique Sánchez, Eduardo Fernández-Medina, y Mario Piattini, "La Seguridad como una asignatura indispensable para un Ingeniero del Software", JENUI 2010, pgs. 205-212. http://upcommons.upc.edu/revistes/bitstream/2099/11778/1/a25.pdf.

[16] Blair Taylor, Harry Hochheiser, Shiva Azadegan, y Michael O'Leary, "Cross-site Security Integration: Preliminary Experiences across Curricula and Institutions", P*roceedings of the 13th Colloquium for Information Systems Security Education, S*eattle, WA June 1- 3, 2009.

[17] Georgory White and Georgory Nordstrom. 1997. "Security across the curriculum: using computer security to teach computer science principles". En *Internet besieged*, Dorothy E. Denning and Peter J. Denning (Eds.). ACM Press/Addison-Wesley Publishing Co., New York, NY, USA 519-525.