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

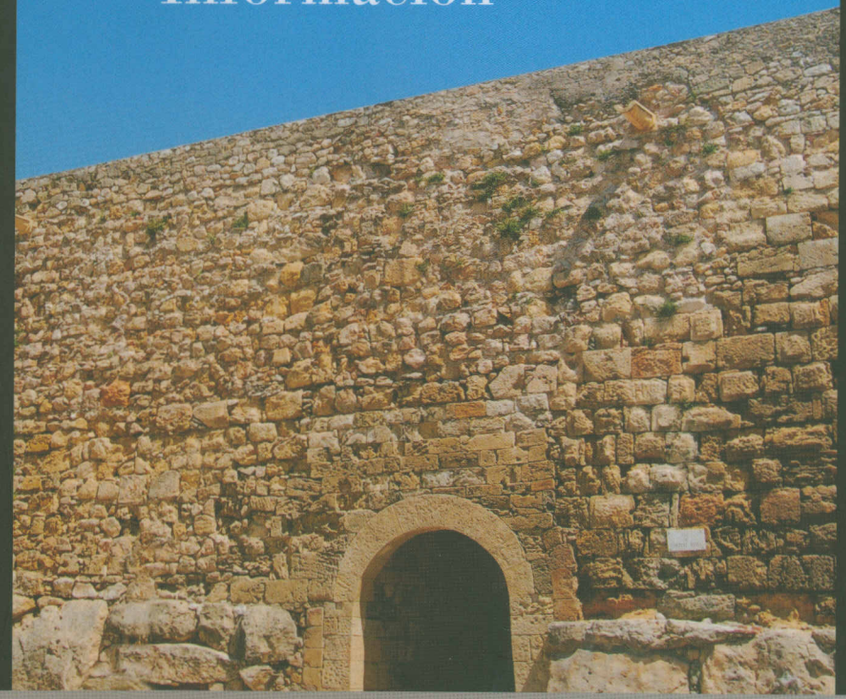
RECSI 2010 | XI Reunión Española sobre Criptología y Seguridad de la Información

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

Patrones de Seguridad: ¿Homogéneos, validados y útiles?

Santiago Moral-García
Grupo Kybele
Dep. de Lenguajes y Sistemas Informáticos II
Universidad Rey Juan Carlos
Email: santiago.moral@urjc.es

Roberto Ortiz
S21sec Labs. SOC
Grupo S21sec Gestión S.A.
Email: rortiz@s21sec.com

Belén Vela
Grupo Kybele
Dep. de Lenguajes y Sistemas Informáticos II
Universidad Rey Juan Carlos
Email: belen.vela@urjc.es

Javier Garzás
Grupo Kybele
Dep. de Lenguajes y Sistemas Informáticos II
Universidad Rey Juan Carlos
Kybele Consulting
Email: javier.garzas@urjc.es; javier.garzas@kybeleconsulting.com

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

***Resumen*—Actualmente, la seguridad de la información es uno de los pilares principales en la gestión de las organizaciones. La evolución de los sistemas conlleva un aumento de su complejidad, y esto a su vez ha derivado en un incremento de los ataques a los sistemas de información, ya que hay muchas más posibilidades de que los atacantes encuentren nuevas vulnerabilidades. Por todo esto, es necesario proveer a los diseñadores de sistemas de soluciones fiables para minimizar este número de ataques y conseguir un menor impacto en su organización. Los patrones de seguridad son un buen mecanismo para aportar soluciones a problemas concretos de seguridad, ya que proporcionan soluciones estructuradas que solventan problemas recurrentes. Existen muchas propuestas enfocadas a la creación de nuevos patrones de seguridad, pero en la actualidad no se utilizan unas pautas homogéneas para realizar su descripción. Además, la mayoría de patrones existentes difícilmente pueden ser aplicables en el diseño de sistemas complejos, ya que en su descripción no contemplan la complejidad de las instalaciones reales. En este artículo se va a realizar una síntesis de un conjunto de propuestas que describen patrones de seguridad, basada en una revisión sistemática realizada anteriormente. Posteriormente se va a realizar un análisis en relación al contexto en el que se utilizan los patrones de seguridad, las plantillas y elementos que se usan a la hora de describir este tipo de patrones y además se estudiará la aplicabilidad de éstos en entornos reales. Finalmente se realizará una discusión para detectar las carencias ofreciendo a su vez una serie de propuestas de mejora.**

***Palabras Clave*—patrones, patrones de seguridad, seguridad de la información.**

I. Introducción

En los últimos años los avances tecnológicos están mejorando multitud de aspectos relacionados con el diseño y desarrollo de los Sistemas de Información (SI), provocando un crecimiento de la funcionalidad y aplicación de la que son dotados estos sistemas. Este crecimiento conlleva un aumento de la complejidad de los SI, incrementando el impacto de los ataques informáticos, ya que los atacantes tienen más posibilidades de encontrar nuevas vulnerabilidades en los sistemas, tales como Cross-Site Scripting, inyección de código, ejecución de ficheros maliciosos, etc. [1].

Por esta razón, la seguridad de la información es una de las principales preocupaciones que tienen las organizaciones en los últimos años. Por un lado, las compañías quieren evitar que su información esté en peligro y por otro lado, hay un incremento de ataques informáticos debido a los beneficios que pueden obtener los atacantes con la información que sustraen de las organizaciones. Debido a estos ataques, los diseñadores de SI deben incluir requisitos de seguridad a la hora de diseñar sus sistemas, es decir, deben asegurar la confidencialidad, integridad y disponibilidad de los datos siempre que sea necesario, para así, proteger los activos de información de la organización. La importancia en el diseño de sistemas seguros ha aumentado desde que la mayoría de los ataques a sistemas de software están basados en vulnerabilidades causadas por un deficiente diseño y desarrollo de las funcionalidades de las que se dota a los sistemas [2]. Para evitar estas deficiencias, los diseñadores de SI necesitan elaborar soluciones específicas para resolver problemas relacionados con las vulnerabilidades de seguridad, y así minimizar el número de ataques exitosos contra sus SI.

Los patrones son una buena forma de satisfacer esta necesidad, ya que describen un problema que ocurre una y otra vez en un entorno, proporcionando una solución documentada y validada que puede ser usada múltiples veces [3]. Una de las principales ventajas de los patrones es que combinan experiencia y buenas prácticas en el diseño de SI [4], haciéndolo más eficiente. También es importante resaltar que los patrones no son una solución a un problema propuesto, sino una guía homogénea que documenta cómo problemas similares fueron resueltos anteriormente.

Por lo tanto, los diseñadores de SI podrían usar patrones de seguridad para obtener soluciones fiables relacionadas en este campo, ya que son un buen mecanismo para optimizar

el proceso de decisión a la hora de resolver un problema de seguridad recurrente. Otra ventaja que encontramos en los patrones de seguridad es que incorporan un conocimiento extenso acumulado sobre seguridad de forma estructurada, proporcionando una serie de pautas para el diseño, construcción y evaluación de SI seguros [5].

La utilización de patrones de seguridad como guía para diseñar un SI seguro es una práctica bastante extendida [6, 7, 8, 9]. De hecho, en los últimos años, el número de patrones de seguridad publicados ha crecido de manera considerable [10, 11, 12, 13, 14]. Sin embargo, existe una gran variedad y diversidad en las pautas de descripción de cada una de las propuestas [15, 16, 17, 18], incluso, en repetidas ocasiones, se han propuesto varios patrones diferentes que dan respuesta al mismo conjunto de requisitos o problemas de seguridad [19, 20], es decir, existe una superposición de soluciones.

En este artículo se va a realizar una síntesis sobre las principales propuestas que describen patrones de seguridad, basada en una revisión sistemática que se ha realizado previamente, siguiendo la propuesta de [21]. El objetivo principal del trabajo que aquí se presenta es realizar un análisis sobre el contexto en el que se emplean los patrones de seguridad, las plantillas utilizadas para describirlos y los elementos usados en estas descripciones. Adicionalmente, se va a comprobar cuántas propuestas están basadas y validadas en casos reales y cuántas en ejemplos teóricos. Este estudio ayudará a verificar la aplicabilidad que tienen los patrones de seguridad analizados en procesos de diseño de SI reales.

El resto del artículo se organiza de la siguiente manera. En la Sección II se realiza una síntesis de un conjunto de propuestas que describen patrones de seguridad. La Sección III muestra los resultados obtenidos y expone una discusión sobre los mismos. Finalmente, la Sección IV presenta las principales conclusiones y los trabajos futuros.

II. Síntesis de Propuestas de Patrones de Seguridad

En esta sección se va a realizar una síntesis de las principales propuestas que describen patrones de seguridad. Debido a la diversidad de soluciones que se proponen, agruparemos los trabajos según la problemática que solucionan los patrones que describen.

A. Patrones de seguridad para comunicaciones seguras

En este apartado se han agrupado los artículos relacionados con soluciones de seguridad centradas en el ámbito de las comunicaciones entre los distintos sistemas, y el envío y recepción de mensajes que realizan.

En [22] se presentan cuatro patrones de seguridad que pueden ser utilizados para el diseño seguro de sistemas VoIP, ya que proponen soluciones que pueden controlar muchos de los posibles ataques brindando un entorno de trabajo para ayudar a los diseñadores a aplicar la seguridad en sus SI.

En [23] se proponen tres patrones de diseño para las implementaciones de sistemas VoIP en relación con problemas de seguridad específicos. Se propone una técnica de cifrado y descifrado para paquetes de voz y añaden una nueva propuesta de generación de claves. También desarrollan un módulo de IPsec para sistemas VoIP en entornos Cliente/Servidor.

En [24] se presenta un patrón para reforzar el canal de comunicaciones entre diferentes sistemas. Este patrón puede ayudar a los diseñadores de SI agregando controles de seguridad en la fase de procesado del flujo de datos.

B. Patrones de seguridad para control de acceso e identificación seguros

En este apartado se incluyen trabajos que muestran patrones para aumentar la seguridad de los SI, reforzándolos con mecanismos efectivos de identificación, autorización, autenticación y control de acceso.

En [25] se propone un lenguaje de patrones para el sistema de gestión de identidades, compuesto por tres patrones. Este lenguaje de patrones está basado en SAML (Security Assertion Markup Language), que proporciona un formato específico para la comunicación de información acerca de la identidad de los diferentes dominios de seguridad.

En [26] se describe una solución de control de acceso, para los datos generados por sensores inalámbricos. Esta propuesta está formada por tres patrones de seguridad que definen un modelo abstracto de control de acceso basado en criptografía.

En [27] se propone un patrón de seguridad que describe el uso de la identificación de la información de credenciales para definir la autenticación y el control de acceso. Este patrón está descrito para ser usado en sistemas distribuidos con el fin de asegurar estos requisitos.

En [28] se describen varios patrones para abordar aspectos relativos a las sesiones en modelos de control de acceso. Los autores muestran un patrón que controla el acceso de las diferentes sesiones, describiendo cómo una sesión puede limitar el derecho de un usuario. Además, se utilizan dos patrones más, que combinados con el patrón anterior, pueden constituir un patrón específico de control de acceso. Por último, esta propuesta muestra un entorno de trabajo real basado en el conjunto de patrones descrito.

C. Patrones de seguridad para garantizar la privacidad

En este apartado se incluyen los trabajos que proponen soluciones al problema de la privacidad tratando de preservar este aspecto utilizando patrones de seguridad. La privacidad es muy relevante en los intercambios de datos personales entre los usuarios y sistemas.

En [29] se presenta un conjunto de patrones para la estandarización del desarrollo de políticas de privacidad con el fin de ser utilizado en sitios web. Estos patrones consideran principalmente aspectos relacionados con la seguridad, la información del usuario y la privacidad. Además, los autores muestran un ejemplo ficticio de una política de privacidad en la que se combinan todos los patrones descritos en la propuesta, pudiendo ser aplicada en un sitio web.

En [18] se presentan dos patrones de seguridad: uno para la manipulación de cookies, que protege la identidad de los usuarios cuando tienen acceso a un sitio web y otro, que permite a los usuarios utilizar un servicio de correo electrónico sin revelar su propia identidad.

En [30] los autores enfocan su trabajo en mejorar los patrones de privacidad existentes. Además, para reforzar este escenario se describen tres patrones adicionales. Estos nuevos patrones pueden ayudar a preservar la privacidad pretendiendo que las organizaciones online, los diseñadores de páginas web y los usuarios puedan utilizar información personal sin ningún problema de seguridad.

D. Patrones de ataque y de mal uso

En este apartado se incluyen los trabajos que describen otro tipo de patrones de seguridad: los patrones de ataque y los patrones de mal uso. En este tipo de patrones los autores se colocan en el lado del atacante y describen paso a paso todos los elementos del ataque a un sistema. Para ello definen el contexto del ataque, exponen los patrones de seguridad que lo neutralizan y proponen mecanismos para trazar las evidencias que deja el ataque una vez que ha ocurrido.

En [16] se propone un patrón de uso indebido y se presenta un modelo que expone la estructura de este tipo de patrón. De manera similar al anterior trabajo, en [31] se presenta un patrón de ataque, que proporciona una descripción específica de los objetivos del ataque. Además, se presenta como ejemplo ficticio un ataque de denegación de servicio en las redes de tipo VoIP para demostrar la efectividad del patrón expuesto.

E. Patrones de seguridad para mejorar la relación de confianza

En este apartado se incluyen los trabajos que proponen patrones de seguridad para reforzar las relaciones de confianza entre el usuario y los sistemas o entre dos usuarios, para tratar de cumplir los requisitos fundamentales de seguridad.

En [32] se presenta un patrón de seguridad para desarrollar una interfaz gráfica de usuario segura. Este patrón puede ayudar a reforzar los sistemas de interfaz gráfica de usuario y evaluar su uso en diferentes ámbitos. Además, se muestra cómo analizar los requisitos de seguridad para fomentar la confianza, preservando al mismo tiempo la flexibilidad que demandan las interfaces gráficas de usuario.

En [33] se describen patrones para reforzar las relaciones de confianza entre diferentes usuarios. Estos patrones permiten que dos usuarios puedan verificar mutuamente el perfil del otro sin revelar su identidad.

F. Otros patrones de seguridad para construir sistemas seguros

En este apartado se muestran varias propuestas para construir sistemas seguros utilizando patrones de seguridad, tanto de diseño como arquitectónicos.

En [34] se propone un patrón para reforzar las arquitecturas basadas en tres capas. Este patrón puede ser aplicado a sistemas distribuidos y enfocado a la ejecución de aplicaciones complejas y heterogéneas. Hay distintos debates sobre las propiedades del patrón arquitectónico en tres capas, así como varios patrones desarrollados [35, 36], pero ninguno de éstos considera la seguridad.

En [37] se describen patrones de seguridad para la representación de los procesos y subprocesos de los sistemas operativos. Como los sistemas operativos son muy críticos, los autores proponen varios patrones para resolver sus problemas de seguridad.

En [38] se introducen patrones para monitorizar las propiedades de seguridad básicas de un SI. Con ellos se puede comprobar, en tiempo de ejecución, la robustez de los requisitos generales de seguridad de un SI.

III. Resultados y Discusión

Como se ha mostrado en la sección anterior, existe una gran variedad de propuestas que trabajan descubriendo nuevos patrones de seguridad en relación a las necesidades de los SI. En esta sección se van a analizar, por un lado, los criterios de descripción utilizados en las propuestas sintetizadas y por otro lado, los entornos en los que son aplicados los patrones descritos. Finalmente, se mostrará una discusión en relación a los resultados obtenidos y se propondrán una serie de mejoras.

En la Figura 1 se muestran horizontalmente las referencias de los trabajos sintetizados y el contexto al que pertenece cada uno de ellos, siguiendo la estructura de los apartados descritos en la sección anterior. Verticalmente se muestran las plantillas que han sido utilizadas para describir las propuestas, detallando los elementos utilizados en la descripción de cada uno de los patrones de seguridad. Las plantillas de descripción incluidas en la Figura 1 son, la plantilla resultante de la fusión de elementos de la plantilla propuesta por Gang of Four [39] adaptada a los patrones de seguridad y de la plantilla propuesta por Buschmann et al. [40] denominada PoSA, la plantilla propuesta en el proyecto SERENITY utilizada en [26], la plantilla propuesta por Alexander [3], y la plantilla de descripción de patrones en forma de eventos de cálculo [38]. Se sombrearán las casillas que correspondan a las plantillas o elementos de descripción que utilicen cada una de las propuestas respectivamente. Como se puede extraer de la Figura 1 y más concretamente de las columnas que representan las plantillas utilizadas en la descripción de patrones, no existe una plantilla estándar que sirva de guía para la descripción de patrones de seguridad que pueda ser utilizada por los expertos en esta materia. Esta situación provoca una variabilidad significativa en relación a los elementos que componen un patrón de seguridad. Como se observa en las columnas que se refieren a los elementos utilizados en las descripciones de patrones, cada autor describe los patrones siguiendo sus propias directrices, aunque existen algunos elementos comunes de las diferentes plantillas [18, 26, 30]. Incluso utilizando la misma plantilla, algunos autores no repiten en su totalidad todos los elementos de ésta, probablemente fruto de evolución en sus propuestas y tratando de mejorar la usabilidad de los patrones, optan por añadir nuevos elementos [25, 27, 29].

Los elementos más utilizados en las descripciones de patrones de seguridad son la tripleta "Contexto", "Problema" y "Solución" propuesta en [3]. Esto demuestra que existe

Contexto de Patrones	Referencias	Plantillas de Representación				Elementos para describir los patrones																									
		Gang of Four + ProSA	SERENITY	Alexander	Eventos de Cálculo	Nombre	Intención	Ejemplos	Contexto	Problema	Solución	Implementación	Consecuencias	Patrones Relacionados	Usos conocidos	Casos Reales/Escenarios	Estructura	Dinámica	Ejemplos resueltos	Ver también	Precondiciones	Propiedades	Características	Fuerzas	*	Reglas	Variantes	Evidencias
Comunicaciones	[22]																														
	[23]																														
	[24]																														
Gestión de la Identidad	[25]																														
	[26]								2	2	1																				
	[27]																														
	[28]																														
Privacidad	[29]																														
	[18]																														
	[30]																														
Punto de Vista del Atacante	[16]																														
	[31]																														
Relaciones de Confianza	[32]																														
	[33]								2	2	1																				
Arquitecturas 3 capas	[34]																														
Sistemas Operativos	[37]																														
Monitorización de la Seguridad	[38]																														

1. Estos trabajos desarrollan el elemento de descripción "Solución" con más detalle
2. Estos trabajos contienen una sección con los siguientes elementos: problema/requisitos y contexto
*. Sección que contiene los siguientes elementos: Seguridad / Acceso / Elección / Transparencia

Fig. 1. Características de las propuestas estudiadas

una necesidad por parte de los investigadores de definir una serie de conceptos básicos a la hora de documentar un patrón descubierto, pero al carecer de una plantilla estándar para exponer los patrones de seguridad, se genera una diversidad muy destacada en las distintas descripciones. Debido a esta diversidad aumenta la complejidad para realizar un catálogo homogéneo de patrones de seguridad, ya que es difícil unificar toda la literatura existente sobre éstos. Este hecho también puede provocar que los diseñadores de SI tengan cada vez más dificultad a la hora de seleccionar los patrones más apropiados para unos determinados requisitos de seguridad dados [41]. Localizado este problema se detecta la necesidad de diseñar un conjunto de pautas que recojan una serie de características esenciales para la descripción de los patrones de seguridad, con el fin de conseguir un catálogo homogéneo. La principal aportación de este catálogo sería conseguir soluciones equivalentes entre distintos diseñadores de SI seguros.

Adicionalmente al análisis realizado sobre las distintas descripciones utilizadas en el diseño de patrones de seguridad, se ha realizado un análisis sobre los entornos en los que son validadas las propuestas seleccionadas. En la Figura 2 se muestran los porcentajes de las propuestas que han sido validadas en entornos reales (SI), las que han sido validadas parcialmente en entornos reales (PARCIALMENTE), es decir, han simulado un entorno real a pequeña escala y las que están basadas en casos de laboratorio (NO). Como se puede observar en la Figura 2, el 59% de las propuestas seleccionadas están basadas en ejemplos teóricos o casos de laboratorio, el 29% de ellas están validadas en un entorno real simulado, mientras que sólo el 12% de las propuestas han sido validadas completamente en entornos reales.

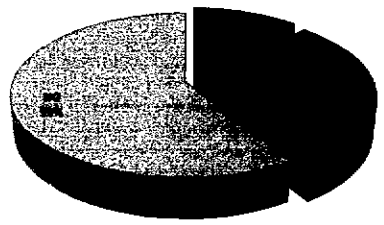


Fig. 2. Propuestas validadas en entornos reales

Tras realizar este análisis se detecta una carencia de visión real en los patrones de seguridad, es decir, no se expone una aproximación práctica específica para el diseño de SI seguros basado en patrones de seguridad. Este aspecto difiere en su totalidad de la propia definición de patrón, que precisamente declara que una de las principales bondades de los patrones es que proporcionan soluciones validadas que resuelven problemas similares. Este hecho puede provocar una escasa aplicabilidad de los patrones de seguridad en diseños de SI reales, ya que probablemente éstos no han sido generados cómo conclusión de la solución a un problema en un entorno real complejo.

Un patrón de seguridad debería servir para simplificar la toma de decisiones de un ingeniero de seguridad de la información a la hora de diseñar un nuevo SI o implantar un nuevo sistema dentro de un sistema mayor, reduciendo el tiempo y el coste del análisis de seguridad. Desde nuestra experiencia, a la hora de realizar el análisis de seguridad de un SI en un entorno real es necesario considerar los aspectos relativos a: a) el número de elementos físicos y lógicos que componen el SI; b) la gestión y aprovisionamiento de usuarios; c) el proceso de copias de seguridad y sobre qué elementos habría que realizarlas; d) la trazabilidad de la solución aportada; e) la expansión de la solución de forma masiva; f) el impacto en los parámetros básicos de un SI, la memoria, la capacidad de proceso, el almacenamiento, el ancho de banda consumido, etc. Por todo esto, los patrones de seguridad basados en casos de laboratorio difícilmente pueden ser utilizados en un proceso de diseño de un SI real, ya que la mayoría no tienen en cuenta la complejidad de las instalaciones reales incumpliendo las premisas anteriores cuando son diseñados. En caso de ser utilizados por un ingeniero de SI, existe la posibilidad que aumente el tiempo y el coste del análisis de seguridad en el ciclo de vida del diseño del SI.

Para concluir este apartado se van a exponer las necesidades detectadas tras el análisis realizado. En primer lugar, hay que destacar la complejidad que presenta ofrecer actualmente, tanto al experto como al no experto en seguridad, una guía de soluciones reutilizables, a fin de que sea usada para diseñar un sistema seguro, ya que como queda demostrado, no es tarea fácil alinear los diferentes criterios de descripción en el ámbito de los patrones de seguridad. Por este motivo, se detecta la necesidad de establecer una metodología dentro del ámbito de la Seguridad de la Información en la que paso a paso, se describa cómo resolver un problema utilizando patrones de seguridad. Esta metodología debería aportar soluciones equivalentes entre distintos diseñadores de SI, con el fin de que esas soluciones puedan ser utilizadas por cualquiera que lo necesite, beneficiándose sin necesidad de tener conocimientos avanzados en el campo de la seguridad. Las soluciones aportadas llegarían a ser reutilizables y exportables, ya que recogerían todas las características técnicas del sistema, las personas involucradas en la solución planteada, etc. Además, se detecta una clara necesidad de crear soluciones de seguridad estructuradas en forma de patrones que reflejen soluciones validadas en entornos reales complejos siguiendo las premisas que se han expuesto anteriormente. Finalmente, se detecta la necesidad de enriquecer y completar la descripción de los patrones de seguridad actuales, con un conjunto de elementos que describan los aspectos principales para un diseñador de SI a la hora de implementar la solución en instalaciones reales, con el fin de aumentar la aplicabilidad de estos patrones ya descubiertos en este tipo de entornos.

IV. Conclusiones y Trabajos Futuros

En este trabajo se han sintetizado un conjunto de propuestas que describen patrones de seguridad. Se puede observar que el número de estudios dentro de este ámbito es muy elevado y abarca distintos contextos, encontrando gran heterogeneidad en el proceso de creación de patrones descrito por los distintos investigadores. Cada uno de los enfoques selecciona un conjunto distinto de elementos para realizar la descripción de los patrones, provocando un aumento de complejidad al realizar una clasificación homogénea de los patrones existentes. Por este motivo, los diseñadores de los SI pueden tener una mayor dificultad a la hora de seleccionar una serie de patrones apropiados para diseñar sus sistemas seguros. Por todo esto, se cree necesario definir un conjunto de pautas de descripción de patrones de seguridad que sea aceptado y utilizado por todos los investigadores relacionados con este campo.

Partiendo de la base de que los patrones por definición son un mecanismo validado, en la realización del estudio se han encontrado muy pocas propuestas validadas en entornos reales complejos. Por nuestra experiencia, los patrones de seguridad deberían considerar aspectos tales como medidas volumétricas de los parámetros básicos de un SI (memoria, capacidad de proceso, almacenamiento, etc.), gestión de usuarios, medidas de complejidad de uso, tanto para administradores como para usuarios finales, etc. En la actualidad, los patrones existentes no contemplan estos aspectos, por lo que se propone una profunda investigación para descubrir nuevos patrones que sí los reflejen. Además, se considera necesaria una evolución de los patrones existentes para cubrir las necesidades anteriores. Por último, se propone el desarrollo de una metodología de seguridad basada en patrones que guie al usuario a la hora de afrontar un problema en este ámbito. Esta metodología debería ser útil para cualquier tipo de diseñador de sistemas de seguridad, ya sea experto o no en este ámbito.

En trabajos futuros, se pretende abordar el desarrollo de una serie de pautas que recojan un conjunto de características principales para la definición de nuevos patrones de seguridad, con el fin de mantener un criterio equivalente entre las distintas propuestas que se vayan realizando. También, se pretende descubrir nuevos patrones de seguridad que cumplan los requisitos expuestos para aplicarlos en entornos reales. Finalmente, se propondrá una metodología de seguridad basada en patrones que aporte soluciones homólogas, validadas y reutilizables. Esta metodología servirá para dar soporte a los diseñadores de SI seguros para que paso a paso sepan cómo afrontar un problema de seguridad guiándoles para que lo resuelvan de la manera más óptima y eficiente posible.

Agradecimientos

Esta investigación ha sido llevada a cabo en el entorno de trabajo de los siguientes proyectos: MODEL-CAOS (TIN2008-03582/TIN) financiado por el Ministerio de Educación y Ciencia de España, IDONEO (PAC08-0160-6141).

QUASIMODO (PAC08-0157-0668), SISTEMAS (PII2I09-0150-3135) y SEGMENT (HITO-09-138) financiados por la Viceconsejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha y FEDER y el proyecto BUSINESS (PET2008-0136) financiado por el Ministerio de Ciencia e Innovación de España.

REFERENCIAS

[1] "The Open Web Application Security Project (OWASP)",http://www.owasp.org

[2] S. T. Halkidis, N. Tsantalis, A. Chatzigeorgiou y G. Stephanides "Architectural Risk Analysis of Software Systems Based on Security Patterns" *IEEE Transactions on Dependable and Secure Computing*, pp. 129-142, 2008.

[3] C. Alexander, S. Ishikawa y M. Silverstein "*A Pattern Language: Towns, Buildings, Constructions*" Oxford University Press, 1977.

[4] E. Fernandez "Security Patterns and Secure Systems Design" en *Dependable Computing*, 2007, pp. 233-234.

[5] E. Fernandez, H. Washizaki, N. Yoshioka, A. Kubo y Y. Fukazawa "Classifying Security Patterns" en *Progress in WWW Research and Development*, 2008, pp. 342-347.

[6] E. B. Fernandez, J. Wu, M. M. Larrondo-Petrie y Y. Shao "On building secure SCADA systems using security patterns" en *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies* Oak Ridge, Tennessee: ACM, 2009.

[7] A. Maña, D. Serrano, J. F. Ruiz, A. Armenteros, B. G. N. Crespo y A. Muñoz "Development of Applications Based on Security Patterns" en *DEPEND '09. Second International Conference on Dependability*, 2009, pp. 111-116.

[8] C. Steel, R. Nagappan y R. Lai "*Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management*", Prentice Hall ed., 2005.

[9] M. Schumacher y U. Roedig "Security engineering with patterns" *PLoP 2001 Conference*, 2001.

[10] M. Schumacher, E. Fernandez-Buglioni, D. Hybertson, F. Buschmann y P. Sommerlad "*Security Patterns: Integrating Security and Systems Engineering*", Wiley ed., 2006.

[11] K. Yskout, T. Heyman, R. Scandariato y W. Joosen "An inventory of security patterns" *Technical Report CW-469, Katholieke Universiteit Leuven, Department of Computer Science*, 2006.

[12] D. G. Rosado, C. Gutiérrez, E. Fernández-Medina y M. Piattini "Security patterns and requirements for internet-based applications" *Internet Research: Electronic Networking Applications and Policy*, 2006.

[13] B. Blakley y C. Heath "Security Design Patterns. The Open Group Security Forum" 2004.

[14] D. M. Kienzle, M. C. Elder, D. Tyree y J. Edwards-Hewitt "Security patterns repository, version 1.0" 2006.

[15] J. Garzás y M. Piattini "Object Oriented Microarchitectural Design Knowledge" *IEEE Software*, pp. 28-33, 2005.

[16] E. B. Fernandez, N. Yoshioka y H. Washizaki "Modeling Misuse Patterns" en *ARES '09. International Conference on Availability, Reliability and Security*, 2009, pp. 566-571.

[17] Z. Anwar, W. Yurcik, R. E. Johnson, M. Hafiz y R. H. Campbell "Multiple design patterns for voice over IP (VoIP) security" en *Performance, Computing, and Communications Conference, 2006. IPCCC 2006. 25th IEEE International*, 2006, pp. 8 pp.-492.

[18] M. Schumacher "B. Example Security Patterns and Annotations" en *Security Engineering with Patterns*, 2003, pp. 171-178.

[19] A. Sarmah, S. M. Hazarika y S. K. Sinha "Security Pattern Lattice: A Formal Model to Organize Security Patterns" en *DEXA '08. 19th International Conference on Database and Expert Systems Application*, 2008, pp. 292-296.

[20] E. Fernandez, G. Pernul y M. Larrondo-Petrie "Patterns and Pattern Diagrams for Access Control" en *Trust, Privacy and Security in Digital Business*, 2008, pp. 38-47.

[21] B. Kitchenham "Guideline for performing Systematic Literature Reviews in Software Engineering. Version 2.3" *University of Keele (Software Engineering Group, School of Computer Science and Mathematics) and Durham (Department of Computer Science)*, 2007.

[22] E. B. Fernandez, J. C. Pelaez y M. M. Larrondo-Petrie "Security Patterns for Voice over IP Networks" en *ICCGI 2007. International Multi-Conference on Computing in the Global Information Technology*, 2007, pp. 33-33.

[23] N. A. Chavhan y S. A. Chhabria "Multiple design patterns for voice over IP security" en *Proceedings of the International Conference on Advances in Computing, Communication and Control* Mumbai, India: ACM, 2009.

[24] E. B. Fernandez y J. L. Ortega-Arjona "The Secure Pipes and Filters Pattern" en *DEXA '09. 20th International Workshop on Database and Expert Systems Application*, 2009, pp. 181-185.

[25] N. Delessy, E. B. Fernandez y M. M. Larrondo-Petrie "A Pattern Language for Identity Management" en ICCGI 2007. *International Multi-Conference on Computing in the Global Information Technology*, 2007, pp. 31-31.

[26] A. Cuevas, P. El Khoury, L. Gomez y A. Laube "Security Patterns for Capturing Encryption-Based Access Control to Sensor Data" en *SECURWARE '08. Second International Conference on Emerging Security Information, Systems and Technologies*, 2008, pp. 62-67.

[27] P. Morrison y E. B. Fernandez "The credentials pattern" en *Proceedings of the 2006 conference on Pattern languages of programs* Portland, Oregon: ACM, 2006.

[28] E. B. Fernandez y G. Pernul "Patterns for session-based access control" en *Proceedings of the 2006 conference on Pattern languages of programs* Portland, Oregon: ACM, 2006.

[29] L. L. Lobato, E. B. Fernandez y S. D. Zorzo "Patterns to Support the Development of Privacy Policies" en *ARES '09. International Conference on Availability, Reliability and Security*, 2009, pp. 744-749.

[30] S. Romanosky, A. Acquisti, J. Hong, L. F. Cranor y B. Friedman "Privacy patterns for online interactions" en *Proceedings of the 2006 conference on Pattern languages of programs* Portland, Oregon: ACM, 2006.

[31] E. Fernandez, J. Pelaez y M. Larrondo-Petrie "Attack Patterns: A New Forensic and Design Tool" en *Advances in Digital Forensics III*, 2007, pp. 345-357.

[32] T. Fischer, A. R. Sadeghi y M. Winandy "A Pattern for Secure Graphical User Interface Systems" en *DEXA '09. 20th International Workshop on Database and Expert Systems Application*, 2009, pp. 186-190.

[33] A. Sorniotti, P. El Khoury, L. Gomez, A. Cuevas y A. Laube "A Security Pattern for Untraceable Secret Handshakes" en *SECURWARE '09. Third International Conference on Emerging Security Information, Systems and Technologies*, 2009, pp. 8-14.

[34] E. B. Fernandez, M. Fonoage, M. VanHilst y M. Marta "The Secure Three-Tier Architecture Pattern" en *CISIS 2008. International Conference on Complex, Intelligent and Software Intensive Systems*, 2008, pp. 555-560.

[35] A. Aarsten, D. Brugali, G. Menga, K. Brown y R. Hirschfeld "Patterns of three-tier client server architectures" *Proceedings of the 1996 Pattern Languages of Programs (PLoP) Conference, Monticello, IL, September 1996*, 1996.

[36] O. Vogel "EuroPLoP 2001 design fest designing a three-tier architecture pattern language" *Design Fest EuroPLoP 2001, POSA3, Irsee, Germany, July 2001*, 2001.

[37] E. B. Fernandez, T. Sorgente y M. M. Larrondo-Petrie "Even more patterns for secure operating systems" en *Proceedings of the 2006 conference on Pattern languages of programs* Portland, Oregon: ACM, 2006.

[38] G. Spanoudakis, C. Kloukinas y K. Androutsopoulos "Towards security monitoring patterns" en *Proceedings of the 2007 ACM symposium on Applied computing* Seoul, Korea: ACM, 2007.

[39] E. Gamma, R. Helm, R. Johnson y J. M. Vlissides "Design Patterns: Elements of Reusable Object Oriented Software" *Addison Wesley*, 1995.

[40] F. Buschmann, R. Meunier, H. Rohnert, P. Sommerlad y M. Stal. "Pattern-oriented software architecture" *Wiley*, 1996.

[41] M. Weiss y H. Mouratidis "Selecting Security Patterns that Fulfill Security Requirements" en *International Requirements Engineering, 2008. RE '08. 16th IEEE*, 2008, pp. 169-172.

Euskalert: Red Vasca de Honeypots

Urko Zurutuza, Enaitz Ezpeleta, Ignacio Arenaza, Iñaki Vélez de Mendizabal,
Jesús Lizarraga, Roberto Uribeetxeberria, Miguel Fernández
Escuela Politécnica Superior
Mondragon Unibertsitatea
Email: uzurutuza,eezpeleta,iarenaza,ivelez,jlizarraga,ruribeetxeberria,mfernandez@eps.mondragon.edu

***Abstract*—Las firmas de seguridad y especialmente los fabricantes de Antivirus dan fe del aumento exponencial de las amenazas que acechan las actividades realizadas en Internet [1], habiendo analizado más ejemplares de malware en el 2009 que en la suma de todos los años anteriores. Se constata que fabricantes de virus, gusanos, troyanos, spyware, spam etc. no realizan sus actividades maliciosas de forma aislada, sino que se trata de bandas organizadas y consolidadas [2] que buscan obtener un beneficio económico a través de sus acciones ilícitas.**

En este trabajo se presenta Euskalert, una infraestructura de máquinas trampa que recopila ataques a nivel de red y malware.

I. INTRODUCCIÓN

A lo largo de los últimos 3 años desde la Escuela Politécnica Superior de Mondragon Unibertsitatea, en adelante MU, se ha trabajado en el proyecto Euskalert [3]. Se ha implantado una red de honeypots en la Comunidad Autónoma del País Vasco (CAPV). Los participantes alojan un sensor en su red corporativa y los datos sobre los ataques son recibidos y almacenados en nuestras instalaciones, todo ello de forma eficiente y segura. Los participantes tienen a su disposición un sitio Web donde pueden consultar libremente información y estadísticas sobre los ataques recibidos, así como compararse con otros participantes de forma anónima. Una vez la plataforma se encuentra estable y con cierta capacidad de análisis, las posibilidades en cuanto a la explotación de la información tanto a nivel de red como de aplicación se multiplican.

El malware es cualquier tipo de código diseñado específicamente con intención dañina, como por ejemplo virus, gusanos, caballos de troya o spyware. Debido al exponencial aumento del malware, y por consiguiente el beneficio económico que ciberdelincuentes obtienen mediante su uso [4], [5], el estudio, análisis y mitigación representa una necesidad prioritaria para investigadores y gobiernos.

En la actualidad, la solución principal para luchar contra el malware recae en los sistemas antivirus, basados mayoritariamente en firmas sintácticas, que caracterizan instancias conocidas de malware mediante firmas. Las firmas representan el o los bytes específicos o secuencias de instrucciones que se consideran maliciosas. Cuando al escanear un fichero se identifica este patrón, es clasificado como malware. Este método ha resultado efectivo hasta el momento, cuando las amenazas son conocidas de antemano y es la solución más extendida en el software antivirus.

El sistema Euskalert resulta muy beneficioso para obtener nuevas instancias de malware para ser analizadas. De todos modos, el método tradicional de analizar el malware implica que un analista deba realizar ciertos tests y extraer la información significativa para clasificar la muestra y desarrollar una firma específica [6]. Con el incremento percibido del número de código malicioso detectado, más de 37.000 nuevas variantes de malware al día según Panda Security, las compañías antivirus reciben miles de ficheros sospechosos que deben ser analizados y clasificados como software benigno, o al contrario malware. Por esta razón, la automatización de algunas de estas tareas de análisis y clasificación en un tiempo corto es un punto importante a tratar.

II. ESTADO DEL ARTE

A. Honeypots o Máquinas Trampa

Un sistema trampa es un recurso de seguridad informática cuyo valor reside en ser explorado, atacado o puesto en compromiso [7]. Un sistema trampa no tiene ninguna función autorizada ni ningún valor productivo dentro de una red corporativa. Por tanto, un sistema trampa no debería recibir ningún tipo de tráfico. Cualquier intento de conexión con un sistema trampa es, con total seguridad, una exploración, un ataque o un intento de comprometer la máquina o el servicio que está ofreciendo [8]. Cuanto más conozcamos cómo actúan los atacantes, sus métodos y las herramientas que utilizan, mejor podremos protegernos.

Los sistemas trampa pueden clasificarse en función de varios aspectos. Por un lado, según su objetivo se pueden diferenciar entre sistemas trampa con sentido productivo (para prevención y ayuda en la respuesta en redes corporativas) y aquellos dedicados a la investigación (con el fin de recopilar información y analizarla para aprender métodos utilizados por los atacantes). Por otro lado, una de las clasificaciones más extendidas en torno a los sistemas trampa es la que hace referencia a su nivel de interacción. Los sistemas trampa de baja interacción ofrecen una baja y limitada interactividad hacia los atacantes. La mayoría de los desarrollos e implementaciones de sistemas trampa de baja interacción, no son más que simuladores de servicios y de sistemas operativos. Ejemplos de este tipo de sistemas trampa son Honeyd [9], LaBrea [10] o Honeytrap [11]. En los sistemas trampa de alta interacción la estrategia es distinta. No se simula nada, sino que se trabaja con sistemas operativos y aplicaciones reales, generalmente ejecutandose en máquinas virtuales. En este apartado se encuentran Argos [12], Minos [13], y algunos proyectos de la Honeynet Research Alliance [14]. También se podrían encontrar sistemas trampa reconocidos como de