INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. X , No. X, (mes, 2018) pp-pp ISSN 2550-6730

Recibido: –/–/—-
Aceptado: –/–/—-

La seguridad de la información: Un oscuro espacio multidimensional

Humberto Díaz-Pando[1,1] Miguel Rodríguez-Veliz[2,2] Yulier Nuñez-Musa[3,3] Roberto Sepúlveda-Lima[1,4]

[1]Departamento de Inteligencia Artificial e Infraestructura de Sistemas Informáticos, Universidad Tecnológica de la Habana "José Antonio Echeverría", La Habana, Cuba. [2]Departamento de Informática y Electrónica, Universidad Técnica de Manabí (UTM), Portoviejo, Ecuador. [3]Departamento de Informática, Universidad Agraria de La Habana "Fructuoso Rodríguez Pérez", San José de Las Lajas, Cuba.
[1]hdiazp@ceis.cujae.edu.cu, [2]mjrodriguez@utm.edu.cu, [3]yuliernm@unah.edu.cu, [4]sepulveda@mes.gob.cu

RESUMEN

This paper presents the dimentions that defines the Information Security essentials from the authors point of view and their experience on studying Cryptography, Steganography, controls for data integrity and executable components, reverse engineering attacks, information systems auditing and a set of researching related with solving these problems. A critical focusing is applied for expressing the perception that a considerable portion of computer science community has about these dimentions. Some advances related with software tamper resistance and code obfuscation techniques are discussed.

El artículo presenta las dimensiones que definen los elementos esenciales de la Seguridad de la Información desde el punto de vista de los autores y su experiencia en el estudio de la criptografía, la esteganografía, los controles de integridad de datos y componentes ejecutables, ataques de ingeniería inversa, la auditoría de sistemas de información y un conjunto de investigaciones relacionadas con la solución de estos problemas. Se discute con enfoque crítico la percepción que sobre estas dimensiones exhibe una parte considerable de la comunidad relacionada con el desarrollo de soluciones informáticas y se enuncian algunos avances en la obtención de software resistente a modificaciones y a la aplicación de técnicas de ofuscación de códigos.

PALABRAS CLAVES: plataforma, procesamiento de electrooculogramas, SCA2.

1. Introducción

La problemática asociada con la seguridad de la información, parece mantenerse en una discusión de segundo orden en la mayor parte de los ambientes de explotación y desarrollo de tecnologías, componentes y aplicaciones.

Existe más de una razón concreta que puede explicar este arriesgado comportamiento, que va desde el desconocimiento a profundidad de las amenazas a las que se enfrentan las tecnologías del presente hasta la ingenuidad al concebir soluciones de seguridad poco fundamentadas y probadas, pasando por la desestimación consciente del tema.

No parece haberse establecido un conjunto de posiciones y buenas prácticas que permitan comprender y actuar con la celeridad requerida ante la explotación de vulnerabilidades de seguridad por parte de los atacantes.

El acercamiento desde la óptica conceptual a las dimensiones que constituyen la seguridad, un espacio insuficientemente explorado y en muchos casos oscuro, parece imprescindible para asimilar situaciones específicas y comprender el carácter esencial que deben exhibir las soluciones de seguridad.

En este trabajo, se reiteran algunos atributos y dimensiones de la seguridad con la pretensión de establecer consideraciones sobre los mismos y hacia donde se han dirigido los trabajos realizados por los autores con relación a este medular aspecto.

2. Las dimensiones de la seguridad de la información

Aunque existen varias denominaciones y definiciones relacionadas con la seguridad de la información, y muchas consideraciones en mayor o menor detalle, es posible realizar señalamientos críticos, interpretaciones y refinamientos que completen éstas, matizadas muchas veces por el espacio o medios específicos hacia el que se enfoca el interés, ya sea el almacenamiento, la transmisión o el intercambio de la información. Probablemente, este sea uno de los problemas de la actualidad que está a la espera de una mejor definición [1, 2, 3].

Dentro de la lógica de la diversidad de enfoques y definiciones, se considera más oportuno comprender las esencialidades y apostar por un enfoque general y una visión conceptual que permita avanzar hacia una cultura flexible y escalable hacia la comprensión de un fenómeno en el que los atacantes parecen haber ganado terreno a las buenas intenciones de los diseñadores de controles de seguridad.

En ese orden de cosas, es común considerar que la seguridad de la información se define sobre cinco atributos o dimensiones que son: la integridad, la autenticación, la confidencialidad, el no repudio y la disponibilidad [1, 2]. Se considera necesario en coincidencia con [3], adicionar como atributo indispensable y complementario a los anteriores el de la auditabilidad.

De una forma u otra se reportan avances en las últimas décadas a aproximaciones conceptuales y de implementación en todas estas dimensiones. Sin embargo, al pretender efectuar un análisis que explique el éxito de determinados ataques, se detectan flagrantes violaciones u omisiones al aplicar determinados controles de seguridad o al definir una solución de seguridad de carácter integral.

2.1. La dimensión de la integridad

La integridad [4], es quizás el atributo más estudiado y antiguo. Contradictoriamente, parece ser el más olvidado y probablemente constituye la parte más sólida del hormigón armado sobre el que se establece un esquema de seguridad robusto.

La dimensión de la integridad aspira a colocar controles específicos que permitan detectar o corregir, cualquier cambio en la composición de la información que se almacena o transmite. Existe una marcada tendencia a relacionarse con los datos o paquetes de información, pero es de radical importancia aplicarla a las componentes de software, ya sean ejecutables, archivos complementarios y cualquier otro objeto susceptible de ser atacado y modificado, dado que el atacante siempre estudiará la componente más vulnerable y este será su principal objetivo.

Los autores han realizado alguna experimentación sobre el tema [5] y realizado ataques de ingeniería inversa sobre componentes de software donde han lamentables omisiones de adecuados controles de integridad presentes aún en sistemas operativos comerciales.

Existe más de un mecanismo adecuado para aplicar controles de integridad entre los que se encuentran los controles de redundancia cíclica (CRC) [6] y las funciones de hash [7, 8].

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. X , No. X, (mes, 2018) pp-pp ISSN 2550-6730

2.2. La dimensión de la confidencialidad

La confidencialidad o secreto [9] es una dimensión que produce controles que puedan ser robustos a partir del presupuesto de que la información a ser atacada puede caer siempre en poder de los interceptores. La confidencialidad se alcanza, generalmente, por medio de la Criptografía [1], la Esteganografía [10], la Ofuscación de códigos [11] o la combinación de estas técnicas.

En el primer caso, la Criptografía se fundamenta en aplicar algoritmos y transformaciones matemáticas complejas a nivel binario que consigan transformar un texto claro en una componente extraordinariamente confusa e ilegible. En general, se admite que el conocimiento de los algoritmos criptográficos e incluso de los códigos fuentes de los programas correspondientes, no aporta elementos que permitan la decodificación exitosa de los textos cifrados interceptados y que solo el descubrimiento de la clave o de un segmento de esta, una vulnerabilidad o falla encontrada o provocada al programa podría contribuir al descubrimiento del texto claro.

La Esteganografía, oculta en documentos inocuos, tales como imágenes, audio o vídeo, información de carácter sensible que únicamente se puede recuperar con conocimiento de aspectos específicos que se mantienen en celoso secreto por el emisor y el receptor del documento correspondiente.

De igual manera, la ofuscación de códigos intenta romper las estructuras clásicas de los datos, del control ya sea en el interior de una función ejecutable o en el grafo de control de llamadas, retardandado el éxito de una acción de ingeniería inversa por parte de un atacante, ya sea en el medio de almacenamiento o de manera dinámica mientras se ejecuta el programa.

Si se combinan de manera coherentes estas técnicas, es fácil deducir, que la recuperación de una componente codificada (ilegible) que se oculta en un documento aparentemente inocuo, traerá consigo una decodificación muy compleja del texto claro que se codifica y oculta. Si se trata de una componente ejecutable, será mucho más difícil decodificar su semántica por medio de un ataque de ingeniería inversa.

Sobre estas técnicas, se establecen controles de distribución y comercialización y aunque hay alguna tendencia a elaborar algoritmos propietarios para garantizar la confidencialidad, es natural apostar por la aplicación de estándares profesionales validados por una amplia comunidad de expertos.

2.3. La dimensión de la autenticación

La autenticación de los usuarios, componentes y aplicaciones [12] que intercambian información o se comunican en un ambiente tecnológico específico es determinante para materializar un nivel confortable de seguridad. Para su materialización confluyen las dimensiones de la confidencialidad y de la integridad, fundamentalmente.

Es obvio que, por ejemplo, recibir y decodificar un paquete de información sensible conformado por un emisor al que no se ha verificado con el rigor requerido su identidad, podría introducir graves fallas en la seguridad del intercambio. Similar situación implica entregar información a un receptor al que no se le ha validado correctamente.

Aunque existe más de una solución para realizar la autenticación, presentándose una tendencia bastante marcada a aplicar para ello, los certificados y firmas digitales, y las infraestructuras de claves públicas [13], sobre protocolos de intercambio que emplean controles de integridad, combinados con dispositivos físicos para la identidad, como tarjetas inteligentes y otros medios físicos y biométricos.

Es importante brindarle valor a la autenticación mutua, es decir, tanto emisor como receptor deben ser reconocidos entre sí.

2.4. La dimensión del no repudio

Quizás sea el no repudio [14] una dimensión que empieza a exigir más luz en el confuso espacio de la seguridad de la información.

Los intercambios de hoy y del futuro, necesitarán el sustento de una base absolutamente segura de que, una vez que se ha conformado el intercambio con garantía de los controles de integridad, confidencialidad y autenticación necesarios, ninguna de las partes pueda reclamar no haber sido parte de la transacción.

Analícese cuán grave sería si no se dispone de un mecanismo probatorio de que una extracción que deja vacía una cuenta bancaria, no ha sido realizado por la persona autorizada. Reanalícese el caso desde la posición de la entidad bancaria que recibe una reclamación y se determinará cuan simétrica, importante y compleja es la situación.

Para garantizar el no repudio, es necesario establecer, controles de tiempo, firmas digitales, y en muchos casos, terceras partes confiables, con infraestructuras tecnológicas y autoridad notarial o legal para dirimir posibles conflictos.

En esta dimensión, otra vez, se presenta una disquisición conceptual que se resuelve con enfoques de integración de un grupo de herramientas específicas y enfoques que aportan el resto de las dimensiones, entre ellas, la de la integridad, la autenticación y la confidencialidad.

2.5. La dimensión de la auditabilidad

El entorno actual parece no haber asimilado con claridad la importancia de la Auditoría de las Tecnologías y Sistemas Informáticos, aspecto que, a nuestro juicio, requiere de una reparación inmediata. En muchos momentos esta dimensión se trata como una componente adicional apartada del tema de la seguridad [14].

Al parecer hay una tendencia de profesionales del área de la auditoría clásica a asimilar conocimientos tecnológicos y desempeñarse en este espacio profesional, no siempre con el éxito esperado. En un menor grado se observan profesionales de Sistemas e Informática con intereses en el área de la Auditoría.

Como si fuera poco, los aspectos básicos de la auditoría y el cómo materializarla, no son tema de preocupación notable en los ambientes de desarrollo informático actual.

En muchas ocasiones, las funciones de auditar quedan radicadas en almacenar trazas (logs) de acceso y conexión a las componentes del sistema en archivos que gestionan terceras aplicaciones, como el sistema operativo, por ejemplo.

Estos archivos almacenados normalmente en texto claro y sin controles específicos de seguridad, definidos en las dimensiones de integridad, autenticación, confidencialidad y no repudio, pueden ser leídos y modificados muchas veces a través de herramientas y procedimientos triviales de ataques.

Más que pretender “auditar el sistema” habría que preguntarse ¿es auditable la infraestructura informática? Esta pregunta no tiene una respuesta precisa aún en el plano conceptual, pudiéndose granular una respuesta que incluya pistas controladas de acceso a menúes, secuencias de acciones o accesos a las bases de datos, hasta componentes autónomos de monitoreo que conviertan el conjunto en una colección con baja disponibilidad funcional.

Hacia lo interno de los desarrolladores de sistemas, existen escenarios en los que se omite conscientemente las funciones relacionadas con el auditor entre los casos de uso que documentan una solución informática segura y auditable. O peor aún, se colocan casos de uso para la auditoría para que sean iniciados y operados por el Administrador de Seguridad, convirtiéndose por decreto en el actor más capacitado-y autorizado-para atacar al sistema.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. X , No. X, (mes, 2018) pp-pp ISSN 2550-6730

El avance en la comprensión y concreción de la dimensión de la auditabilidad parece ser ínfimo. Los autores consideran que esta dimensión debe estructurarse a partir del resto de las dimensiones, es decir, se audita lo que previamente se planifica asegurar y según las evidencias que aporten los controles de integridad respectivos. Y en ese sentido sería muy arriesgado enfocar la auditoría como un concepto externo al de la seguridad de la información.

2.6. La dimensión de la disponibilidad

La disponibilidad tiene un enunciado simple, pero su carácter es altamente determinante y complejo.

Arreciar en el resto de las dimensiones de la seguridad, antes descritas, requiere de esfuerzo en la conceptualización de soluciones y en la implementación de algoritmos, controles y herramientas, por tanto, el presupuesto de que si se aumentan y perfeccionan los componentes para garantizar alta seguridad, se pueden comprometer de manera notable algunos parámetros de desempeño, se requiere de recursos adicionales almacenamiento, y crece el tiempo de ejecución del conjunto de componentes aseguradas [15].

Si para garantizar la seguridad que requiere el sistema, la aplicación de controles de seguridad cambia radicalmente los parámetros de funcionamiento, probablemente sea necesario desestimarla como aplicación. Si, por el contrario, ésta es altamente disponible a costa de presentar vulnerabilidades y ausencia de controles elementales en las dimensiones de seguridad discutidas, será fácilmente atacable.

En cualquier caso, ambos extremos introducen situaciones reprochables y la dimensión de la disponibilidad se constituye en un aspecto de compromiso. Lamentablemente está presente con mayor frecuencia la solución de alta disponibilidad y baja seguridad que su par complementario.

3. Aproximaciones a la solución de estos problemas

Los atributos o dimensiones de la seguridad antes descritos pueden ser comprometidos por un atacante, haciéndose valer para ello de distintas técnicas y herramientas. La forma en que son llevados a cabo los ataques a los sistemas puede variar según el contexto donde es efectuado. Main [16] clasifica los ataques a través de dos modelos de amenazas (*threat model*) determinado por el contexto de ataque.

En un primer modelo de amenaza, los ataques son efectuados de forma remota a través de la red (network threat model) mediante la explotación de posibles vulnerabilidades presentes en aplicaciones. En este modelo, las aplicaciones son ejecutadas en un ambiente seguro (trusted host) e inaccesible para un atacante de forma local. Entre las vulnerabilidades más comunes se encuentra el desbordamiento de buffer [17], inyección SQL [18], cross-site scripting [19], etc. Los objetivos fundamentales de estos ataques son la obtención de privilegios y manipulación de equipos remotos con diversos fines (acceso a información restringida, denegación de servicios, etc.).

En el segundo modelo de amenaza, los ataques se realizan de forma local en la propia máquina donde ocurre la ejecución de la aplicación (*untrusted host threat model*). Bajo este modelo, el ambiente de ejecución de la aplicación se considera no confiable (*Untrusted Host*) [19], pues el atacante cuenta con suficientes privilegios y herramientas para llevar a cabo el análisis y modificación de la aplicación.

Bajo un modelo de amenaza de ambiente de ejecución no confiable, las técnicas tradicionales para garantizar los atributos o dimensiones de la seguridad antes descritos dejan de ser eficaces. Esto conlleva a la necesidad de rediseñar dichas técnicas o identificar otras nuevas que permitan mitigar los ataques potenciales.

Los algoritmos criptográficos tradicionales empleados para garantizar la privacidad, tales como triple DES y AES, han sido rediseñados bajo este contexto, dando lugar a la criptografía de caja [20, 21].

La criptografía de caja blanca se define como "una aplicación criptográfica diseñada para resistir un ataque de caja blanca" [22]. El objetivo fundamental de esta técnica es implementar un algoritmo criptográfico que evite la extracción de la clave de cifrado del código de la aplicación que es protegida. Si esto se lograse, el sistema se convertiría en una caja negra, pues el código estaría cifrado y el atacante no tendría la forma de poder descifrarlo.

El término de criptografía de caja blanca fue expuesto inicialmente por Chow *et al* [22, 23]. En su investigación, el autor expone el funcionamiento de dicha técnica para el ocultamiento de la clave de cifrado/descifrado en algoritmos simétricos de bloque; usando como ejemplo versiones de implementación de los algoritmos DES [22] y AES [23]. Con ello, se evade el complejo problema del intercambio de claves por un canal de comunicaciones seguro tal y como fue conceptualizado en el Modelo de Shannon [24].

Otras nuevas técnicas para garantizar la privacidad son el código automodificable [25] y la ofuscación de código [11].

Durante la ejecución de una aplicación el código de la misma permanece estático; o sea las instrucciones de ejecución no cambian. Se dice que una aplicación contiene código automodificable cuando es capaz de modificar sus propias instrucciones de código, además de sus datos, durante su ejecución [25].

La ofuscación de código consiste, básicamente, en realizar transformaciones sobre el código de una aplicación (generalmente en tiempo de compilación), obteniéndose como resultado un nuevo código muy diferente al anterior sintácticamente, pero que preserva la semántica de la funcionalidad de la aplicación [11]. Con estas transformaciones se logra que la aplicación sea difícil de analizar pues el código se hace "ilegible" tras la realización de dichas transformaciones. Una aplicación ofuscada podría ser considerada como una "caja negra" a la cual entran valores y se obtienen resultados, desconociendo en todo momento su funcionamiento interno, no por el hecho de que no se pueda acceder a su código, sino por la complejidad interna de los algoritmos que complican su comprensión.

Por otra parte, de la rama de la esteganografía, se adoptaron los algoritmos de marcas de agua tradicionales, para ser incorporados en aplicaciones y garantizar en cierto grado los atributos de integridad y no repudio [26].

Una definición de marcas de agua para software fue la expuesta por Christian Collberg [27] al plantear que consiste básicamente en la inserción de determinada información en una aplicación, de forma tal que la misma pueda ser recuperada nuevamente a pesar de que la aplicación sea sometida a transformaciones sintácticas que preserven su funcionalidad. Además la información insertada debe estar oculta, no debe afectar el desempeño de la aplicación y debe estar matemáticamente probado que la información fue insertada intencionalmente para evitar el repudio.

Por último para garantizar la integridad de las aplicaciones se identifican las técnicas que garantizan resistencia ante la manipulación de las aplicaciones, destacándose la autoverificación de integridad [28, 29].

Acorde a la definición propuesta por Aucsmith, "(...) un software resistente a manipulación, es un software que es resistente a observaciones y modificaciones" [30]. Tomando esta definición como referencia, un software resistente a manipulación (*tamper resistant software*) es capaz de garantizar sus atributos de integridad, mostrando un comportamiento o apariencia que retarda el éxito de un ataque.

Los mecanismos de auto-verificación de integridad [29], también referidos en la literatura como software resistente a manipulación (*software tamper resistant*) [28] o a prueba de manipulación (software tamper-proofing) [27], están dirigidos a aumentar la resistencia ante ataques por modificación, ya sean estáticos o dinámicos. Se emplea el término auto-verificación porque el software es el encargado de protegerse a sí mismo, a través de los componentes de control que le fueron adicionados como parte del mecanismo de protección.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. X , No. X, (mes, 2018) pp-pp ISSN 2550-6730

4. Conclusiones

Los autores de este artículo conformamos un colectivo que, en los últimos diez años, se ha centrado, en asimilar con un enfoque de ingeniería aspectos que se enmarcan de una manera u otra en las dimensiones presentadas.

A través del estudio de la Criptografía, los controles de integridad, los protocolos criptográficos, la auditoría informática, la ingeniería inversa de ejecutables y bases de datos, y la propuesta de soluciones teóricas y prácticas en el ámbito de la seguridad, hemos observado una diversidad de enfoques y matices en esta temática que mantienen estrecha relación con los criterios enunciados.

El avance alcanzado, en el conocimiento y comprensión de la problemática de la seguridad de la información es, sin dudas, muy limitado si se tiene en cuenta la manera en que las tecnologías, el conocimiento y las herramientas de ataques han invadido el presente y se reproducirán exponencialmente en el futuro.

Se observan dos escenarios extremos. El más grave: no hacer nada por el tema de la seguridad y dejar una brecha abierta a los atacantes.

En el segundo escenario, se tiene conciencia del problema, y a veces con cierta frustración se desconfía de todo o se confía en cualquier solución o herramienta de seguridad anunciada, comprada o diseñada de manera propietaria. En un extremo, ello equivale a caer en una especie de primer escenario.

Consideramos procedente acercarse a un modelo del segundo escenario hacia un principio de confianza moderada [31], aplicando el conocimiento general y específico a las soluciones propias y de terceros, para alcanzar un estado de seguridad confortable y verificable.

Un abordaje al plano conceptual, integral y general de la Seguridad de la Información, a través de las dimensiones presentadas, puede hacer más claro el espacio actual en que se desenvuelve esta temática y entender mejor los escenarios específicos que permitan obtener soluciones sólidas y estándares.

No es de dudar, que las tecnologías, los problemas y el futuro, adicionen otras dimensiones y complejidad al ya oscuro espacio de la seguridad.

5. Referencias

Referencias

[1] Alfred J. Menezes, Scott A. Vanstone y Paul C. Van Oorschot. *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, Inc, 1996.

[2] Bruce Schneier. *Applied Cryptography (2Nd Ed.): Protocols, Algorithms, and Source Code in C*. New York, NY, USA: John Wiley & Sons, Inc., 1995. ISBN: 0-471-11709-9.

[3] Adrian Baldwin y Simon Shiu. «Enabling Shared Audit Data». En: *Information Security*. Ed. por Colin Boyd y Wenbo Mao. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, págs. 14-28. ISBN: 978-3-540-39981-0.

[4] Gustavus J. Simmons. *Contemporary Cryptology: The Science of Information Integrity*. Piscataway, NJ, USA: IEEE Press, 1994. ISBN: 0879422777.

[5] Roberto Sepúlveda Lima, Frank D. Abá Medina y Léster Crespo Sierra. «Escenarios típicos de fallas de seguridad relacionadas con la integridad de datos.» En: *Ingeniería Industrial* 24.3 (2003), págs. 87-90.

[6] Tsonka Baicheva, Stefan Dodunekov y Peter Kazakov. «On the cyclic redundancy-check codes with 8-bit redundancy». En: *Computer Communications* 21.11 (1998), págs. 1030-1033. ISSN: 0140-3664.

[7] Bart Preneel. «The State of Cryptographic Hash Functions». En: *Lectures on Data Security, Modern Cryptology in Theory and Practice, Summer School, Aarhus, Denmark, July 1998*. London, UK, UK: Springer-Verlag, 1999, págs. 158-182. ISBN: 3-540-65757-6.

[8] D. R. Stinson. «Some Observations on the Theory of Cryptographic Hash Functions». En: *Des. Codes Cryptography* 38.2 (feb. de 2006), págs. 259-277. ISSN: 0925-1022.

[9] Paul B. Thompson. «Privacy, Secrecy and Security». En: *Ethics and Inf. Technol.* 3.1 (mayo de 2001), págs. 13-19. ISSN: 1388-1957.

[10] Huaiqing Wang y Shuozhong Wang. «Cyber Warfare: Steganography vs. Steganalysis». En: *Commun. ACM* 47.10 (oct. de 2004), págs. 76-82. ISSN: 0001-0782.

[11] A. K. Dalai, S. S. Das y S. K. Jena. «A code obfuscation technique to prevent reverse engineering». En: *Proc. Signal Processing and Networking (WiSPNET) 2017 Int. Conf. Wireless Communications*. Mar. de 2017, págs. 828-832.

[12] Ji Ma y Mehmet A. Orgun. «Formalising Theories of Trust for Authentication Protocols». En: *Information Systems Frontiers* 10.1 (mar. de 2008), págs. 19-32. ISSN: 1387-3326.

[13] Reto Kohlas, Jacek Jonczy y Rolf Haenni. «A New Model for Public-Key Authentication». En: *Kommunikation in Verteilten Systemen (KiVS)*. Ed. por Torsten Braun, Georg Carle y Burkhard Stiller. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, págs. 213-224. ISBN: 978-3-540-69962-0.

[14] Jose A. Onieva, Jianying Zhou y Javier Lopez. «Multiparty Nonrepudiation: A Survey». En: *ACM Comput. Surv.* 41.1 (ene. de 2009), 5:1-5:43. ISSN: 0360-0300.

[15] Shengzhi Zhang y col. «Availability-sensitive Intrusion Recovery». En: *Proceedings of the 1st ACM Workshop on Virtual Machine Security*. VMSec '09. Chicago, Illinois, USA: ACM, 2009, págs. 43-48. ISBN: 978-1-60558-780-6.

[16] P.C. van Oorschot A. Main. «Software Protection and Application Security: Understanding the Battleground». En: *International Course on State of the Art and Evolution of Computer Security and Industrial Cryptography*. Heverlee, Belgium, 2003.

[17] Alex Shaw. «Program Transformations to Fix C Buffer Overflows». En: *Companion Proceedings of the 36th International Conference on Software Engineering*. ICSE Companion 2014. Hyderabad, India: ACM, 2014, págs. 733-735. ISBN: 978-1-4503-2768-8.

[18] A. Sadeghian, M. Zamani y S. M. Abdullah. «A Taxonomy of SQL Injection Attacks». En: *Proc. Int. Conf. Informatics and Creative Multimedia*. Sep. de 2013, págs. 269-273.

[19] D. Das, U. Sharma y D. K. Bhattacharyya. «Detection of Cross-Site Scripting Attack under Multiple Scenarios». En: *The Computer Journal* 58.4 (abr. de 2015), págs. 808-822. ISSN: 0010-4620.

[20] M. Beunardeau y col. «White-Box Cryptography: Security in an Insecure Environment». En: *IEEE Security Privacy* 14.5 (sep. de 2016), págs. 88-92. ISSN: 1540-7993.

[21] K. Bai, C. Wu y Z. Zhang. «Protect white-box AES to resist table composition attacks». En: *IET Information Security* 12.4 (2018), págs. 305-313. ISSN: 1751-8709.

[22] Stanley Chow y col. «A White-Box DES Implementation for DRM Applications». En: *Digital Rights Management*. Springer, 1 de ene. de 2003. ISBN: 978-3-540-40410-1.

[23] Stanley Chow y col. «White-Box Cryptography and an AES Implementation». En: *Revised Papers from the 9th Annual International Workshop on Selected Areas in Cryptography*. SAC '02. London, UK, UK: Springer-Verlag, 2003, págs. 250-270. ISBN: 3-540-00622-2.

[24] C. E. Shannon. «Communication theory of secrecy systems». En: *The Bell System Technical Journal* 28.4 (oct. de 1949), págs. 656-715. ISSN: 0005-8580.

[25] M. Xianya y col. «A Survey of Software Protection Methods Based on Self-Modifying Code». En: *Proc. Int. Conf. Computational Intelligence and Communication Networks (CICN)*. Dic. de 2015, págs. 589-593.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. X , No. X, (mes, 2018) pp-pp ISSN 2550-6730

[26] N. Zong y C. Jia. «Software Watermarking Using Support Vector Machines». En: *Proc. IEEE 39th Annual Computer Software and Applications Conf.* Vol. 2. Jul. de 2015, págs. 533-542.

[27] C. S. Collberg y C. Thomborson. «Watermarking, tamper-proofing, and obfuscation - tools for software protection». En: *IEEE Transactions on Software Engineering* 28.8 (ago. de 2002), págs. 735-746. ISSN: 0098-5589.

[28] Mariusz H. Jakubowski, Chit Wei (Nick) Saw y Ramarathnam Venkatesan. «Tamper-Tolerant Software: Modeling and Implementation». En: *Advances in Information and Computer Security*. Springer, 1 de ene. de 2009. ISBN: 978-3-642-04845-6.

[29] Yulier Nuñez Musa y col. «A Non-Deterministic Self-Checking Mechanism to Enhance Tamper-Resistance in Engineering Education Software». En: *International Journal of Engineering Education* 28 (ene. de 2012), págs. 1393-1398.

[30] David Aucsmith. «Tamper resistant software: an implementation». En: *Information Hiding*. Ed. por Ross Anderson. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, págs. 317-333. ISBN: 978-3-540-49589-5.

[31] A. Avizienis y col. «Basic concepts and taxonomy of dependable and secure computing». En: *IEEE Transactions on Dependable and Secure Computing* 1.1 (ene. de 2004), págs. 11-33. ISSN: 1545-5971.