Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información

RECSI XIII

Alicante, 2-5 de septiembre de 2014

Rafael Álvarez · Joan Josep Climent · Francisco Ferrández · Francisco M. Martínez
Leandro Tortosa · José Francisco Vicent · Antonio Zamora
(editores)

Publicaciones de la Universidad de Alicante

Campus de San Vicente, s/n
03690 San Vicente del Raspeig
Publicaciones@ua.es - http://publicaciones.ua.es
Teléfono: 965 903 480

ISBN: 978-84-9717-323-0

Universitat d'Alacant
Universidad de Alicante

RECSI XIII
ALICANTE 2014

Organización XIII RECSI

Comité Científico

- Abascal Fuentes, Policarpo *(Universidad de Oviedo)*
- Álvarez Sánchez, Rafael *(Universidad de Alicante)*
- Amigó García, José María *(Universidad Miguel Hernández de Elche)*
- Areitio Bertolín, Javier *(Universidad de Deusto)*
- Arenaza Nuño, Ignacio *(Mondragón Unibertsitatea)*
- Borrell Viader, Joan *(Universidad Autónoma de Barcelona)*
- Bras Amorós, Maria *(Universidad Rovira i Virgili)*
- Caballero Gil, Pino *(Universidad de La Laguna)*
- Castellà Roca, Jordi *(Universidad Rovira i Virgili)*
- Climent Coloma, Joan Josep *(Universidad de Alicante)*
- Domingo Ferrer, Josep *(Universidad Rovira i Virgili)*
- Durán Díaz, Raúl *(Universidad de Alcalá)*
- Fernández-Medina Patón, Eduardo *(Universidad de Castilla-La Mancha)*
- Ferrer Gomila, Josep Lluís *(Universidad de las Illes Balears)*
- Fúster Sabater, Amparo *(C.S.I.C.)*
- García Bringas, Pablo *(Universidad de Deusto)*
- García Teodoro, Pedro *(Universidad de Granada)*
- 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 *(Universidad Autónoma de Barcelona)*
- Huguet Rotger, Llorenç *(Universidad de las Illes Balears)*
- Jacob Taquet, Eduardo *(Universidad del País Vasco/Euskal Herriko Unibertsitatea)*
- López Muñoz, Javier *(Universidad de Málaga)*
- Martín del Rey, Ángel *(Universidad de Salamanca)*

- Martínez López,Consuelo *(Universidad de Oviedo)*
- Megías Jiménez, David *(Universitat Oberta de Catalunya)*
- Miret Biosca, José María *(Universidad de Lleida)*
- Morillo Bosch, Paz *(Universidad Politécnica de Catalunya)*
- Muñoz Muñoz, Alfonso *(Universidad Politécnica de Madrid)*
- 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)*
- Rifá Coma, Josep *(Universidad Autónoma de Barcelona)*
- Sáez Moreno, Germán *(Universidad Politécnica de Catalunya)*
- Salazar Riaño, José Luis *(Universidad de Zaragoza)*
- Sánchez Ávila, Carmen *(Universidad Politécnica de Madrid)*
- Sebé Feixa, Francesc *(Universidad de Lleida)*
- Soriano Ibáñez, Miguel *(Universidad Politécnica de Catalunya)*
- Tortosa Grau, Leandro *(Universidad de Alicante)*
- Uribeetxeberria Ezpeleta, Roberto *(Mondragón Unibertsitatea)*
- Tena Ayuso, Juan *(Universidad de Valladolid)*
- Vicent Francés, José Francisco *(Universidad de Alicante)*
- Villar Santos, Jorge *(Universidad Politécnica de Catalunya)*
- Zamora Gómez, Antonio *(Universidad de Alicante)*
- Zurutuza, Urko *(Mondragón Unibertsitatea)*

Comité Organizador

- Álvarez Sánchez, Rafael *(Universidad de Alicante, Vicepresidente)*
- Climent Coloma, Joan Josep *(Universidad de Alicante)*
- Ferrández Agulló, Francisco *(Universidad de Alicante)*
- Martínez Pérez, Francisco Miguel *(Universidad de Alicante)*
- Tortosa Grau, Leandro *(Universidad de Alicante)*
- Vicent Francés, José Francisco *(Universidad de Alicante, Vicepresidente)*
- Zamora Gómez, Antonio *(Universidad de Alicante, Presidente)*

Contenidos

Prefacio

Si tuviéramos que elegir un conjunto de palabras clave para definir la sociedad actual, sin duda el término información sería uno de los más representativos. Vivimos en un mundo caracterizado por un continuo flujo de información en el que las Tecnologías de la Información y Comunicación (TIC) y las Redes Sociales desempeñan un papel relevante. En la Sociedad de la Información se generan gran variedad de datos en formato digital, siendo la protección de los mismos frente a accesos y usos no autorizados el objetivo principal de lo que conocemos como Seguridad de la Información.

Si bien la Criptología es una herramienta tecnológica básica, dedicada al desarrollo y análisis de sistemas y protocolos que garanticen la seguridad de los datos, el espectro de tecnologías que intervienen en la protección de la información es amplio y abarca diferentes disciplinas. Una de las características de esta ciencia es su rápida y constante evolución, motivada en parte por los continuos avances que se producen en el terreno de la computación, especialmente en las últimas décadas. Sistemas, protocolos y herramientas en general considerados seguros en la actualidad dejarán de serlo en un futuro más o menos cercano, lo que hace imprescindible el desarrollo de nuevas herramientas que garanticen, de forma eficiente, los necesarios niveles de seguridad.

La Reunión Española sobre Criptología y Seguridad de la Información (RECSI) es el congreso científico español de referencia en el ámbito de la Criptología y la Seguridad en las TIC, en el que se dan cita periódicamente los principales investigadores españoles y de otras nacionalidades en esta disciplina, con el fin de compartir los resultados más recientes de su investigación. Del 2 al 5 de septiembre de 2014 se celebrará la decimotercera edición en la ciudad de Alicante, organizada por el grupo de Criptología y Seguridad Computacional de la Universidad de Alicante. Las anteriores 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), Salamanca (2008), Tarragona (2010) y San Sebastián (2012).

Hacia un Proceso de Migración de la Seguridad de Sistemas heredados al Cloud

Luis Márquez Alcañiz
Comision Nacional
de la Competencia
Madrid
luismarquezalcaniz@gmail.com

David G. Rosado
Departamento de TSI
Grupo GSyA
Universidad Castilla-La Mancha
Ciudad Real
david.grosado@uclm.es

Daniel Mellado
Agencia Tributaria
Madrid
damefe@esdebian.org

Eduardo Fernández-Medina
Departamento de TSI
Grupo GSyA
Universidad Castilla-La Mancha
Ciudad Real
eduardo.fdezmedina@uclm.es

***Resumen*—El desarrollo de la computación en la nube es una tendencia fuerte en la industria de las TI que hace que los clientes de este nuevo modelo de prestación de servicios, sobre todo las empresas, se enfrenten a desafíos nuevos en lo que se refiere a la gestión de la seguridad de sus aplicaciones heredadas en el nuevo entorno. La cuestión es en cómo migrar de forma segura los sistemas de información heredados de estas empresas. Este artículo presenta un proceso (SMiLe2Cloud) y un marco de trabajo con el que se puede migrar de forma segura los sistemas corporativos heredados a infraestructuras o entornos en la nube, siguiendo los 14 dominios de seguridad del CSA y utilizando ingeniería inversa.**

***Palabras clave*—Cloud, seguridad informática, migración de sistemas heredados, KDM, SLA, SecSLA.**

I. Introducción

Para algunos expertos, la computación en la nube está "desalineada con los modelos y controles de seguridad tradicionales" [1]. Sin embargo, otros ven en este modelo una gran oportunidad para mejorar la seguridad de los sistemas heredados [2]. Sin embargo, hay algo en lo que todos coinciden: la nube supone nuevas amenazas y estas amenazas deben ser resueltas antes de que las aplicaciones de las grandes corporaciones entren en juego.

¿Qué tienen en especial esas aplicaciones de las grandes corporaciones? Que la mayoría de ellas se basan en sistemas de información heredados (LIS-Legacy Information Systems). Según una encuesta realizada por MeriTalk [3] a un total de 166 directivos de TI del gobierno federal norteamericano, el 47 % de las aplicaciones de TI se basan en tecnología heredada que necesita modernización?. Y gran parte de la modernización no sólo se beneficiaría de una mejora tecnológica pura, sino que entrarían en juego reducciones de coste importantes a raíz de una migración a la nube de parte de la infraestructura que las soporta [4].

Y sin embargo, aunque la modernización de los LIS por medio de la migración a la nube podría implicar inmensos ahorros y reducciones de los presupuestos, y a pesar de la preocupación a la que antes nos hemos referido relativa a la seguridad intrínseca del modelo en la nube, hasta la fecha parece que todavía no hay un modelo que permita la migración a la nube de sistemas que de forma explícita incluyan procesos relacionados con la seguridad de dichos sistemas. Sí que es cierto que existen propuestas de procesos de migración [5][6][7][8], pero ninguno de ellos propone una verdadera integración con las cuestiones específicas de seguridad en forma de necesidades y/o de oportunidades que se derivan del modelo en la nube.

Nuestro propósito con este artículo es proponer un marco de trabajo para tal proceso mediante un conjunto de métodos que resuelvan de forma concreta las cuestiones de seguridad y la integración de la seguridad con procesos de otra naturaleza orientados todos ellos a la migración segura a la nube de sistemas de información heredados. En [9] se realizó un estudio de la importancia de la seguridad en los entornos Cloud y se analizó algunas propuestas de migración al Cloud, que fue descrito formalmente planteando un "mapping study" en [11], donde se indica la falta de iniciativas con respecto a la seguridad en el propio proceso de migración. En [10] se da algunas pautas y criterios a la hora de tomar algunas decisiones en cuanto a qué características debemos migrar al Cloud y cuáles no. Este artículo, que se presenta aquí, avanza en el sentido de que una vez descubierta la necesidad de disponer de un proceso de migración donde se incorpore la seguridad desde el principio, se define dicho proceso de migración con el propósito de servir de soporte y ayuda para migrar las características de seguridad de sistemas heredados al Cloud Computing.

El artículo está estructurado en 2 secciones adicionales a esta introducción. En la sección 2 presentamos el marco de trabajo propiamente dicho. Y en la sección 3 ofrecemos unas someras conclusiones y presentamos lo que serán las líneas de actuación futuras.

II. SMILE2CLOUD: Proceso para la Migración a la nube de la Seguridad de los Sistemas Heredados

En esta sección proponemos un proceso (denominado SMiLe2Cloud - Security MIgration of LEgacy systems TO Cloud computing) que pretende resolver el problema de la migración con seguridad a la nube de sistemas de información heredados. Este proceso está basado en el modelo de herradura del SEI (Software Engineering Institute) [12], pero también tiene una vocación de proceso de mejora continua al estilo de Deming.

Dado que estamos interesados en los aspectos propiamente relacionados con la seguridad (y no en los esfuerzos generales de ingeniería inversa necesarios para obtener la especificación funcional) hemos partido de la base de que los ingenieros a cargo de la migración ya han desarrollado un modelo del sistema heredado que define las especificaciones funcionales y los elementos arquitectónicos de sistema (con exclusión de las especificaciones relacionadas con la seguridad y la arquitectura de seguridad) y que han documentado dichas especificaciones y elementos en un entorno que puede exportar dicha especificación en formato KDM (Knowledge Discovery Metamodel) [13]. Es en este punto en el que nosotros entramos y empezamos a desarrollar los aspectos de seguridad a partir del diseño obtenido mediante ingeniería inversa y luego continuamos con el resto del proceso de segurización del sistema migrado.

II-A. Visión general

Como se ha indicado antes, nuestro proceso comienza en el punto más alto del modelo de herradura del SEI, una vez que la arquitectura básica ha sido obtenida, y justo antes de que comience la transformación. Desde este punto, continuará transformando y refinando el sistema objetivo, ya desde una perspectiva puramente enfocada en los temas relacionados específicamente con la nube.

El proceso SMiLe2Cloud consta de siete actividades dirigidas por 14 dominios de seguridad del CSA (Cloud Security Alliance) [14] que son mostradas en Figura 1. La actividad de *"extracción"* está enfocada al uso de la reingeniería inversa para extraer aspectos de seguridad desde el LIS a un modelo de seguridad (modelo SMiLe) definido para nuestro proceso de migración. La segunda actividad es la *"valoración"* durante la cual se estudian las principales características del cloud, los principales proveedores y diferentes modelos cloud. La tercera actividad es el *"análisis"* de los requisitos de seguridad, las cláusulas en los acuerdos a nivel de servicio de seguridad y los servicios ofrecidos por los proveedores de seguridad del cloud. La actividad de *"diseño"* está enfocada en el diseño de la arquitectura de seguridad y en la definición de una estrategia de migración que será aplicada en la siguiente actividad del proceso de migración, que es la actividad de *"migración"* donde los elementos de seguridad son desarrollados, configurados y contratados siguiente la estrategia previamente definida. La sexta actividad es la *"evaluación"* donde se verifica y valida el modelo de seguridad migrado. Finalmente, la actividad de *"mejora"* captura los nuevos aspectos de seguridad que se quieren incorporar dentro de un nuevo ciclo del proceso y se analizan las mejoras y cambios propuestos para nuestro sistema cloud.

Dado que KDM carece de elementos específicos para modelar aspectos de seguridad de un sistema heredado, en realidad parte de nuestro proceso debe realizarse antes de que exista una especificación completa del sistema obtenida por ingeniería inversa. La actividad de extracción, específicamente definida en nuestro proceso, precisamente trata con esta última parte de la fase de reingeniería del modelo de herradura. Sin embargo, esta fase no es específica de un proceso de migración a la nube. Podría ser utilizada de forma separada en cualquier proceso que pretendiera migrar un sistema heredado de forma segura a cualquier tipo de arquitectura objetivo.

Lo que sí es necesario entender de antemano, cuando estamos pensando en migrar a la nube, es el papel central que tienen para la seguridad y para la arquitectura del sistema completo los acuerdos de nivel de servicio (SLA - Service Level Agreement) específicos de seguridad (comúnmente denominados SecSLA). Los SecSLA son el núcleo de la seguridad en la nube y la mayoría de controles específicos que se pueden implantar se instancian como cláusulas en el SecSLA siempre que es posible. Por supuesto, esto depende en gran media del modelo de despliegue elegido; con un modelo de infraestructura como servicio (IaaS - Infrastructure as a Service) como el que ofrece Amazon EC2, la organización que está migrando el sistema heredado tiene que trabajar a un nivel más bajo y diseñar e implementar controles tradicionales por sí misma; sin embargo, con modelos de software como servicio puros (SaaS - Software as a Service), casi todos los controles de seguridad deben ser implementados como SecSLA ya sean acordados con el proveedor funcional del servicio o con un proveedor específico de seguridad como servicio (SecaaS - Security as a Service); finalmente con un modelo de plataforma como servicio (PaaS - Platform as a Service) como el que ofrece Google App Engine una solución intermedia que balancee controles de ambos tipos será la aproximación adecuada (la seguridad de la plataforma recae en el proveedor y la seguridad de las aplicaciones y la seguridad del propio proceso de desarrollo y despliegue es responsabilidad del cliente).

Todo esto es importante para la definición de la arquitectura de seguridad, puesto que algunas actividades en un proceso tradicional de aseguramiento de sistemas (ya sea en migración de sistemas o en desarrollo de sistemas desde cero) implican el diseño de controles, mientras que en un proceso orientado a la nube, la mayoría del proceso tiene que ver con el aspecto nuclear de seleccionar qué controles diseñados por los proveedores son aplicables y asegurar que las cláusulas del SLA cubren dichos controles. De esa manera, las cláusulas se convierten, de facto, en los propios controles que salvaguardan a la organización cliente (normalmente mediante la aplicación de obligaciones contractuales o penalizaciones en caso de que el proveedor no pueda cumplir dichas obligaciones). El problema, pues, se convierte en una mezcla de diseño de sistemas, selección de proveedores de servicio y técnicas de negociación de contratos.

En nuestro caso, el objetivo es orientar nuestra aproximación lo más posible hacia la ingeniería de sistemas de información. Por ello excluiremos inicialmente las soluciones puramente SaaS que tienden a estar orientadas principalmente hacia la reingeniería de procesos que a la de sistemas. Esto es, una propuesta SaaS supone normalmente un diseño de cómo el proceso de negocio debe ser migrado (es decir cómo podemos seleccionar el mejor proveedor SaaS que pueda cumplir con el proceso de negocio y/o en qué manera debe cambiar dicho

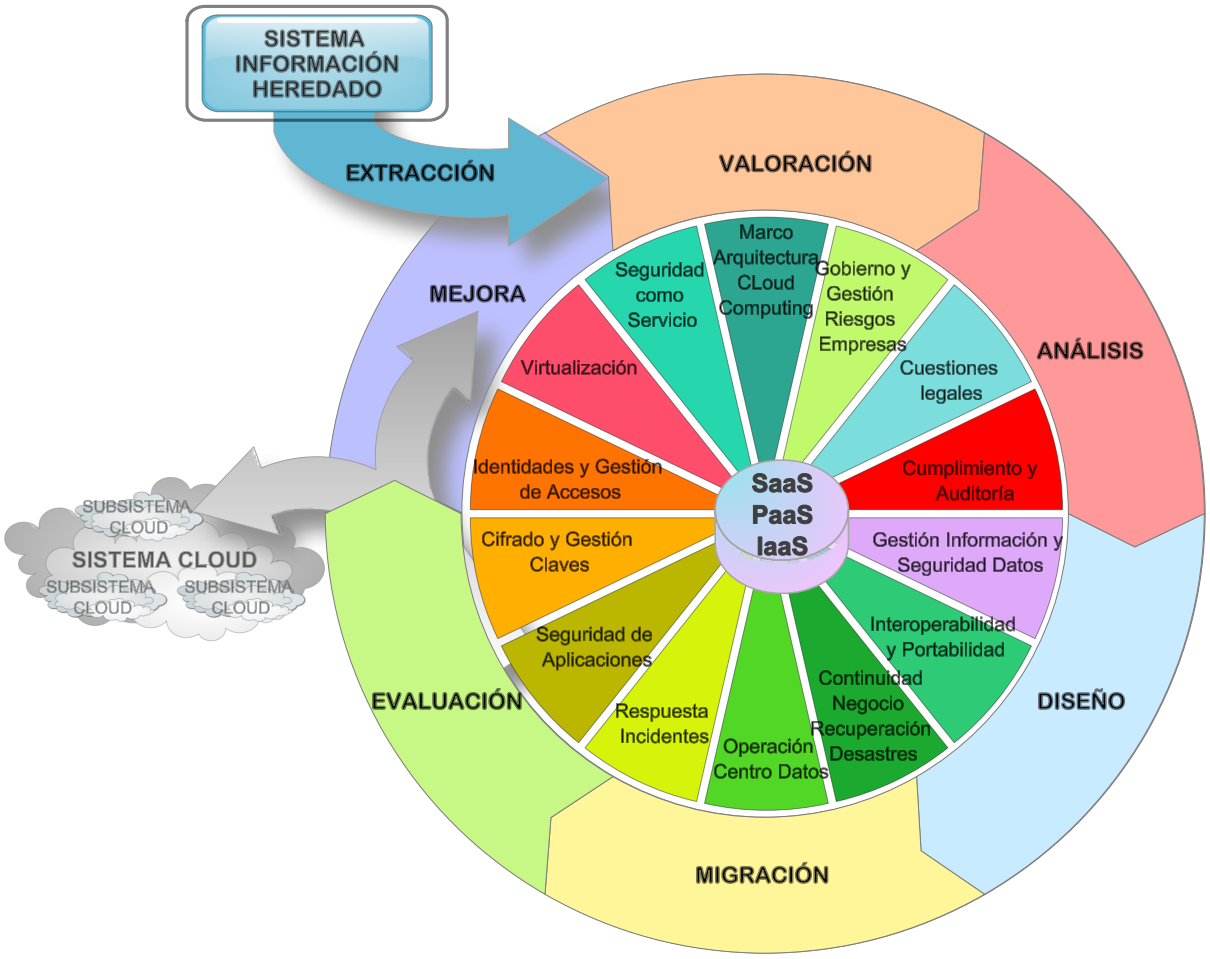

Figura 1. El proceso SMiLe2Cloud: un proceso para migrar a la nube la seguridad de sistemas de información heredados.

proceso de negocio para acomodarse al nuevo sistema) pero tiene poco que ver con cuestiones relacionadas con la ingeniería de sistemas. En cierto sentido, una solución puramente SaaS no sería una migración pura de un sistema heredado, sino que sería un cambio completo del sistema que trataría con cuestiones como la migración de los datos del sistema heredado original más que la migración de funcionalidades.

II-B. Actividades de SMiLe2Cloud

En esta sección presentaremos una descripción en profundidad del conjunto de actividades en nuestro proceso SMiLe2Cloud las cuales son mostradas en Figura 1. El proceso tiene 7 actividades: Extracción, Valoración, Análisis, Diseño, Migración, Evaluación y Mejora, y un amplio conjunto de artefactos de entrada y salida para cada una de las actividades y que son descritas de forma resumida a continuación.

II-B1. Actividad 1: Extracción: La extracción es la actividad en la que el modelo de seguridad del sistema heredado es obtenido a partir del propio código del sistema y de la documentación del mismo. Se trata de un subproceso de ingeniería inversa que se puede realizar en paralelo al subproceso de obtención del modelo de arquitectura general del sistema heredado. Normalmente ambos procesos se supone que son realizados con la ayuda parcial de herramientas de ingeniería inversa que faciliten las tareas y pasos que el analista debe realizar para identificar los diferentes requisitos y controles de seguridad existentes en el sistema origen.

Se trata de una actividad orientada por los datos y parte de la especificación formal de los programas y subprogramas del sistema heredado, así como de los datos gestionados por cada unidad de programa. Esta especificación formal tiene la forma de árbol de sintaxis abstracta (AST - Abstract Syntax Tree) que modeliza cada unidad de programa y los datos manejados.

- A1.1 Definir el árbol de sintaxis abstracta (AST-abstract syntax tree)

Un árbol de sintaxis abstracta es una representación en forma de árbol de la estructura del programa y de los elementos de datos del sistema heredado y ofrece una equivalencia 1-a-1 entre todos los elementos incluidos en el código en forma de estructura arbórea. El AST es usado para derivar los requisitos de seguridad del sistema.

- A1.2 Extraer aspectos de seguridad del AST

Para cada elemento de datos y de subprograma que ha sido representado en el AST, el analista de sistemas debe extraer los parámetros de seguridad concretos para cada uno de los perfiles de usuarios definidos en su operación habitual normal (acceso, creación, modificación, borrado, administración, auditoría).

- A1.3 Definir el modelo de seguridad en KDM (Knowledge Discovery Metamodel)

Nuestra aproximación propone evitar esta situación haciendo que cada artefacto y control de seguridad del sistema heredado sea instanciado en una regla de seguridad de negocio y se incluye en el modelo conceptual durante la fase de análisis.

- A1.4 Definir el modelo de seguridad (modelo SMiLe)

El modelo SMiLe (Security MIgration of LEgacy systems) es un modelo de seguridad de un sistema heredado que ha sido derivado desde las reglas de negocio de seguridad definidos mediante KDM y los activos identificados en el paso A1.3. Ahora es necesario incluir las políticas y controles de seguridad que fueron predefinidos para el sistema heredado (con independencia de si el sistema debe ser migrado a la nube o no).

II-B2. Actividad 2: Valoración: La actividad de valoración es en la que el modelo general de seguridad del sistema heredado es adaptado al nuevo entorno (en nuestro caso, a la nube). Comenzamos con un modelo SMiLe que no está específicamente adaptado al entorno de la nube y en dicho modelo estudiamos las fortalezas, debilidades, oportunidades y amenazas específicas que la nube incorpora. Esta actividad comienza con el modelo SMiLe (esto es, el modelo de seguridad del sistema heredado obtenido por ingeniería inversa) y es realmente la primera actividad de ingeniería directa del modelo de herradura que define nuestro proceso.

Los objetivos de esta actividad son los siguientes: refinar el modelo SMiLe para obtener un modelo SMiLe2Cloud (esto es, adaptar el modelo del sistema heredado con las amenazas específicas de la nube, los activos específicos en la nube, los escenarios específicos de la nube, los requisitos específicos de la nube, etc.); seleccionar un conjunto de proveedores de servicios en la nube y de proveedores de seguridad en la nube que, al menos parcialmente, cumplan con los requisitos de seguridad del modelo SMiLe2Cloud del sistema heredado según nuestra especificación de seguridad; y validar los modelos de servicio y de despliegue que pueden utilizarse dentro de los límites de dichas especificaciones de requisitos de seguridad.

- A2.1 Definir la matriz DAFO (Debilidades, Amenazas, Fortalezas y Oportunidades) e incorporar los elementos específicos de la nube en el modelo SMiLe

Se define una matriz (DAFO) con las debilidades, fortalezas, oportunidades y nuevas amenazas que el modelo cloud plantea al LIS.

- A2.2 Validar proveedores en la nube

Una vez que la matriz DAFO se ha completado, el analista debe contrastarlo con el modelo SMiLe del LIS y comprobar la lista de proveedores de servicios cloud que puede abordar las especificaciones funcionales del LIS y extraer las especificaciones de seguridad que ofrecen dentro de los términos del acuerdo de nivel de servicio. El analista también debe comprobar cuáles términos relacionados con la seguridad del acuerdo a nivel de servicio están abiertos a negociación.

- A2.3 Validar modelos en la nube

Dado que las diferentes propuestas de modelos cloud (modelos de servicios y modelos de despliegue) forman parte de la arquitectura del modelo cloud y no del modelo de seguridad, no se debe tratar de cambiar los modelos seleccionados o propuestos definidos en la arquitectura LIS. Sin embargo, los modelos conducen a una diferencia en las restricciones de seguridad que el sistema migrado deberá enfrentar. Por tanto, es necesario validar si los modelos seleccionados o propuestos, de los proveedores seleccionados en el paso anterior, pueden o no cumplir con los requisitos de seguridad del LIS. Si no, el riesgo que no está cubierto por el requisito de seguridad no cumplido debe ser aceptado o un cambio en la arquitectura destino debe ser recomendada, proporcionando una lista de modelos aceptables que cumplen con los requisitos de seguridad.

II-B3. Actividad 3: Análisis: La actividad de análisis es en la que definimos los requisitos de seguridad a implementar e identificamos el conjunto de servicios de seguridad contratables a proveedores específicos de seguridad como servicio (SecaaS) que se integrarán en nuestra aplicación una vez migrada a la nube. También se identificarán otros controles tales como las cláusulas estándar del SLA que afectan a cuestiones de seguridad y también puede que volvamos a validar si los proveedores de servicio en caso de que algún proveedor concreto no pueda cumplir dentro de su marco contractual con los requisitos fundamentales de seguridad definidos.

- A3.1 Análisis de requisitos de seguridad en la nube

El modelo SMiLe2Cloud actualizado, proveedores cloud validados, modelos de servicio y despliegue son usados para derivar un conjunto de requisitos de seguridad con la cual el sistema diseñado debe cumplir con el nuevo entorno. Los requisitos serán un subconjunto de requisitos del LIS que el LIS ten?a y con los requisitos que se incluyeron en el desempe?o del análisis DAFO.

- A3.2 Asociación de los requisitos de seguridad con los elementos de SMiLe

Los artefactos obtenidos a partir de la tarea anterior deben ser utilizados para desarrollar un mapeo entre los requisitos de seguridad del LIS y una especificación formal de los requisitos de seguridad con la que el sistema destino debe cumplir para estar seguro de acuerdo con la especificación de la nueva arquitectura.

- A3.3 Análisis de los acuerdos estándar de nivel de servicio

Una vez que los requisitos de seguridad se han identificado y definido formalmente, es necesario seguir analizando el SLA estándar definido por los proveedores de la nube en busca de

problemas de seguridad, políticas de seguridad, elementos de seguridad que pueden ser medidos, etc.

- A3.4 Análisis de servicios de seguridad

La última tarea de esta actividad se ocupa de los servicios de seguridad actuales que son ofrecidos por los proveedores de servicios de seguridad. Una vez más, esto puede implicar el análisis de SLA de estos proveedores y mapear algunas cláusulas del SLA en requisitos de las actividades anteriores.

II-B4. Actividad 4: Diseño: En la actividad de diseño se definen los componentes propiamente dichos que forman el núcleo de la arquitectura de seguridad del sistema (cláusulas, controles personalizados, protocolos, etc.), y no sólo se define el diseño, sino que también se define la forma en la que deben ser validados y se planifican las actividades que serán necesarias en la migración real de la seguridad del sistema heredado.

- A4.1 Diseñar la arquitectura de seguridad básica para la nube

En esta tarea, se toma la especificación de los requisitos de seguridad y las cláusulas del SLA identificados en los pasos anteriores, junto con la lista de los anteriores servicios de seguridad cloud y se desarrolla la arquitectura de seguridad básica en términos de controles que se pueden ser integrados para cumplir con los requisitos de seguridad.

- A4.2 Diseñar los acuerdos personalizados de nivel de servicio

Siempre que sea posible, SLA (ya sea SLA general o SecSLA) debe ser personalizado para satisfacer las necesidades específicas del cliente. La mayoría de los analistas cloud aconsejan que los contratos de servicio se adapten a las necesidades del cliente. En la práctica, esto sólo será un motivo de preocupación para los grandes clientes que pueden negociar contratos lucrativos. Por otra parte, es evidente que no todos los proveedores de servicios permitirán la personalización de los servicios y/o cláusulas hasta el grado deseado.

- A4.3 Validar la arquitectura de seguridad específica de la nube

Una vez que la arquitectura de seguridad ha sido obtenida, y antes que la migración actual comience, tiene lugar la validación de la arquitectura. Esta validación involucra una revisión formal del diseño que hemos propuesto (ya sea SLA o controles personalizados). Después de esta validación, la aplicabilidad y viabilidad técnica de la arquitectura debería ser aclarada; es decir, todos los controles que se implementen a través de SLA deberían ser elegibles o dentro del ámbito SLA de los proveedores seleccionados y la responsabilidad de entregar el control siempre debe estar clara (es decir, cuando usamos dos proveedores de servicios, debemos asegurarnos que no hay ninguna posibilidad de que los contratos deleguen mutuamente la responsabilidad del control de seguridad). Como alternativa, los controles deben poder aplicarse como controles personalizados en el modelo seleccionado (es decir, en PaaS, el acceso está disponible para definir usuarios y otorgar permisos en una base de datos).

- A4.4 Planificar la estrategia de migración

Finalmente, la última tarea de la actividad de diseño es desarrollar un plan relativo a cómo la seguridad del LIS será implementada con recursos, horarios, logros, etc.

II-C. Actividad 5: Migración

Finalmente, la propia migración tiene lugar y es necesario contratar en la realidad los servicios y firmar los acuerdos de nivel de servicio y desarrollar los elementos de seguridad personalizados e implantarlos y configurarlos para dejar todos los controles de seguridad en condiciones de operación habitual.

- A5.1 Contratar servicios de seguridad

En este punto tiene lugar la formalización del contrato. Este contrato puede ser un acuerdo de nivel de servicio con un proveedor de servicios de seguridad en la nube o pueden ser las cláusulas específicas de seguridad que se definen en los contratos con proveedores de servicios IaaS, PaaS o Saas.

- A5.2 Desarrollar controles de seguridad a medida

Si nuestra arquitectura define controles de seguridad personalizados, ha llegado el momento de desarrollarlos. Por ejemplo, si hemos definido que nuestro sistema tendrá una pieza de software que controlará los perfiles de usuario en una base de datos ofrecida por un proveedor de PaaS que no incorpora un sistema de roles internamente en la propia base de datos, será necesario desarrollar la pieza de software que realice la gestión del roles e integrarla en nuestras aplicaciones y programas que desarrollan elementos funcionales; también será necesario en este punto hacer las pruebas unitarias de software de los controles de seguridad a medida.

- A5.3 Configurar controles de seguridad

Para los controles de seguridad personalizados definidos, contratados y/o implantados de forma personalizada en los pasos anteriores, normalmente es necesario realizar una función de despliegue en el sistema final. Además, si los controles necesitan algún tipo de configuración, en este punto deberán ser configurados y afinado su funcionamiento.

II-D. Actividad 6: Evaluación

Una vez que todo el proceso ha concluido y el sistema heredado ha sido movido a la nube de forma segura, es el momento de verificar y validar el sistema y los controles de seguridad.

- A6.1 Verificar seguridad del sistema cloud

En actividades anteriores (durante el análisis y el diseño) algunos de los artefactos de salida eran entradas en la parte del proceso y del modelo de seguridad que trata con las cuestiones de pruebas, verificación y certificación de la seguridad.

- A6.2 Validar seguridad del sistema cloud

Técnicamente, la validación es la actividad formal que hace que un sistema sea válido para el responsable de las cuestiones de seguridad de las tecnologías de la información: el administrador de la seguridad. La tarea consiste en revisar las evidencias obtenidas en la actividad anterior y en producir un documento que establece que la gestión de la seguridad está de acuerdo con la seguridad de los sistemas heredados (LIS) migrados a la nube de acuerdo con los requisitos especificados.

II-E. Actividad 7: Mejora

Dado que nuestro proceso tiene vocación de mejora continua (se trata de un ciclo de Deming) no finaliza con la validación real del sistema en funcionamiento. Periódicamente, el responsable de la seguridad del sistema heredado deberá reunir nuevas evidencias que permitan asegurar que el sistema está permanentemente configurado según los requisitos y parámetros de seguridad definidos y que permita renovar la validación. También estudiará mejoras que afecte al análisis DAFO, al análisis de seguridad en la nube o incluso a la lista de servicios en la nube que pueden ser considerados en las anteriores tareas.

- A7.1 Estudiar mejoras

La nube es un entorno cambiante. Algunos de los problemas que ahora están siendo objeto de estudio por parte de la mayor parte de los expertos, hace un par de años ni siquiera se conocían. En un par de años, puede que haya servicios completamente nuevos que ayuden a fortalecer la seguridad de un sistema heredado migrado a la nube. Además, dado que al mover un sistema a la nube, delegamos la responsabilidad sobre la aplicación de algunos controles, es necesaria y aconsejable que se vigilen los niveles y métricas definidos para asegurar su cumplimiento.

- A7.2 Renegociar cuestiones de seguridad

Finalmente, hemos definido una actividad que permita renegociar con los proveedores de servicios y proveedores de seguridad las incidencias de seguridad. Esta negociación es diferente de la que supone la renegociación de nuevos servicios.

III. Conclusión

En este artículo hemos presentado un proceso que permite la migración de la seguridad o la migración segura a la nube de un sistema de información heredado. Comenzamos en el punto en el que el sistema ha sido objeto de un proceso de ingeniería inversa y tenemos disponibles una serie de modelos KDM que definen la parte funcional del sistema heredado. Desde este punto, ofrecemos una serie de actividades que permitirán evolucionar estas especificaciones en formato KDM en una arquitectura de seguridad para el sistema heredado y desde allí en un sistema objetivo migrado a la nube en forma segura; actualmente estamos desarrollando técnicas y plantillas para automatizar parcialmente el proceso de entrega de una arquitectura segura y para mapear la arquitectura de seguridad deseada en un modelo que de forma específica trate las cuestiones específicas de la nube como las amenazas específicas que la nube presenta, los requisitos de seguridad específicos para la nube, los controles específicos relacionados con la nube (ya sean en su forma de seguridad como servicio o como controles personalizados); todo ello con la intención de que una aplicación heredad que sea migrada a la nube cumpla estándares de seguridad en la nube tales como la matriz de controles de la CSA. Nuestro trabajo futuro se enfocará en un refinamiento del propio proceso y en el desarrollo de herramientas y patrones que permitan de forma semiautomática asistir al analista de seguridad en las actividades de obtención del modelo de seguridad del sistema heredado y la derivación del modelo de seguridad del sistema migrado a la nube a partir de aquél. La aplicación real de migración de un sistema heredado al cloud se definirá y ejecutará siguiendo SMiLe2Cloud.

Agradecimientos

Esta investigación es parte de los siguientes proyectos: GEODAS (TIN2012-37493-C03-01) y SIGMA-CC (TIN2012-36904) financiados por el "Ministerio de Economía y Competitividad y Fondo Europeo de Desarrollo Regional FEDER", España.

Referencias

[1] W. Jansen, T. Grance, "Guidelines on Security and Privacy in Cloud Computing".*NIST SP - 800-144*, 2011.

[2] J.R.V. Winkler, in "Securing the Cloud. Cloud Computing Security. Techniques and Tactics", B. Meine, Editor. Syngress, Elsevier. p. 25. 2011.

[3] M. Tobin, and B. Bass. "Federal Application Modernization Road Trip: Express Lane or Detour Ahead?". MeriTalk. 2011.

[4] V. Kundra, "Federal Cloud Computing Strategy", U.S.C.I. Office, Editor. 2011.

[5] W. Zhang, A. J.Berre, D. Roman, and H. Aage Huru. "Migrating Legacy Applications to the Service Cloud", in OOPSLA 2009, Towards Best Practices in Cloud Computing. 2009.

[6] S. Frey and W. Hasselbrind. "Model-Based Migration of Legacy Software Systems into the Cloud: The CloudMIG Approach", in 12 Workshop on Software-Reengineering of the GI-SRE. 2010.

[7] H. Zhou, H. Yang, and A. Hugill. "An Ontology-Based Approach to Reengineering Enterprise Software for Cloud Computing", in IEEE 34th Annual Computer Software and Applications Conference. 2010. Seoul, Korea. p. 383-388.

[8] Q.H. Vu and R. Asal, "Legacy Application Migration to the Cloud: Practicability and Methodology", in IEEE Eighth World Congress on Services. 2012.

[9] D.G. Rosado, R. Gómez, D. Mellado, and E. Fernández-Medina, "Security Analysis in the Migration to Cloud Environments". Future Internet, 2012. 4(2): p. 469-487.

[10] R. Gomez, D.G. Rosado, D. Mellado, and E. Fernández-Medina, "Security Criteria in Deciding on Migration of Systems to the Cloud", in 9th International Workshop on Security in Information Systems. 2012: Wroclaw, Poland. p. 93-100.

[11] L. Marquez Alcañiz, D.G. Rosado, D. Mellado, and E. Fernández-Medina, "Security in legacy migration to the cloud: a systematic mapping study", in 11th International Workshop on Security in Information Systems. 2014: Lisbon, Portugal. p. 26-37.

[12] R. Seacord, D. Plakosh, and G. Lewis, "Modernizing Legacy Systems: Software Technologies, Engineering Processes, and Business Practices". 1st ed. 2003: Addison Wesley.

[13] KDM, "Knowledge Discovery Meta-Model", Version 1.3. OMG specification formal 2010-12-12. 2011.

[14] CSA, "Security Guidance for Critical Areas of Focus in Cloud Computing V3.0". 2011.