Comparando Patrones de Seguridad y Tácticas de Seguridad para construir sistemas seguros: Identificando amenazas de seguridad

René Noël[1], Gilberto Pedraza-García[2], Hernán Astudillo[3], Santiago Matalonga[4] , Oscar Encina[3]

[1] Escuela de Ingeniería Civil Informática,
Universidad de Valparaíso, Valparaíso, Chile
rene.noel@uv.cl

[2] Universidad de los Andes,
Bogotá, Colombia
g.pedraza56@uniandes.edu.co

[3] Departamento de Informática,
Universidad Técnica Federico Santa María, Valparaíso, Chile
hernan@inf.utfsm.cl, oscar.encina@usm.cl

[4] Universidad ORT Uruguay
smatalonga@uni.ort.edu.uy

Resumen. Los Patrones de seguridad y la Tácticas de la arquitectura para seguridad son dos enfoques de reuso de conocimiento en la toma de decisiones para la construcción de sistemas seguros. Ambos enfoques presentan una serie de decisiones de diseño, de distinto nivel de profundidad y detalle en su definición. En trabajos anteriores se realizó una evaluación exploratoria, donde los sujetos tenían que identificar y mitigar las amenazas de seguridad. En este trabajo se presenta una evolución del diseño experimental original con el fin de evaluar si la identificación de amenazas y mitigación podrían enfocarse como dos actividades diferentes. El protocolo experimental también se ha mejorado mediante la separación y estructuración de una guía paso a paso para la actividad de identificación. Se realizó un nuevo acercamiento experimental con 13 sujetos. Los resultados muestran una mejora significativa en el número de amenazas identificadas para el mismo problema por sujetos sin experiencia previa en el diseño de sistemas seguros.

1 Introducción

Los Patrones de Seguridad [8] y las Tácticas de Arquitectura para Seguridad [3] son dos enfoques para el diseño y el desarrollo de sistemas seguros. Ambos enfoques se basan en el reuso de conocimiento, específicamente, decisiones de diseño. En nuestro trabajo previo [14], comparamos ambos enfoques mediante una actividad experimental, con el objetivo de explorar el impacto de cada uno sobre la calidad y

productividad en el diseño de un mismo sistema, analizando además el impacto de la experiencia de los sujetos. La naturaleza práctica del enfoque experimental permitió identificar tópicos no abordados en forma precisa en la literatura. Algunos de los temas de interés identificados a partir de esta experiencia son los siguientes:

- Las Tácticas de Arquitectura hacen referencia a conceptos que requieren un conocimiento previo del dominio.
- La lista de Tácticas de Arquitectura propuesta por Bass [3] carece de especificidad y homogeneidad: algunas tácticas son de un nivel cercano a un principio de diseño, mientras otras son más específicas. Mientras unas abordan el "qué", otras especifican el "cómo".
- La lista de tácticas parece incompleta, omitiéndose algunos tipos de decisiones importantes, como "ocultamiento de información"

Por otro lado, el ejercicio de llevar ambos enfoques a la resolución de un problema concreto durante la experiencia, llevó al equipo de investigación a cuestionar aspectos propios de la actividad de toma de decisiones de diseño para la seguridad:

- ¿Cuáles son los insumos para la aplicación de Tácticas y Patrones de Seguridad?¿Son los mismos para ambas técnicas?
- ¿Cómo se expresan las decisiones de diseño para el aseguramiento de la calidad? ¿Pueden ser documentadas?
- ¿Es posible separar la toma de decisiones para asegurar el sistema de la actividad de identificar las posibles amenazas de seguridad?
- ¿Es necesaria la formalización y entrenamiento de la actividad de identificación de amenazas?

Para abordar estas preguntas y para avanzar a hacia la aplicación práctica de ambas técnicas, se ha diseñado un enfoque de investigación que combina propuestas para la sistematización de la aplicación de los métodos con la generación de un marco teórico uniforme desde la experiencia de practicantes y expertos, tomando un enfoque empírico para validar cada una de estas propuestas.

Este trabajo presenta una evolución del diseño experimental original, en el que se ha incorporado una propuesta de sistematización de la actividad de identificación de amenazas, separándola de las actividades de mitigación con patrones o tácticas de seguridad. La sección 2 presenta el trabajo relacionado revisado para la sistematización de la identificación de tácticas. La sección 3 entrega el enfoque de investigación general mencionado anteriormente, mientras que la sección 4 describe en detalle el planteamiento, operación y análisis de resultados de la replicación.

2 Enfoque de investigación y motivación

En el primer acercamiento experimental a la comparación de Patrones y Tácticas de seguridad [14], se identificó la necesidad de definir cómo usar las técnicas en la práctica, cuáles eran los insumos para poder aplicarlas, cómo expresar los resultados de su aplicación, y cómo cuantificar estos resultados. Si bien se encontraron algunas propuestas en la literatura, no todas ellas eran completas ni consistentes entre sí. Más aún, las técnicas tenían distintos niveles de madurez y profundidad en su definición. Esto llevó a realizar un experiencia experimental exploratoria en el que se

establecieron algunos supuestos, con el fin de iluminar los espacios oscuros en la teoría. Además de los resultados cuantitativos, se identificaron tres necesidades de elaboración teórica:

- La estructuración de un método de identificación de amenazas a ser mitigadas con Patrones de Seguridad.
- La propuesta de un método de identificación de amenazas para su mitigación usando Tácticas de Seguridad. Se considera esta preocupación como una distinta a la anterior, por operar ambas técnicas en niveles distintos de abstracción.
- La comparación de Patrones y Tácticas desde la identificación a la mitigación, con los métodos anteriores.
- El contraste teórico de los métodos propuestos, obtenidos fundamentalmente de la literatura, y los conceptos asociados, con la visión de expertos y practicantes de diseño de sistemas seguros.

Para abordar estas necesidades, definimos tres objetivos de investigación:

- Proponer métodos de mitigación de amenazas de seguridad, en los que cada actividad sea experimentalmente operacionalizable, y con esto, comparable. Por operacionalización se define el paso de las técnicas teóricas a una serie de instrucciones y artefactos que permiten aplicarlos de forma sistemática, eliminando en lo posible la ambigüedad y espacios de toma de decisión que requieran una experticia más allá del conocimiento del método.
- Validar y comparar empíricamente las propuestas en cuanto a su impacto sobre la calidad (desde el punto de vista del seguridad) y la efectividad en la identificación de amenazas de seguridad.
- Transferir estos métodos a contextos industriales de uso, a partir de la construcción de un vocabulario común entre los métodos propuestos y los conceptos y actividades realizadas por los practicantes y expertos de seguridad, usando *grounded theory [1],* y la realización de estudios de casos en proyectos reales.

En el presente trabajo se elabora la evolución del diseño experimental con el obejtivo de aboradar el primero de los puntos anteriores. A saber, mejorar la operacionalización del protocolo de ejecución de las tecnincas evaluadas.

3 Trabajo relacionado

3.1. Patrones de Seguridad y Tácticas de Seguridad

Los patrones de diseño [8] son soluciones encapsuladas a problemas recurrentes en contextos específicos; los Patrones de seguridad se basan en esta idea mediante la definición de soluciones recurrentes manejar amenazas de seguridad o solucionar una vulnerabilidad [7]. Los Patrones de seguridad se consideran una buena manera de construir sistemas seguros y existen varias metodologías basadas en ellos [7],[6]. Los Patrones de seguridad incluyen una solución a un problema de seguridad y varias

secciones que definen su uso, aplicabilidad, ventajas y desventajas. Una forma alternativa de construir sistemas seguros se basa en la idea de Tácticas, que son "medidas" o "decisiones" adoptadas para mejorar atributo de calidad [11] [9]; son "bloques de construcción arquitectural de los cuales se crean patrones arquitectónicos"[3]. Las Tácticas arquitectónicas también son vistas como decisiones que codifican y registran mejores prácticas para lograr algún atributo de calidad [11]. Bass [3] plantea que las Tácticas son unidades atómicas de toma de decisión, que son componentes de otras estrategias más complejas para la toma de decisiones de seguridad, como los Patrones de Seguridad. Una idea similar es la presentada por [16], que analiza Patrones y Tácticas como elementos de distinto nivel de abstracción, pero no desarrolla un estudio comparativo formal de ambos enfoques. La concepción de Patrones y Tácticas como soluciones de distinto nivel de abstracción ha sido soportado por modelos para la reclasificación de patrones de alto nivel como tácticas, como el propuesto en [17], sin embargo, no existe un modelo teórico que permita evidenciar la relación entre Patrones de Seguridad y Tácticas de Seguridad.

3.2. Trabajo previo: comparación de Patrones de Seguridad y Tácticas de Seguridad

En [14], se presentó una actividad experimental exploratoria con el fin de comparar los Patrones de Seguridad y las Tácticas de Arquitectura para el atributo de seguridad. Los resultados principales de este estudio no mostraron evidencia significativa de diferencias en las técnicas en cuanto a su capacidad de mitigación de amenazas, pero si se detectaron diferencias significativas en la cantidad de amenazas de seguridad identificadas entre los participantes expertos y los novatos. Este hallazgo llevó a dos cuestionamientos: ¿es la identificación de amenazas era una actividad separable de la mitigación?, y ¿es factible operacionalizarla, tal como lo se hizo con la mitigación de amenazas?. Como resultado se realizó una búsqueda bibliográfica de técnicas de identificación de amenazas para poder diseñar una replicación que permitiera realizar esta actividad de manera guiada, y así explorar diferencias con el estudio anterior.

3.3. Trabajo relacionado: Identificación de amenazas de seguridad

Se llevó a cabo una revisión bibliográfica para determinar si la identificación de amenazas podía ser tratada como una actividad independiente. En [12], se esquematiza el proceso de toma de decisiones de seguridad como un continuo ir y venir desde los requerimientos de seguridad las decisiones para satisfacerlos. Estas soluciones a su vez establecen nuevos requerimientos de seguridad, que deben ser considerados en el siguiente refinamiento del proceso iterativo-incremental. En este proceso, las tácticas son las decisiones de diseño del primer ciclo de iteraciones, que posteriormente son materializadas en componentes concretos.

En [2], el autor propone un enfoque para la captura de requerimientos de seguridad desde los Casos de Uso tradicionales, mediante el análisis de los *inversos* de un caso de uso (*mis-casos de uso o misuse cases*), es decir, “las funciones que el sistema no debería permitir”. También se analizan los *mis-actores*, como un ente para el que no

se quiere que el sistema ofrezca apoyo. Son los *mis-actores* los que inician los *mis-casos de uso*. La técnica no plantea relación alguna entre la identificación de requerimientos de seguridad y su mitigación.

En [4], se propone el uso de diagramas de actividad para la identificación de requerimientos de seguridad. La técnica propone analizar cada actividad de un diagrama e identificar como puede ser subvertidas para producir usos maliciosos de la información. Otra técnica que permite identificar requerimientos de seguridad son los *Fault Trees* [5], que permiten derivar amenazas específicas. En [15] y en [13], se realiza una comparación experimental entre árboles de ataque y *misuse cases*, concluyendo que los árboles de ataque son más efectivos, sobre todo cuando no hay casos de uso previamente escritos, sin embargo los *misuse cases* permiten identificar amenazas complementarias a los de los *attack trees*. Finalmente, [7] plantea un proceso que va desde identificación de amenazas de seguridad a su mitigación, que se integra con el proceso de desarrollo e incorpora las técnicas de *misuse activities* y patrones de seguridad.

En resumen, con los antecedentes aquí descritos, se considera que sí existe evidencia de que la actividad de identificación de amenazas ha sido tratada previamente como un problema separado de la mitigación.

4 Método de identificación de amenazas

El método utilizado está principalmente basado en *misuse activities* [4]. Se seleccionó este método debido al buen nivel de detalle de la técnica, que especifica un conjunto de pasos abordables y productos intermedios, y que puede ser seguido por sujetos sin conocimiento avanzado en seguridad.

Se operacionalizó distinguiendo las tareas listadas a continuación:

1. Revisar antecedentes: Los sujetos revisan una descripción general del sistema, sus casos de uso, diagramas de secuencia del sistema, modelo de dominio, diagrama de componentes y despliegue. También se describen las políticas de seguridad para el sistema. No existen productos de trabajo asociados a esta actividad.
2. Identificar assets de datos: Desde el modelo de dominio, los sujetos deben listar las entidades que manejan datos sensibles. El producto de trabajo asociado es una lista de los assets de datos, con un identificador correlativo que será referenciado en actividades posteriores.
3. Identificar assets funcionales: Para un conjunto definido de casos de uso, los sujetos seleccionan las interacciones sensibles de seguridad. En este punto, se introduce una modificación método original de misuse activities, consistente en considerar las interacciones entre los actores y el sistema, descrita en diagramas de secuencia del sistema, como el universo posible de funciones sensibles. Esta propuesta se sustenta en la idea de que todas las interacciones de usuario sistema son potenciales puntos de ataque. Esta hipótesis fue validada en entrevistas con expertos.

4. Identificar amenazas: Los sujetos identifican amenazas de seguridad, respondiendo a la siguiente pregunta:

"Qué mal uso podría hacerse en la <*asset funcional*> por parte de <*origen*> que comprometa la <*atributo de seguridad*> del <*asset de datos*>"

Donde:

- *asset funcional* corresponde a las interacciones identificadas en el paso 2.
- *origen* puede ser externo (outsider), interno autorizado, o interno no autorizado.
- los *atributos de seguridad* son confidencialidad, integridad, disponibilidad y responsabilidad (*accountability*)
- los *assets de datos* son los identificados en el paso 1.

En este punto, se utilizó el mismo formato y técnica descrita en [4]. Los resultados son listados en una estructura como la mostrada en la tabla 1.

Tabla 1. Tabla de identificación de amenazas.

Actor	**Asset Funcional**	**Id Amenaza**	**Atributo de Seguridad**	**Origen**	**Descripción**	**Asset de datos**

En esta estructura, cada tupla actor-actividad-atributo-origen-asset de dato es considerada una amenaza distinta.

Para poder llevar a cabo la actividad con sujetos sin conocimiento experto en seguridad, se realizó un entrenamiento en el que se presentaron los conceptos base de seguridad, los atributos de seguridad, y fundamentos conceptuales y aplicación práctica de la identificación de assets de datos, funcionales y amenazas con el método propuesto. El entrenamiento fue realizado dos semanas previas a la ejecución de la evaluación empírica.

5 Evaluación empírica

5.1. Objetivo, hipótesis y variables

El objetivo de la actividad es doble: se busca comparar la cantidad de amenazas identificadas con el método de identificación propuesto con los resultados de la anterior ejecución del experimento, y mejorar el diseño experimental anterior para continuar en el objetivo de conseguir comparar Patrones y Tácticas como técnicas de mitigación de amenazas de Seguridad. Para ello, se han reutilizado la mayoría de las definiciones y materiales de la anterior ejecución, salvo los cambios propios del nuevo método de identificación.

Considerando este objetivo dual, las hipótesis son la existencia de diferencias en la cantidad de amenazas identificadas sin utilizar método alguno comparadas con la

cantidad de amenazas identificadas con el método propuesto, y como evolución de la actividad experimental anterior, la existencia de diferencias en la calidad de la mitigación usando patrones o tácticas de seguridad.

Las variables definidas para responder estas hipótesis son la cantidad de amenazas listadas por los sujetos, y la calidad de la mitigación de estas amenazas con patrones o tácticas de seguridad.

Los sujetos de la actividad original y esta nueva iteración son distintos pero comparables en experiencia y formación, y trabajarán sobre el mismo problema de la primera ejecución. En esta iteración no participarán sujetos expertos, pero caracterizamos de manera más detallada a los sujetos inexpertos, con el fin de buscar diferencias dadas por experiencia o formación. En la actividad original, se consideró como un sujeto experto a profesionales TI con experiencia en toma de decisiones de arquitectura de software y seguridad. Tanto en la actividad experimental original como en esta nueva iteración, los sujetos inexpertos son estudiantes de pregrado de quinto año, sin experiencia en decisiones arquitectónicas o de seguridad en proyectos reales de desarrollo de software.

En la actividad original, los sujetos listaron las amenazas identificadas, que fueron comparadas con un *ground truth* establecido por evaluadores expertos. Para poder comparar estas observaciones con los resultados producidos por el método propuesto, se consideró la totalidad de amenazas identificadas por los sujetos, no sólo aquellas consideradas como prioritarias según el *ground truth*.

Para la evaluación de calidad, se tomó el mismo enfoque que en la actividad experimental anterior, consistente en la evaluación experta de las tácticas o patrones de seguridad seleccionados para mitigar cada amenaza. Cada amenaza es evaluada en una escala de 1 a 5, de acuerdo a la escala mostrada en la tabla 2.

Tabla 2. Escala de evaluación para la revisión experta

Escala de Evaluación	**Resultado**
5	Mitiga todos los casos en la amenaza
4	Mitiga casi todos los casos, pero hay excepciones peligrosas
3	Mitiga algunos casos, pero la mayoría de ellos sigue abierto
2	Mitiga casos triviales, pero no la mayoría
1	La amenaza no es mitigada

5.2 Ajustes a procedimiento de mitigación de amenazas

Tanto los patrones como las tácticas de seguridad fueron aplicadas de la misma forma que en el experimento original, esto es, seleccionando una o más tácticas desde los catálogos disponibles. A diferencia del experimento original, las tácticas y patrones fueron listados y asociados a amenazas, y se omitió su descripción usando la nomenclatura de [10]. Este cambio obedece a que los expertos opinaron que su uso no aportó en el entendimiento de la solución propuesta por los sujetos, y que no es una práctica estandarizada o masificada en la industria.

Para impedir que el paso previo de identificación afectara los resultados de la mitigación, se entregó a los sujetos un listado de amenazas base a mitigar, en forma posterior a la actividad de identificación de amenazas.

5.3 Ejecución de la actividad

Todos los sujetos participantes fueron entrenados satisfactoriamente, lo que se verificó mediante un ejercicio comparable al problema a resolver en el experimento.

La actividad experimental tuvo la siguiente distribución de sujetos:

Tabla 3. Distribución final se sujetos entre grupos, para mitigación de amenazas.

	Cantidad de participantes
Técnica 1: Tácticas	7
Técnica 2: Patrones	6

Los datos recolectados fueron revisados en busca de no adherencias al proceso. Para ello, se verificó la existencia de los productos intermedios definidos por cada paso en la actividad, no encontrándose casos problemáticos a primera vista. En el caso del segundo grupo de 5 sujetos, por un imprevisto técnico no se pudo recopilar la encuesta de salida.

Considerando la actividad experimental anterior, para mitigación los sujetos quedaron distribuidos de la siguiente forma:

Tabla 4. Distribución final se sujetos entre grupos, para identificación de amenazas.

	Cantidad de participantes
Técnica 1: sin método de identificación	12
Técnica 2: con método de identificación de amenazas propuesto	13

5.4 Análisis

Se evaluó la diferencia en la cantidad de amenazas identificadas en las dos ejecuciones del experimento. En la primera ejecución, los sujetos no utilizaron un método específico de identificación, mientras que en la segunda ejecución utilizaron la adaptación de *misuse activities* propuesta.

En este caso, el diseño considerado es de comparación de dos grupos, entre sujetos, con una variable (el método de identificación utilizado). La cantidad de amenazas considera corresponde al conteo de las amenazas listadas por los sujetos. Cabe señalar que en la ejecución de 2013 sólo se habían contabilizado las amenazas prioritarias (establecidas en un *ground truth* definido por expertos), pero en esta oportunidad se consideró el listado completo generado por cada sujeto.

Se excluyó a los expertos de cursos de postgrado del grupo de la ejecución original, para tener poblaciones comparables (alumnos de quinto año). Los datos finales se ilustran en la tabla 5.

Para comparar el efecto de los tratamientos, se realizó un análisis descriptivo. Para el grupo que no utilizó un método de identificación de amenazas, no se cumple la suposición de normalidad, como muestra la tabla 6. Para el grupo que utilizó el método de identificación propuesto, se encontraron dos outliers, por los extremos superior e inferior de la población. Al analizar el procedimiento seguido por ambos sujetos, se decide no descartar las observaciones, ya que no se aprecian deficiencias en la ejecución del método, pues ambos sujetos siguen todos los pasos sugeridos y sus resultados finales son coherentes con los pasos intermedios. Con estos antecedentes, se descarta la aplicación de un t-test.

Tabla 5. Datos de identificación de amenazas

Método	**Sujeto**	**Nº Amenazas**
Sin Método	1	4,00
Sin Método	2	4,00
Sin Método	3	4,00
Sin Método	4	5,00
Sin Método	5	4,00
Sin Método	6	4,00
Sin Método	7	3,00
Sin Método	8	5,00
Sin Método	9	3,00
Sin Método	10	4,00
Sin Método	11	3,00
Sin Método	12	3,00

Método	**Sujeto**	**Nº Amenazas**
Método propuesto	13	10,00
Método propuesto	14	13,00
Método propuesto	15	9,00
Método propuesto	16	7,00
Método propuesto	17	11,00
Método propuesto	18	16,00
Método propuesto	19	10,00
Método propuesto	20	10,00
Método propuesto	21	10,00
Método propuesto	22	4,00
Método propuesto	23	3,00
Método propuesto	24	8,00
Método propuesto	25	9,00
Método propuesto	26	11,00

Se toma un enfoque no paramétrico, encontrándose diferencias en la distribuciones al aplicar el test U de Mann-whitney, lo que impide realizar una comparación de medianas. Finamente se aplica un Test de Medianas, encontrándose diferencias significativas entre ambas, con un nivel de significancia del 95%. Los resultados sugieren que el método propuesto produce mejores resultados en identificación de amenazas que el enfoque original, es decir, sin un enfoque sistemático para la identificación de amenazas.

Tabla 6. Prueba de normalidad para identificación de amenazas.

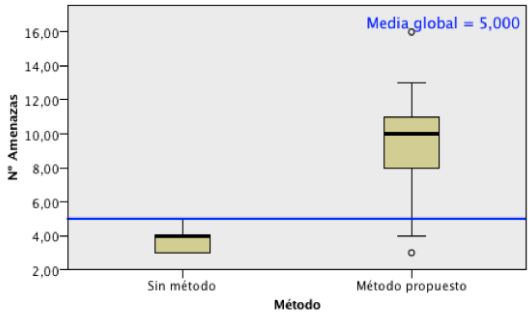
Pruebas de normalidad

	Método	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
		Estadístico	gl	Sig.	Estadístico	gl	Sig.
Nº Amenazas	Sin método	,258	12	,026	,818	12	,015
	Método propuesto	,157	13	,200*	,956	13	,688

*. Este es un límite inferior de la significación verdadera.

a. Corrección de la significación de Lilliefors

Prueba de medianas de muestras independientes



N total	25
Mediana	5,000
Probar estadística	18,132
Grados de libertad	1
Sig. asintótica (prueba de dos caras)	,000
Sig. exacta de Fisher (prueba de dos caras)	,000

Resumen de prueba de hipótesis

	Hipótesis nula	Test	Sig.	Decisión
1	Las medianas de Nº Amenazas son las mismas entre las categorías de Método.	Prueba de medianas de muestras independientes	,000[1,2]	Rechazar la hipótesis nula.

Se muestran las significancias asintóticas. El nivel de significancia es ,05.

[1]Se muestra la significancia exacta para esta prueba.

[2]Sig. exacta de Fisher

Fig. 1. Prueba de medianas para identificación de amenazas.

En cuanto a la mitigación de amenazas, no se encontraron diferencias significativas al utilizar patrones de seguridad y tácticas de seguridad. Cabe mencionar que en este resultado no influyó la identificación de amenazas, pues la actividad de mitigación partió sobre un listado de amenazas predefinido. Se espera evaluar el proceso completo desde identificación a mitigación en una próxima actividad experimental.

5.5 Discusión de validez

Siendo una actividad exploratoria con enfoque experimental, buscamos fortalecer principalmente la validez interna y de constructo [18]. En este contexto, se ha fortalecido la validez de constructo respecto a la actividad original, al formalizar la identificación de amenazas, lo que permite evolucionar nuestra actividad experimental hacia un experimento formal de comparación de tácticas y patrones. El hecho de haber hecho dos ejecuciones para la segunda actividad (agosto y diciembre)

podría constituir una amenaza, sin embargo, aplicando el mismo test de medianas, no se pudo establecer diferencias entre ambos grupos. Respecto a la validez interna, el diseño experimental y la asignación aleatoria de los sujetos a los grupos permite mitigar esta amenaza. Si bien se aplicó un pre-test de experiencia, sus datos no se consideraron relevantes para clasificarlos en grupos, pues no contaban con experiencia industrial real en actividades ligadas al diseño y/o construcción de sistemas seguros, y los aspectos conceptuales fueron nivelados a través del entrenamiento. La cantidad de sujetos puede ser también considerada una amenaza a la validez según [18], considerándose como trabajo futuro la realización de nuevas actividades involucrando más sujetos.

6 Conclusiones y trabajo futuro

Con el objetivo de comparar patrones y tácticas de seguridad con un enfoque empírico, se ha evolucionado el diseño experimental original, incorporando un nuevo método de identificación de amenazas. El método propuesto ha permitido formalizar una actividad que, en el acercamiento experimental preliminar, surgió como una amenaza para la comparación rigurosa de ambas técnicas. Se verificó que el método es aplicable en la práctica, y más aún, se obtuvo evidencia estadísticamente significativa de que este método propuesto es más efectivo en la identificación de amenazas que un enfoque ad hoc, aún con sujetos sin experiencia en el diseño de sistemas seguros. Este resultado contribuye al objetivo final de lograr un método sistemático para la mitigación de amenazas de seguridad. El trabajo futuro se centrará en la formalización experimental de un método de mitigación que incorpore el método de identificación propuesto, y que permita la comparación formal de Patrones y Tácticas de seguridad. Se explorará también la aplicación del método con problemas de mayor tamaño y complejidad, de modo de estudiar si la naturaleza combinatoria del análisis de amenazas no condiciona en la práctica la escalabilidad del método.

Agradecimientos

Este trabajo ha sido financiado por la Comisión Nacional de Investigación Científica y Tecnológica, CONICYT, a través del Fondo Nacional de Ciencia y Tecnología, FONDECYT regular folio 1140408.

Referencias

1. Adolph, S. et al.: A methodological leg to stand on: lessons learned using grounded theory to study software development. Presented at the (2008).
2. Alexander, I.: Misuse cases: use cases with hostile intent. IEEE Software. 20, 1, 58–66 (2003).
3. Bass, L. et al.: Software architecture in practice. Addison-Wesley, Upper Saddle

River, NJ (2013).
4. Braz, F.A. et al.: Eliciting Security Requirements through Misuse Activities. Presented at the September (2008).
5. Brooke, P.J., Paige, R.F.: Fault trees for security system design and analysis. Computers & Security. 22, 3, 256–264 (2003).
6. Fernandez, E.B. et al.: Defining Security Requirements Through Misuse Actions. In: Ochoa, S.F. and Roman, G.-C. (eds.) Advanced Software Engineering: Expanding the Frontiers of Software Technology. pp. 123–137 Springer US.
7. Fernandez, E.B.: Security patterns in practice: designing secure architectures using software patterns. John Wiley & Sons Ltd, Chichester, West Sussex (2013).
8. Gamma, E. ed: Design patterns: elements of reusable object-oriented software. Addison-Wesley, Reading, Mass (1995).
9. Harrison, N.B. et al.: On the impact of fault tolerance tactics on architecture patterns. Presented at the (2010).
10. Harrison, N.B., Avgeriou, P.: How do architecture patterns and tactics interact? A model and annotation. Journal of Systems and Software. 83, 10, 1735–1758 (2010).
11. Harrison, N.B., Avgeriou, P.: Leveraging Architecture Patterns to Satisfy Quality Attributes. In: Oquendo, F. (ed.) Software Architecture. pp. 263–270 Springer Berlin Heidelberg, Berlin, Heidelberg (2007).
12. Heyman, T. et al.: The Security Twin Peaks. In: Erlingsson, Ú. et al. (eds.) Engineering Secure Software and Systems. pp. 167–180 Springer Berlin Heidelberg, Berlin, Heidelberg (2011).
13. Karpati, P. et al.: Comparing attack trees and misuse cases in an industrial setting. Information and Software Technology. 56, 3, 294–308 (2014).
14. Noël, R. et al.: An Exploratory Comparison of Security Patterns and Tactics to Harden Systems. ISBN: 978-1-63266-649-9 17th Conferencia Iberoamericana en Software Engineering. 378–391 (2014).
15. Opdahl, A.L., Sindre, G.: Experimental comparison of attack trees and misuse cases for security threat identification. Information and Software Technology. 51, 5, 916–932 (2009).
16. Rehn, C.: Software Architectural Tactics and Patterns for Safety and Security. TU Kaiserslautern, 67663 Kaiserslautern, Germany.
17. Ryoo, J. et al.: A Methodology for Mining Security Tactics from Security Patterns. Presented at the (2010).
18. Wohlin, C., Runeson,Per, Höst,Martin, Ohlsson,Magnus C, Regnell, B., Wesslén,Anders: Experimentation in Software Engineering. Springer, New York (2012).