La Reunión Española sobre Criptología y Seguridad de la Información (RECSI) es el congreso científico español de referencia en el ámbito de la Seguridad en las Tecnologías de la Información. En septiembre de 2010 se celebra la undécima edición de este congreso en Tarragona. Las pasadas ediciones tuvieron lugar en Palma de Mallorca (1991), Madrid (1992), Barcelona (1994), Valladolid (1996), Torremolinos (1998), Santa Cruz de Tenerife (2000), Oviedo (2002), Leganés (2004), Barcelona (2006) y Salamanca (2008).

Estas actas contienen las contribuciones de la RECSI 2010, cuyas sesiones se organizan en los siguientes ámbitos temáticos: cifrado de flujo, clave pública, criptoanálisis, firmas digitales, privacidad, protocolos, RFID, seguridad, seguridad de redes, *watermarking* y *fingerprinting*.

ISBN 978-84-693-3304-4

SPONSORS/SUPPORTERS

UNESCO Chair in Data Privacy

[DΣIM]

Universitat Rovira i Virgili

Ajuntament de Tarragona

Diputació Tarragona

AGAUR Agència de Gestió d'Ajuts Universitaris i de Recerca

Gobierno de España · Ministerio de Ciencia e Innovación

[publicacions] urv

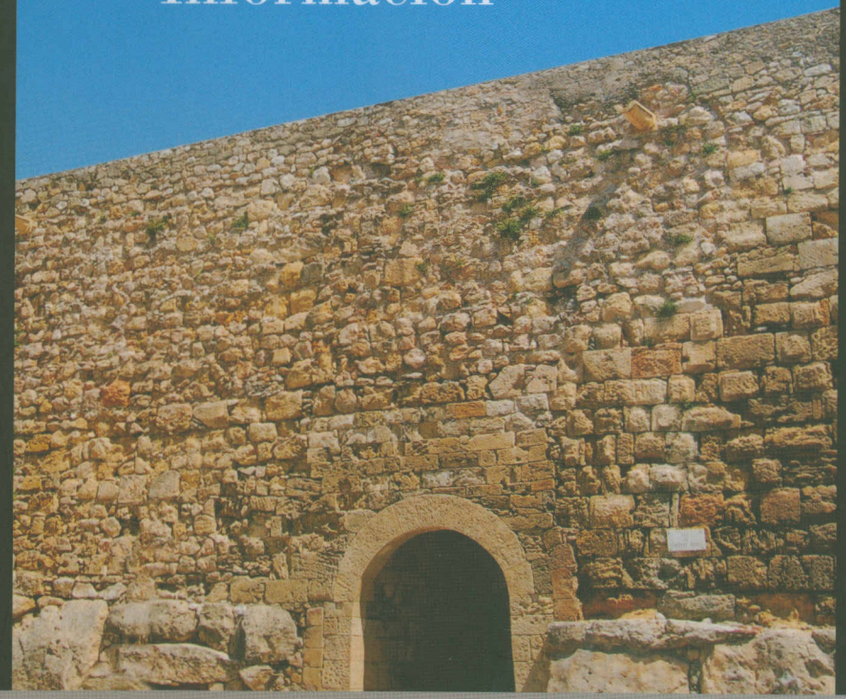
RECSI 2010 | XI Reunión Española sobre Criptología y Seguridad de la Información

RECSI 2010

Tarragona,
7–10 septiembre 2010

Coordinado por:
Josep Domingo Ferrer, Antoni Martínez Ballesté,
Jordi Castellà Roca, Agustí Solanas Gómez

XI Reunión Española sobre Criptología y Seguridad de la Información



[publicacions] urv

RECSI 2010

IX Reunión Española sobre Criptología y Seguridad de la Información

[publicacions] urv
Tarragona 2010

Edita:
Publicacions URV

1ª edició: juliol 2010

Impressió: Gràfiques Arrels, S. L.
Depòsit Legal: T-1099/2010
ISBN: 978-84-693-3304-4

Publicacions de la Universitat Rovira i Virgili:
Av. Catalunya, 35 - 43002 Tarragona
Tel. 977 558 474 - Fax: 977 558 393
www.urv.cat/publicacions
publicacions@urv.cat

Arola Editors: Polígon Francolí, parcel·la 3, nau 5 - 43006 Tarragona
Tel. 977 553 707 - Fax 977 542 721
arola@arolaeditors.com

Cossetània Edicions: C. de la Violeta, 6 - 43800 Valls
Tel. 977 602 591 - Fax 977 614 357
www.cossetania.com
cossetania@cossetania.com

RECSI 2010

IX Reunión Española sobre Criptología y Seguridad de la Información

Tarragona 7–10 de septiembre 2010

Coordinado por:
Josep Domingo Ferrer
Antoni Martínez Ballesté
Jordi Castellà Roca
Agustí Solanas Gómez

[publicacions] urv
Tarragona, 2010

Prefacio

Los grandes avances realizados en las tecnologías de la información y de las comunicaciones (TIC) han elevado nuestra capacidad de generar y compartir información hasta límites insospechados, y con esta capacidad también han aumentado los riesgos que ello supone.

El mundo electrónico-digital tiende a reemplazar a los antiguos sistemas, más lentos e ineficientes. Algunos ejemplos cotidianos los encontramos en el correo electrónico, el comercio electrónico, la votación electrónica, la administración digital, la televisión digital, etc. El mundo de lo electrónico y lo digital está llamado a ser el dominante y es por ello que resulta de vital importancia el estudio de teorías y métodos que permitan garantizar la privacidad y la seguridad de los usuarios en este nuevo contexto.

Con esta idea en mente, y con el objetivo de servir de foro de intercambio de conocimientos para los investigadores, en 1991 nació la Reunión Española sobre Criptología y Seguridad de la Información (RECSI), la cual en aquel entonces vino a llamarse Primera Jornada Española sobre Criptografía.

Este año, Tarragona acoge en septiembre la undécima edición de la RECSI, el congreso científico español de referencia en el ámbito de la seguridad en las tecnologías de la información. Las pasadas ediciones se realizaron en Palma de Mallorca (1991), Madrid (1992), Barcelona (1994), Valladolid (1996), Torremolinos (1998), Santa Cruz de Tenerife (2000), Oviedo (2002), Leganés (2004), Barcelona (2006) y Salamanca (2008).

La ciudad de Tarragona ha sido testigo de generaciones cuyas huellas han merecido el reconocimiento mundial. Como elemento representativo de esta RECSI hemos elegido la muralla, símbolo de los vestigios de la Tarragona Romana y uno de los muchos elementos patrimoniales que recomendamos visitar.

Estas actas contienen las 72 contribuciones de la RECSI 2010, cuyas sesiones se organizan en los siguientes ámbitos temáticos: cifrado de flujo, clave pública, criptoanálisis, firmas digitales, privacidad, protocolos, RFID, seguridad, seguridad de redes, watermarking y fingerprinting. Como conferenciantes invitados contamos con Ronald Cramer (Centrum Wiskunde & Informatica, Amsterdam) y Paulo Veríssimo (Universidad de Lisboa).

Desde la organización queremos expresar nuestro agradecimiento a todos los patrocinadores y colaboradores del evento, así como también a todos los ponentes, asistentes, miembros de los comités y revisores.

La compilación de las actas se realizado con LaTeX y el paquete 'confproc'.

Tarragona, septiembre de 2010

Josep Domingo Ferrer
Jordi Castellà Roca
Antoni Martínez Ballesté
Agustí Solanas Gómez

Comité de organización

Presidente

- Josep Domingo Ferrer (Universitat Rovira i Virgili)

Vicepresidentes

- Jordi Castellà Roca (Universitat Rovira i Virgili)
- Antoni Martínez Ballesté (Universitat Rovira i Virgili)
- Agusti Solanas Gómez (Universitat Rovira i Virgili)

Secretaría

- Jesús Manjón Paniagua (Universitat Rovira i Virgili)
- Gloria Pujol Crespo (Universitat Rovira i Virgili)

Comité científico

- Abascal Fuentes, Policarpo (Universidad de Oviedo)
- Álvarez Marañón, Gonzalo (C.S.I.C.)
- Amigó García, José María (Universidad Miguel Hernández)
- Areitio Bertolín, Javier (Universidad de Deusto)
- Borrell Viader, Joan (Universitat Autónoma de Barcelona)
- Bras Amorós, Maria (Universitat Rovira i Virgili)
- Caballero Gil, Pino (Universidad de La Laguna)
- Castellà Roca, Jordi (Universitat Rovira i Virgili)
- Climent, Joan-Josep (Universitat d'Alacant)
- Domingo Ferrer, Josep (Universitat Rovira i Virgili)
- Durán Díaz, Raúl (Universidad de Alcalá de Henares)
- Fernández-Medina Patón, Eduardo (Universidad de Castilla La Macha)
- Ferrer Gomila, Josep Lluís (Universitat de les Illes Balears)
- Fúster Sabater, Amparo (C.S.I.C.)
- González Vasco, Mª Isabel (Universidad Rey Juan Carlos)
- Gutiérrez Gutiérrez, Jaime (Universidad de Cantabria)
- Hernández Encinas, Luis (C.S.I.C.)
- Hernández Goya, Candelaria (Universidad de La Laguna)
- Herrera Joancomartí, Jordi (Universitat Autònoma de Barcelona)
- Huguet Rotger, Llorenç (Universitat de les Illes Balears)

- López Muñoz, Javier (Universidad de Málaga)
- Martín del Rey, Ángel (Universidad de Salamanca)
- Martínez López,Consuelo (Universidad de Oviedo)
- Megías, David (Universitat Oberta de Catalunya)
- Miret Biosca, José María (Universitat de Lleida)
- Morillo Bosch, Paz (Universitat Politècnica de Catalunya)
- Padró Laimon, Carles (Universitat Politècnica de Catalunya)
- Peinado Domínguez, Alberto (Universidad de Málaga)
- Ramió Aguirre, Jorge (Universidad Politécnica de Madrid)
- Ramos Álvarez, Benjamín (Universidad Carlos III de Madrid)
- Ribagorda Garnacho, Arturo (Universidad Carlos III de Madrid)
- Rifà Coma, Josep (Universitat Autònoma de Barcelona)
- Sáez Moreno, Germán (Universitat Politècnica de Catalunya)
- Salazar Riaño, José Luis (Universidad de Zaragoza)
- Sánchez Ávila, Carmen (Universidad Politécnica de Madrid)
- Sebé, Francesc (Universitat de Lleida)
- Sempere Luna, José María (Universitat Politècnica de València)
- Soriano Ibáñez, Miguel (Universitat Politècnica de Catalunya)
- Tena Ayuso, Juan (Universidad de Valladolid)
- Villar Santos, Jorge (Universitat Politècnica de Catalunya)
- Wu, Qianhong (Universitat Rovira i Virgili)
- Zurutuza, Urko (Universidad de Mondragón)

Programa de las sesiones

Cifrado de flujo

Clave pública

Criptoanálisis

Firmas digitales

Privacidad

Protocolos

RFID

Seguridad

Seguridad de redes

Watermarking y fingerprinting

Longitudes de cifrado					
Cifrado	N	K	K'	(NxL)+K	L+K'
SSL+IPSEC+WEP	3	206	125	3L+206	L+125
IPSEC+WEP	2	148	104	2L+148	L+104
SSL+WEP	2	89	73	2L+89	L+73

Tabla V
VALORES DE N, K Y K'.

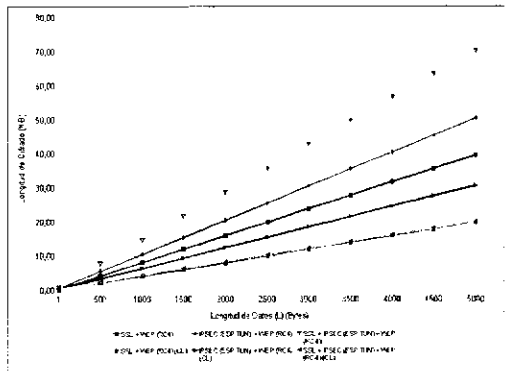


Figura 9. Longitud de Cifrado

El escenario presentado en el apartado I implementa SSL, IPSEC y WEP por lo que las expresiones que cuantifican los octetos cifrados son 3L+206 y L+125. A partir de estas expresiones obtenemos la figura 10 que muestra la variación del número de octetos cifrados por los mecanismos de capa en función de la longitud de los datos de aplicación (L) y compara nuestra solución con la situación de cifrado sin aplicar la solución presentada.

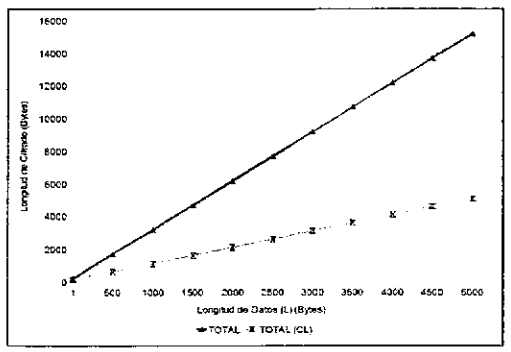


Figura 10. Número total de octetos cifrados.

VI. CONCLUSIONES Y TRABAJO FUTURO.

En este artículo hemos demostrado que al aplicar simultáneamente mecanismos de cifrado en diferentes capas se producen duplicidades, e incluso multiplicidades, en el cifrado de octetos. Hemos calculado que la longitud de cifrado, al aplicar mecanismos de cifrado en las capas TCP, IP y MAC, es (NxL)+K. Hemos propuesto una solución que reduce el cifrado a un orden L+K'.

Nuestra solución requiere que las capas dispongan de información del cifrado realizado en las otras capas. Este problema requiere la aplicación del diseño Cross-Layer en el que las distintas capas intercambien información relativa a las operaciones de cifrado que realizan. La línea de trabajo a seguir consiste en el diseño de un algoritmo Cross-Layer que implemente la solución propuesta. Otro aspecto importante es la cuantificación del impacto del cifrado en términos de energía y rendimiento global y los beneficios que se obtienen al aplicar una solución que reduzca la cantidad de octetos cifrados. Debemos considerar otros servicios de seguridad y mecanismos de cifrado de capa con el objeto de cuantificar la longitud de datos cifrados y los costes de energía en los terminales inalámbricos y el rendimiento en el punto de acceso.

VII. GRADECIMIENTOS

Este trabajo ha sido parcialmente financiado por el MEC y FEDER bajo los proyectos: "Seguridad en la Contratación Electrónica basada en Servicios Web"(CICYT TSI2007-62986) y ARES "Grupo de Investigación Avanzada en Seguridad y Privacidad de la Información"(Consolider - Ingenio CSD2007-004).

REFERENCIAS

[1] IEEE Std 802.11-1997 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.
[2] A.O. Freier, P. Karlton, P.C. Kocher. Transport Layer Security Working Group. *The SSL Protocol. V3.0. Internet Draft*, November 1996.
[3] D. Carrel D. Harkins. *RFC2409:The Internet Key Exchange (IKE)*. IETF. Network Working Group, November 1998.
[4] IETF. Network Working Group. *RFC791: Internet Protocol*. September 1991.
[5] IETF. Network Working Group. *RFC793: Transmission Control Protocol*, September 1991.
[6] S. Kent and R. Atkinson. *RFC2401: Security Architecture for the Internet Protocol*. IETF. Network Working Group, November 1998.
[7] S. Kent and R. Atkinson. *RFC2402: IP Authentication Header*. IETF. Network Working Group, November 1998.
[8] S. Kent and R. Atkinson. *RFC2406: IP Encapsulating Security Payload (ESP)*. IETF. Network Working Group, November 1998.
[9] R. Fielding H. Frystyk R. Fielding, J. Gettys and T. Berners-Lee. *RFC2068: Hypertext Transfer Protocol – HTTP/1.1*. IETF. Network Working Group, January 1997.
[10] T. J. Socolofsky and C.J. Kale. *RFC1180: TCP/IP tutorial*. IETF. Network Working Group, January 1991.

Modelo de Calidad para la Seguridad en Productos Software

Abel Enrique Fornaris
Grupo GSyA. Dep. de Tecnologías y Sistemas de Información
Universidad de Castilla-La Mancha
Email: Fornaris@gmail.com

Luís Enrique Sánchez
Departamento de I+D+i
SICAMAN Nuevas Tecnologías
Juan José Rodrigo, 4. Tomelloso
Ciudad Real, España
Email: LESanchez@sicaman-nt.com

Eduardo Fernández-Medina
Grupo GSyA. Dep. de Tecnologías y Sistemas de Información
Universidad de Castilla-La Mancha
Email: Eduardo.FdezMedina@uclm.es

***Resumen*—La importancia de tener en cuenta la seguridad como requisito no funcional en el éxito de un producto software (PS) es un hecho cada día más notable. Existen varios estándares y aproximaciones en la comunidad científica a la definición de la seguridad como elemento de calidad de un PS, sin embargo existen diferencias y falta de cohesión entre ellas. En este trabajo se estudian las propuestas más importantes en este sentido con el objetivo final de proponer un modelo de calidad integrador para la seguridad en el ámbito de los PS.**

***Palabras Clave*—seguridad; modelo calidad seguridad; seguridad producto software**

I. INTRODUCCIÓN

La seguridad es un requisito no funcional que tiene una repercusión extraordinaria en la calidad de los productos software. De hecho, la seguridad informática ha sido un campo que ha crecido enormemente desde los años 70, dando lugar a una gran cantidad de técnicas, modelos, protocolos, etc., que han venido acompañados también de una actividad muy pronunciada por parte de las organizaciones internacionales de normalización y certificación. Tanto es así, que como se indica en [1], se pueden encontrar numerosas organizaciones internacionales de estandarización que han producido una compleja estructura de estándares relativos a temáticas relacionadas con la seguridad informática, que cambian y se actualizan con mucha frecuencia.

Existen numerosas definiciones de seguridad. Lo habitual es que todas ellas definan la seguridad en términos de otros conceptos relacionados. Por ejemplo, una definición tradicional es la de [2], que la define como la "protección de información procesada por un computador frente a consultas no autorizadas, modificaciones inapropiadas o la falta de disponibilidad de un servicio en un momento dado". Otra definición clásica es la ofrecida por [3], que considera la seguridad como un sub-factor de la calidad del software, y la define como "la capacidad de los productos software para proteger los datos y la información para que personas o sistemas no autorizados no puedan leerla o modificarla y para que el acceso no sea rechazado a personal autorizado". En ambas definiciones están presentes los conceptos de confidencialidad, integridad y disponibilidad. Sin embargo, hay otras definiciones algo más recientes que consideran además, otras propiedades importantes, como son la autenticación, el no repudio y la autorización y control de acceso [4]. Aunque la seguridad se puede interpretar como un aspecto estrictamente técnico, hay autores que piensan que es mucho más que eso, teniendo por el contrario una dimensión estratégica, resultando uno de los criterios más importantes en el gobierno de las TIC [5].

Sin embargo, aunque también se han desarrollado ampliamente en las últimas décadas las técnicas y metodologías propias de la ingeniería del software, éstas no han considerado la seguridad como un aspecto importante del desarrollo, dejando que la construcción metodológica del software se centre fundamentalmente en los requisitos funcionales, y algunos otros requisitos no funcionales, y relegando los requisitos de seguridad a un momento tardío en el proceso de desarrollo de software. Algunas propuestas interesantes que tratan la seguridad, aunque de manera parcial y sin ofrecer un claro seguimiento de esos aspectos de seguridad a lo largo del proceso de desarrollo incluyen [6–13].

Por lo tanto, se hace necesaria la creación de un modelo de seguridad (como componente de calidad) que claramente identifique una taxonomía de requisitos de seguridad que puedan ser identificados, modelados e implementados, junto al resto de requisitos, tanto funcionales como no funcionales.

El objetivo de esta propuesta es analizar los modelos existentes que definan la seguridad y sus componentes como aspectos que inciden en la calidad de los productos software, y construir un modelo unificado, completo y detallado que permita evaluar y mejorar este aspecto del desarrollo que resulta crítico para el éxito de muchos productos software. Este modelo, no incluirá aspectos relativos a técnicas de seguridad, amenazas de seguridad, políticas de seguridad, ataques de seguridad, etc., sino que fundamentalmente especificará las características de seguridad que nos puedan interesar de un producto software.

Para ello, se ha organizado el resto del documento del siguiente modo: En la Sección II se presentan algunos de los modelos de seguridad más relevantes. Posteriormente, en la Sección III se analizan paso a paso y desde un punto de vista integrador todas las características que proponen los trabajos estudiados en la sección anterior y que darán lugar al modelo

de seguridad que se propone en la Sección IV. La Sección V refleja las conclusiones obtenidas de la evolución y desarrollo de la propuesta.

II. Modelos de Seguridad Relevantes

En esta sección se describirán los aspectos más importantes de los modelos de seguridad definidos en los principales estándares más aceptados sobre calidad del software y seguridad.

A. ISO/IEC 9126

Uno de los estándares con mayor reconocimiento para evaluar la calidad de los productos software es el ISO/IEC 9126 [3]. Este estándar define tres tipos de calidad: la calidad interna, la calidad externa y la calidad en uso. El estándar define un modelo de calidad de productos software (tanto para calidad interna como externa) en términos de un conjunto de características (funcionalidad, fiabilidad, usabilidad, eficiencia, mantenibilidad y portabilidad). Este modelo, que ya cuenta con más de una década desde su creación, otorga muy poca importancia a la seguridad como factor de calidad de los productos software.

En cuanto a la calidad en uso, el estándar la define como la capacidad de un producto software para permitir a ciertos usuarios conseguir sus objetivos con eficacia, productividad, seguridad y satisfacción en un contexto de uso específico. En este caso, también se hace una mención explícita a la seguridad, pero relativa al término inglés safety.

Un resumen de dicho modelo puede verse en la Tabla I , donde la seguridad no es una característica del mismo. Sin embargo, sí aparece definida como una sub-característica de la funcionalidad.

Tabla I
Modelo de Seguridad de la ISO/IEC 9126

Modelo de Calidad Interna y Externa		
Funcionalidad	Seguridad	Confidencialidad
		Integridad
		Disponibilidad
Modelo de Calidad en Uso		
Seguridad (safety)		

B. SQuaRE - ISO/IEC 25010

SQuaRE (Software Product Quality Requirements and Evaluation - Requisitos y Evaluación de la Calidad de Productos Software) es una familia de estándares, que tienen como origen el estándar ISO/IEC 9126, y que define la calidad de un producto software como el grado en el que dicho producto satisface las necesidades implícitas y explícitas de sus diferentes usuarios [14]. Este estándar está en proceso de creación, y todavía no están disponibles documentos definitivos, aunque ya se puede intuir con cierta precisión sus aspectos más destacables.

Este estándar considera actualmente tres modelos de calidad: El modelo de calidad de productos software, el modelo de calidad en uso, y el modelo de calidad de datos. Cada uno de estos modelos es definido en términos de un conjunto de propiedades o características. Así, el modelo de calidad de productos software, considera entre sus características la seguridad y la fiabilidad, como destacables. En este modelo, el concepto de disponibilidad se incluye como una sub-característica de la fiabilidad. Por otro lado, el modelo de calidad en uso viene caracterizado por tres aspectos, que son la usabilidad, la flexibilidad y la seguridad (safety), este último de interés, con sub-características asociadas. Por último, el modelo de calidad de datos define un conjunto de características de las cuales son de interés las de confidencialidad y disponibilidad.

Este estándar, a pesar de no estar centrado en la seguridad (como otros que se analizan a continuación) ya ofrece un conjunto más completo de propiedades de seguridad, como se puede ver resumido en la Tabla II, y le otorga a la seguridad un protagonismo como aspecto de calidad que no era reconocido en las versiones anteriores del estándar del que parte SQuaRE, al pasar a estar presente como una característica más en el modelo.

Tabla II
Modelo de Seguridad de la ISO/IEC 25010

Característica	Sub-característica
Modelo de Calidad de Productos Software	
Seguridad	Confidencialidad
	Integridad
	No repudio
	Responsabilidad
	Autenticidad
	Conformidad
Modelo de Calidad en Uso	
Seguridad (safety)	Daño comercial
	Seguridad y salud del operador
	Seguridad y salud pública
	Daño medioambiental
	Conformidad de seguridad (safety)
Modelo de Calidad de Datos	
Confidencialidad	
Disponibilidad	

C. Modelo de Firesmith

Un modelo propuesto por Firesmith [15], lejos de la vorágine de las organizaciones de estandarización, y más en un contexto científico, propone un modelo de la seguridad, como característica de la calidad del software, compuesto por un conjunto de sub-características que a su vez se dividen en sub-características, con la organización que se representa en la Tabla III.

Cada elemento de la propuesta está debidamente definido, excepto las dos últimas sub-características de seguridad.

D. ISO/IEC 15408 o Common Criteria

Este estándar [16] no propone un modelo de seguridad, sino que propone un marco de trabajo para la evaluación

Tabla III
Modelo de Seguridad de Firesmith

Seguridad	Control de acceso	Identificación
		Autenticación
		Autorización
	Detección de ataques	
	No repudio	
	Integridad	Integridad de datos
		Integridad de hardware
		Integridad personal
		Integridad de software
	Auditoría de seguridad	
	Protección física	
	Privacidad	Anonimato
		Confidencialidad
	Recuperación	
	Continuidad	

de la seguridad de productos software y sistemas de información. El mismo no considera la seguridad como un requisito no funcional, sino todo lo contrario, define un conjunto de clases de componentes o requisitos funcionales de seguridad y también un conjunto de componentes de garantía de seguridad organizados en varios niveles de exigencia. Para este trabajo nos vamos a concentrar en las clases de requisitos funcionales, que se dividen en familias funcionales de seguridad, y que a su vez se dividen en componentes. Presentaremos a continuación algunas de las clases y familias, exponiendo un nivel adecuado para acercarnos al problema que nos atañe.

- Clase comunicaciones: Incluye familias de No Repudio de origen y recepción.
- Clase protección de datos de usuarios: Incluye familias de políticas y funciones de control de acceso; autenticación, importación/exportación, recuperación y transferencia interna de datos; políticas de protección de control de flujo, confidencialidad e integridad de datos en tránsito, protección e integridad de información residual y datos almacenados.
- Clase de identificación y autenticación: Familias de autenticación, identificación y enlace entre usuarios; atributos de usuario.
- Clase de privacidad: Incluye familias de anonimato, pseudoanonimato, enlace entre usuario y acciones, observación por parte de otros usuarios.
- Clase de protección de seguridad de un elemento: Familias de disponibilidad, confidencialidad e integridad de datos exportados; protección física, recuperación confiable, repetición de borrado.
- Clase de acceso a elementos: Familias de limitación, establecimiento, terminación y bloqueo de sesiones, historia de accesos.
- Clase de canales y caminos seguros.

E. MAGERIT versión 2

Este documento [17], elaborado por el Consejo Superior de Administración Electrónica de las Administraciones Públicas de España, presenta una metodología de análisis y gestión de riesgos de los sistemas de información, que resulta un documento de referencia tanto a nivel nacional como internacional (metodología oficialmente reconocida por la OTAN [18] y por la OCDE [19]) para la gestión de riesgos, y que es conforme a varias normas internacionales de gestión de la seguridad como es el caso de la ISO/IEC 13335 [20].

Esta metodología no ofrece un modelo de seguridad, pero si identifica una serie de aspectos que son cruciales para cumplir el objetivo de este trabajo. En primer lugar, MAGERIT identifica un conjunto de dimensiones de valoración, que son características o atributos que hacen valioso un activo, es decir, son facetas (sub-características) de seguridad que conviene proteger, en relación con los activos o elementos que constituyen valor dentro del contexto de las tecnologías de la información. En concreto, MAGERIT define las 7 dimensiones de valoración que se resumen en la Tabla IV, del siguiente modo:

Tabla IV
Dimensiones de Valoración de MAGERIT

Característica	Sub-característica
Dimensiones de Valoración de Activos	Disponibilidad
	Integridad de datos
	Confidencialidad de los datos
	Autenticidad de los usuarios del servicio
	Autenticidad del origen de los datos
	Trazabilidad del servicio
	Trazabilidad de los datos

Un segundo aspecto, considerado por MAGERIT, y que resulta especialmente interesante para el trabajo elaborado en este informe es el relativo a las amenazas. Las amenazas representan el impulso que da lugar a requisitos de seguridad, por lo que, además de disponer de un modelo de seguridad compuesto de características, es importante también identificar un conjunto de posibles amenazas que darán lugar a requisitos de seguridad (cuando sean consideradas) y por lo tanto a artefactos de análisis, diseño e implementación en los sistemas que se desarrollen.

En este sentido, MAGERIT define una taxonomía de amenazas clasificadas básicamente en desastres naturales, de origen industrial y errores y fallos no intencionados de los usuarios y del propio sistema.

F. Familia 27000

La familia de normas ISO/IEC 27000 está compuesta de un conjunto de documentos, todos ellos relacionados con la gestión de la seguridad. En concreto, la 27000 [21] incluye la definición de un vocabulario común sobre gestión de seguridad, la 27001 [22] proporciona un modelo para establecer, implementar, operar, controlar, revisar, mantener y revisar los sistemas de gestión de seguridad de la información, la

27002 [23] ofrece un código de buenas prácticas, la 27003 [24] unas guías de implantación, la 27004 [25] es relativa a métricas para la gestión de la seguridad, la 27005 [26] es sobre gestión de riesgos, la 27006 [27] muestra un cuerpo para la certificación de la seguridad y la 27007 [28] ofrece guías de auditoría. Esta familia de normas (todavía incompleta) representa un esfuerzo por la agrupación y unificación de estándares relativos a la gestión de la seguridad, y que se pretende que sea modelo de referencia en el futuro.

En su norma base, se define la seguridad de la información como la preservación de la confidencialidad, la integridad y la disponibilidad de la información. También considera, aunque en un menor nivel de importancia otras propiedades como la autenticación, la responsabilidad, el no repudio, y la fiabilidad. Todas estas características se encuentran rigurosamente definidas en dicho estándar.

G. *COBIT versión 4.1*

COBIT (Control Objectives for Information and Related Technology) [29] es un conjunto de buenas prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA). Este documento ayuda a entender los Sistemas de Información (o tecnologías de la información) y a decidir el nivel de seguridad y control que es necesario para proteger los activos de las compañías mediante el desarrollo de un modelo de administración de las tecnologías de la información. Uno de los aspectos más desarrollados en COBIT es la protección de la seguridad de la información, que aunque no es el único aspecto, aparece destacado frecuentemente. De hecho, por ejemplo, COBIT define un conjunto de "criterios de información" necesarios para conseguir los objetivos de negocio, y la mayoría son relativos a seguridad, ellos son: eficacia, eficiencia, confidencialidad, integridad, disponibilidad, conformidad y fiabilidad. Todos estos conceptos se aproximan a la seguridad, aunque desde un nivel de abstracción muy alto y relativo al negocio y sus procesos.

COBIT proporciona, además, un conjunto de procesos que contribuyen al gobierno de las tecnologías de la información, y son agrupados en diversas categorías. Uno de estos procesos es dedicado monográficamente a la seguridad (se conoce como DS5 Asegurar Seguridad de Sistemas), y para el cual se definen un conjunto de objetivos de control como son gestión y planificación de TI, gestión de identidades y cuentas de usuario, pruebas, vigilancia y control de seguridad, definición de incidencias de seguridad, gestión de claves criptográficas, prevención, detección y corrección de software malicioso, seguridad en redes, intercambio de datos sensibles y protección de la seguridad de la tecnología. Estos objetivos de control representan aspectos que deben ser tenidos en cuenta para garantizar la seguridad de las TI, de modo que existirán probablemente requisitos relativos estos objetivos de control en los sistemas de información, y se tendrá que desarrollar funcionalidad que los resuelvan.

III. Estudio de las Características

En primer lugar, y como paso previo a la construcción del modelo de seguridad del software, hemos realizado un análisis de las distintas características, sub-características y sub-sub-características relacionadas con la seguridad, presente en los diversos modelos que hemos considerado en la sección anterior. Para ello, hemos construido la Tabla VI, donde se indican las distintas propiedades de seguridad de las propuestas analizadas (para mayor legibilidad, dichas propuestas han sido numeradas, y las correspondencias se ofrecen en la Tabla V), y se especifica en el cruce, la relación de cada una de esas propiedades con cada propuesta (en blanco cuando la propiedad no aparece en la propuesta, "C" cuando aparece como característica, "S" cuando aparece como sub-característica y "U" cuando aparece identificado como parte de una sub-sub-característica).

Las diferencias en la consideración de unas propiedades y otras como características, sub-características, o incluso como parte de sub-sub-características, se justifica básicamente por dos hechos: el primero tiene que ver con el cambio en la consideración de la seguridad que ha habido en los últimos años (eso justifica la variación entre la ISO/IEC 9126 y la ISO/IEC 25010), mientras que el segundo es la orientación de las propuestas, ya que aquellas que consideran la seguridad como sub-característica, son propuestas que consideran la calidad de manera general, mientras que las que consideran estas propiedades como características, es porque se trata de propuestas claramente orientadas a la seguridad.

Tabla V
Enlace de columnas de la Tabla VI con los nombres de las propuestas

1	ISO/IEC 9126 Modelo de Calidad Interna y Externa
2	ISO/IEC 9126 Modelo de Calidad en Uso
3	ISO/IEC 25010 Modelo de Calidad de Productos Software
4	ISO/IEC 25010 Modelo de Calidad en Uso
5	ISO/IEC 25010 Modelo de Calidad de Datos
6	Modelo de Firesmith
7	MAGERIT V2
8	Familia 27000
9	COBIT

Analizando las distintas propiedades de la Tabla VI, se puede observar que en muchas ocasiones aparecen propiedades que comparten similitud con otras, y que se diferencian en algún matiz acentuado por una propuesta en concreto. Por ejemplo, la propiedad Confidencialidad, aparece definida en prácticamente todas las propuestas, pero en cambio MAGERIT la define como Confidencialidad de Datos, aunque compartiendo en esencia la definición.

Por ello, se ha construido un grupo canónico de características que reduce el número inicial de propiedades de seguridad, uniendo aquellas propiedades relativas en esencia a aspectos muy cercanos, y dando lugar a propiedades de seguridad cuyo nombre probablemente ya está dentro del

Tabla VI
Comparación de Propiedades de Seguridad

	1	2	3	4	5	6	7	8	9
Anonimato						U			
Auditoría de seguridad						S			
Autenticación						U		C	
Autenticidad de origen de datos							C		
Autenticidad de usuarios del servicio							C		
Autenticidad			S						
Autorización						U			
Confidencialidad	U		S		C	U		C	C
Confidencialidad de datos							C		
Conformidad			S						C
Conformidad (safety)				S					
Control de acceso						S			
Daño Comercial				S					
Daño medioambiental				S					
Detección de Ataques						S			
Disponibilidad	U				C		C	C	C
Fiabilidad								C	C
Identificación						U			
Integridad	U		S			S		C	C
Integridad de datos						U	C		
Integridad de hardware						U			
Integridad personal						U			
Integridad de software						U			
No Repudio			S			S		C	
Privacidad						S			
Protección física						S			
Responsabilidad			S					C	
Seguridad	S		C						
Seguridad (safety)		C		C					
Seguridad y salud del operador				S					
Seguridad y salud pública				S					
Trazabilidad de los datos							C		
Trazabilidad del servicio							C		

conjunto inicial de propiedades, pero cuya definición está enriquecida con los matices identificados en las propiedades iniciales de las que se parte (que en todo caso podrán actuar posteriormente como sub-características de ésta). Además, se han eliminado términos más generales que típicamente agregan algunos más detallados. En particular, se han suprimido los términos Seguridad y Seguridad con la orientación de Safety. También se ha eliminado la propiedad fiabilidad, ya que constituye una característica claramente diferenciada de seguridad, y así queda definida en el modelo de la ISO/IEC 25010.

Otro análisis de la Tabla VI indica que entre todas las propiedades de la seguridad, se puede observar una clara agrupación de aspectos relacionados con problemas de seguridad que son provocados intencionadamente, y por otro lado, en aspectos relacionados con problemas de seguridad fortuitos, que en principio pueden suceder sin que nadie los provoque intencionadamente (relacionados con el término inglés Safety). Todo esto redunda en otra categorización conforme al comentario anterior. Adicionalmente, en esta agrupación se considera la propiedad de conformidad, incluida en ambas categorías, ya que es importante desde ambos puntos de vista.

Estas clasificaciones de canonización e integración de características, así como de separación según la intencionalidad de los problemas de seguridad serán finalmente depuradas en la sección siguiente, con la propuesta de modelo de calidad de seguridad.

IV. Modelo Propuesto para la Seguridad de Productos Software

Tras el análisis y depuración de propiedades de seguridad llevados a cabo en la sección anterior, se presenta el modelo de seguridad (Tabla VII), compuesto por dos grupos de características de seguridad. El primer grupo es relativo a propiedades de seguridad definidas para proteger al sistema ante ataques de seguridad, y el segundo grupo se refiere a propiedades de seguridad definidas para proteger al sistema de fallos y situaciones fortuitas. Cada característica define a su vez un conjunto de sub-características, que se refiere a algún matiz específico que aun estando relacionado con la característica a la que pertenece, tiene algún aspecto claramente diferenciador. Se puede comprobar que el modelo elaborado comparte cierta similitud con la ISO/IEC 25010. pero la enriquece ampliamente con aspectos identificados en propuestas más especializadas en seguridad.

Tabla VII
Modelo de Seguridad Medusas

	Características	Sub-características
Protección ante ataques	Autenticidad	Autenticación
		Identificación
	Confidencialidad	Anonimato
		Privacidad
	Conformidad	
	Detección de ataques	
	Disponibilidad	
	Integridad	Integridad de datos
		Integridad de hardware
		Integridad personal
		Integridad de software
		Protección física
	No Repudio	
	Trazabilidad	
Protección ante accidentes		
	Conformidad (safety)	
	Daño Comercial	
	Daño medioambiental	
	Seguridad y Salud del operador	
	Seguridad y Salud pública	

El modelo considera las siguientes características y sub-características, relativas a la protección de los sistemas de información ante ataques provocados, cuyas definiciones son determinadas a partir de la extracción de conceptos integradores de los estándares y aproximaciones analizados en la Sección II.

- Autenticidad: Tiene que ver con el grado en el que se garantiza que los sujetos y recursos del sistema de información son auténticos.
  - Autenticación: Es relativo al grado en el que se verifica la identidad de los sujetos antes de interactuar con ellos.

- Identidad: Es relativo al grado en que se identifican a los sujetos antes de interactuar con ellos.

- Confidencialidad: Es el grado en el que se asegura que la información es solamente accesible a sujetos autorizados.
  - Anonimato: Es el grado en que se impide el almacenamiento o descubrimiento de la identidad de los usuarios.
  - Privacidad: Es el grado en el que se asegura que la información de carácter personal, privado e íntimo es solamente accesible a sujetos autorizados.
- Conformidad: Es el grado en que los productos software se ajustan a los estándares, acuerdos, o regulaciones de leyes y otras recomendaciones similares de seguridad.
- Detección de ataques: Es el grado en que los intentos de ataque o los ataques realizados con éxito son detectados, almacenados y notificados.
- Disponibilidad: Es el grado en que se asegura que los sujetos autorizados tienen acceso a los datos y aplicaciones en el momento en que lo requieran.
- Integridad: Es el grado en que se protege a los componentes de los sistemas de información de alteraciones intencionada por parte de sujetos no autorizados.
  - Integridad de datos: Concepto de integridad aplicado a los datos.
  - Integridad del hardware: Concepto de integridad aplicado a los componentes hardware del sistema.
  - Integridad del personal: Es el grado en que se protege la seguridad de las personas ante posibles reacciones del sistema provocados intencionadamente.
  - Integridad del software: Es el grado en que se protege los componentes de software de corrupción intencionada.
  - Protección física: Es el grado en que el sistema se protege a sí mismo y a sus componentes de ataques físicos.
- No repudio: Es el grado en que se impide que una parte de una interacción pueda repudiar algún aspecto de la interacción.
- Trazabilidad: Es el grado en que se asegura que las acciones de un sujeto pueden ser trazadas inequívocamente y asociadas a dicho sujeto.

Con respecto al modelo de seguridad, para el caso de características de seguridad relativas a la protección de los sistemas de información ante accidentes no provocados, básicamente se heredan las propiedades definidas por la ISO/IEC 25010 en el modelo de Calidad en Uso.

V. Conclusiones

En el presente trabajo se han analizado los estándares y propuestas centradas en seguridad o con marcado enfoque en ella, donde se exponen un grupo de sus características inherentes y que han servido como base para el modelo de calidad propuesto. Dicho modelo es una propuesta integradora de conceptos con el fin de ofrecer una visión común en el área, tanto en lo que refiere a características y sub-características como a su definición formal.

Agradecimientos

Esta investigación es parte de los proyectos: MEDUSAS (IDI-20090557), financiado por el Centro para el Desarrollo Tecnológico Industrial, BUSINESS (PET2008-0136) concedido por el Ministerio de Ciencia e Innovación de España y SEGMENT (HITO-09-138) y SISTEMAS (PII2I09-0150-3135) financiados por la Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha.

Referencias

[1] ITU. (2009). *ICT Security Standards Roadmap* Available: http://www.itu.int/ITU-T/studygroups/com17/ict/index.html

[2] S. Castano, et al.,*Database Security*: Addison-Wesley, 1995.

[3] ISO/IEC, "ISO/IEC 9126-1. Information Technology. Software Product Quality. Part 1: Quality Model.," ed, 1999.

[4] J. Swartz, "Security systems for a mobile world," *Technology in Society*, vol. 25, pp. 5-25, 2003.

[5] S. Posthumus and R. v. Solms, "A framework for the governance of information security," *Computers & Security*, vol. 22, pp. 638-646, 2004.

[6] J. Jürjens, "UMLsec: Extending UML for secure systems development," in *UML 2002 - The Unified Modeling Language, Model engineering, concepts and tools*, J. Jézéquel, et al., Eds., ed Dresden, Germany: Springer. LNCS 2460., 2002, pp. 412-425.

[7] J. Jürjens, *Secure Systems Development with UML*: Springer-Verlag, 2004.

[8] D. Basin, et al., "Model Driven Security: from UML Models to Access Control Infrastructures," *ACM Transactions on Software Engineering and Methodology*, vol. 15, pp. 39-91, January 2006.

[9] M. Hafner, et al., "SECTET: An Extensible Framework for the realization of Secure inter-organizational Workflows," *Internet Research*, vol. 16, pp. 491-506, 2006.

[10] E. Fernández-Medina and M. Piattini, "Designing Secure Databases," *Information and Software Technology*, vol. 47, pp. 463-477, 2005.

[11] C. Gutiérrez, et al., "Towards a Process for Web Services Security," *Journal of Research and Practice in Information Technology*, vol. 38, pp. 57-67, 2006.

[12] D. Mellado, et al., "A Common Criteria Based Security Requirements Engineering Process for Development of Secure Information Systems," *Computer Standards & Interfaces*, vol. 29, pp. 244-253, 2006.

[13] A. Rodríguez, et al., "Semi-Formal Transformation of Secure Business Processes into Analysis Class and Use Case Models: an MDA approach.," *Information and Software Technology*, 2010.

[14] ISO/IEC 25000, "Systems and software engineering - Software product Quality Requirements and Evaluation SQuaRE."

[15] D. Firesmith, "Specifying Reusable Security Requirements," *Journal of Object Technology*, vol. Vol. 3 (1), January-February., pp. 61-75, 2004.

[16] ISO/IEC, "ISO/IEC 15408. Common Criteria V3.," 2009.

[17] MAP, "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT - v 2)," 2005.

[18] CCN-CERT, "Últimos avances en ciberseguridad (9th NATO cyberdefense workshop). Revista auditoria y Seguridad (www.revista-ays.com). n23-junio: 70-71.," 2008.

[19] OECD, "The promotion of a culture of security for information systems and networks in OECD countries. DSTI/ICCP/REG(2005)1/FINAL, Organisation for Economic Co-operation and Development.," 2005.

[20] ISO/IEC, "ISO/IEC 13335 Information technology - Security techniques - Management of information and communications technology security.," 2004.

[21] ISO/IEC, "ISO/IEC 27000:2009. Information technology – Security techniques – Information security management systems – Overview and vocabulary," ed, 2009.

[22] ISO/IEC, "ISO/IEC 27001:2005. Information technology – Security techniques – Information security management systems – Requirements ", ed, 2005.

[23] ISO/IEC, "ISO/IEC 27002:2005. Information technology – Security techniques – Code of practice for information security management," ed, 2005.

[24] ISO/IEC, "ISO/IEC 27003:2010. Information technology – Security techniques – Information security management system implementation guidance," 2010.

[25] ISO/IEC, "ISO/IEC 27004:2009. Information technology – Security techniques – Information security management – Measurement," ed, 2009.

[26] ISO/IEC, "ISO/IEC 27005:2008. Information technology – Security techniques – Information security risk management," ed, 2008.

[27] ISO/IEC, "ISO/IEC 27006:2007. Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems," 2007.

[28] ISO/IEC, "27007. Information technology – Security techniques – Guidelines for Information security management systems auditing.

[29] ITGI. (2007). COBIT 4.1: Marco de Trabajo, objetivos de control, directrices gerenciales y modelos de madurez. Available: www.itgi.org.

El Spyware como amenaza contra navegadores web

Sergio Castillo-Pérez*, José Alfredo Múrcia Andrés‡, Joaquin Garcia-Alfaro†‡

* Universitat Autònoma de Barcelona, Edifici Q, 08193, Bellaterra
† Institut Telecom, Telecom Bretagne, 35576, Cesson-Sevigne, France
‡ Universitat Oberta de Catalunya, Rambla de Poblenou 156, 08018, Barcelona

***Resumen*—En la última década se ha realizado un progreso sustancial en Internet y en las tecnologías basadas en el paradigma web. Aplicaciones relacionadas con educación, salud, banca, o incluso con relaciones entre individuos o grupos sociales, pueden beneficiarse mediante el uso de dichas tecnologías. Sin embargo, los ataques a sistemas pueden comprometer drásticamente la privacidad de los usuarios que hacen uso de las tecnologías web. En este contexto, la infección de sistemas mediante Spyware es un claro ejemplo. En este artículo analizamos la amenaza del Spyware como vía para comprometer la seguridad y privacidad de los recursos de los navegadores web.**

I. Introducción

El uso del paradigma web en todos los modelos de negocios y organizaciones está convirtiéndose en un aspecto omnipresente. De hecho, su uso aparece como una estrategia emergente en todos los tipos de aplicaciones software de las compañías [1]. Éste permite el diseño de aplicaciones totalmente interactivas que pueden potencialmente ser usadas por miles de usuarios alrededor del mundo. La existencia de nuevas tecnologías para mejorar las características del paradigma web tradicional permite a los ingenieros del software concebir nuevos servicios, que no están restringidos a un sistema operativo específico. Sistemas tradicionales de información relacionados con la educación, salud, banca o incluso sistemas de emergencia, pueden beneficiarse de esta tecnología.

La complejidad actual del paradigma web tiene, sin embargo, un impacto en la seguridad de los navegadores web y, de forma más precisa, en el tratamiento de sus recursos. Los ataques contra navegadores web pueden comprometer la seguridad y la privacidad de los usuarios. Esto puede tener serias consecuencias dada la omnipresencia de software malicioso, como el Spyware. El Spyware puede ser instalado de forma secreta en los navegadores web y robar datos sensibles, tales como identificaciones de usuarios, contraseñas o datos financieros [7]. Los navegadores web deben, por tanto, incluir mecanismos confiables para garantizar la seguridad y privacidad de sus usuarios. En este artículo damos una visión general de algunas técnicas usadas por el Spyware, y que pueden ser usadas por entidades maliciosas para violar la privacidad de los usuarios. Presentamos un escenario que muestra cómo la privacidad de un usuario accediendo a un servicio web puede ser violada por Spyware vinculado al navegador web. Seguidamente discutimos algunos mecanismos de defensa que pueden reducir el riesgo representado por la amenaza del Spyware.

Organización del artículo — La sección II presenta la amenaza del Spyware y desarrolla nuestro escenario de motivación. La sección III presenta una visión general sobre mecanismos de defensa para reducir el riesgo de la amenaza del Spyware. La sección IV concluye el artículo.

II. Spyware

El concepto Spyware (o software espía) es un término utilizado para catalogar al software malicioso (*Malware*) [11] que registra información de usuarios de forma no consentida, violando la privacidad de éstos. La información recolectada por este tipo de aplicaciones suele ser de distinta índole, tal como datos personales, números de tarjeta de crédito, hábitos de navegación web, contraseñas, pulsaciones de teclas, o captura de pantalla. Tal información es transmitida a terceras partes con finalidades como son el fraude electrónico [6], el marketing a través de publicidad web no consentida, u otras actividades normalmente maliciosas. Con la finalidad de conseguir su propósito, dicho software provoca diversos efectos en el comportamiento del sistema afectado, como la aparición de ventanas de navegación con publicidad no deseada, el secuestro del navegador web, instalación de puertas traseras (*backdoors*), modificación de los números de conexión a ISPs a otros con tarifas elevadas, etc. Asimismo, y con motivo de llevar a cabo su finalidad, la ejecución de estas aplicaciones suele conllevar la degradación del rendimiento del sistema, incrementando el uso de CPU, del espacio utilizado en disco, o del ancho de banda de red.

A lo largo del tiempo, el Spyware ha evolucionado incorporando sofisticados mecanismos propios de los rootkits. Estos mecanismos permiten al Spyware esconder su presencia a administradores o a software destinado a su detección. Así, estrategias como la ocultación de procesos, archivos o conexiones de red, o el uso de técnicas antidebugging o de criptografía, suelen ser características habituales en el Spyware de hoy en día. De forma análoga, y con el objetivo de no ser eliminados del sistema infectado, la inclusión de estrategias que dificultan su desinstalación son propiedades comunes en este tipo de software. Este conjunto de metodologías evasivas, junto a los mecanismos para la recopilación de información en sí, suele conllevar la utilización de técnicas de programación que, en ocasiones, provocan cierta inestabilidad del sistema, dando lugar a un comportamiento inesperado de algunas aplicaciones.