Arquitectura de Seguridad por Capas en Sistemas Críticos

Oscar Martín Bianchi [a,b]
oscarmartinbianchi@gmail.com

Ignacio Martín Gallardo Urbini [a,b]
ignaciommgu@gmail.com

German Luis Vila Krause [a]
g.vilakrause@gmail.com

Ignacio Arrascaeta [a]
ignacioarrascaeta@gmail.com

[a] CIDESO[0], DIGID[1] - Ejército Argentino
[b] EST[2], IESE[3] - Ejército Argentino

RESUMEN

El rotundo avance de la tecnología nos presenta continuamente nuevas herramientas y facilidades para el desarrollo de sistemas electrónicos e informáticos, que permiten mejorar y/o complementar los procedimientos existentes en el campo militar. Por este motivo, es esencial identificar los posibles riesgos que estas tecnologías pueden acarrear, para así poder preparar a los sistemas críticos desarrollados en dicho ámbito para posibles contingencias.

La presente investigación plantea la posibilidad de adaptar técnicas de la industria, más específicamente del área de seguridad informática y ciberdefensa, a los sistemas desarrollados por el Centro de Investigación y Desarrollo de Software Operacional (en adelante CIDESO), en el ámbito de los sistemas de propósito crítico[a] (tanto en el área de Comando y Control, como en la de apoyo en situación de catástrofe).

Palabras Clave: *Seguridad Informática, Ciberdefensa, Comando y Control, Arquitectura, Sistemas Críticos.*

CONTEXTO

El Ejército Argentino financia y patrocina la construcción de un sistema de Comando y Control (C2) para sus Grandes Unidades de nivel táctico (Brigadas), así como de sistemas de C2 a nivel unidad de combate, y cuenta con la asignación de presupuesto específico y subsidios asignados por el Programa de Investigación y Desarrollo para la Defensa (PIDDEF) del Ministerio de Defensa de la República Argentina. La finalidad de los sistemas de C2 es dar soporte a los procesos de toma de decisiones que realizan los comandantes y sus equipos de asesores (Estado Mayor), optimizando el flujo de información operativa y decisoria en todos los niveles de la estructura orgánica de las brigadas, integrándose en forma horizontal y vertical.

El CIDESO, posee una amplia experiencia en el desarrollo de aplicaciones militares y sistemas de propósito crítico, tanto para problemas militares operativos – Batalla Virtual (BV), Sistema Integrado Táctico del Ejército Argentino (SITEA) – como para operaciones militares de paz – Simupaz –.

Cómo explotación de esa capacidad, y con la experiencia obtenida tanto en el desarrollo del sistema de C2 del Ejército Argentino (EA), bajo el nombre de proyecto Sistema Integrado Táctico de Comando y Control del Ejército Argentino (SITEA, (BIM) N° 413, PIDDEF

[a] Sistemas cuyo fallo atenta contra el cumplimiento de los objetivos previstos para el mismo, y que pone en riesgo vidas humanas o bienes materiales.

[1] CIDESO: Centro de Investigación y Desarrollo de Software
[2] DIGID: Dirección General de Investigación y Desarrollo
[3] EST: Escuela Superior Técnica – Facultad de Ingeniería del Ejército Argentino
[4] IESE: Instituto de Enseñanza Superior del Ejército – Universidad del Ejército Argentino

037/10), como de BV, se propuso la aplicación del conocimiento logrado para el desarrollo de un sistema que permita la conducción de las operaciones de apoyo de fuego dentro de la red de apoyo de fuego. Así surgió el Sistema de Automático de Tiro de Artillería de Campaña (SATAC).

Ambos sistemas por separado aportaron un gran valor en conocimiento para el desarrollo que se emprendió con el proyecto anteriormente mencionado.

En este contexto, la introducción de la posibilidad de sumar elementos de seguridad resulta absolutamente crucial, dada la criticidad de los proyectos desarrollados.

1. INTRODUCCIÓN

Una de las razones por la que la presente investigación toma especial relevancia es el hecho de que se trata del primer esfuerzo en el diseño de una arquitectura de seguridad para un sistema de propósito crítico por parte del CIDESO, que esté a la altura de las exigencias modernas.

Para esto resultaron claves tanto la pluralidad de conocimientos del equipo conformado por profesionales del ámbito de Sistemas, Defensa y alumnos de distintas universidades de Ingeniería, como el conocimiento del negocio y del entorno del sistema, así como de los posibles factores de riesgo a los que se encontraba expuesto.

Uno de los principales problemas planteados, fue la necesidad de que la solución aportada por la arquitectura a diseñar fuese transparente tanto al medio como a la tecnología a utilizar (1), centrándose más específicamente en la definición de políticas y procedimientos (2).

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

En el marco del desarrollo del proyecto presentado anteriormente, se pretende lograr un avance significativo, no solo en lo que respecta a la seguridad intrínseca de los desarrollos llevados a cabo por el CIDESO, sino que además plantee una base de conocimientos y requerimientos mínimos para el desarrollo de los sistemas de ahora en adelante. Por lo tanto, se plantea lograr:

- Incluir dentro de los sistemas de propósito crítico siendo desarrollados por el CIDESO, estrategias de seguridad que atiendan la criticidad de los sistemas.
- Aportar nuevas herramientas que permitan potenciar los atributos de calidad asociados a la seguridad en los sistemas que están siendo desarrollados actualmente en el CIDESO.
- Posibilidad de desarrollar nuevas estrategias de seguridad basándose en el estado del arte de la industria y las experiencias obtenidas por los actores más destacados.

Así mismo, se decidió separar la investigación en dos grandes áreas:

- Seguridad Física: Dada la naturaleza de los sistemas que están siendo desarrollados por el CIDESO, el acceso físico a los equipos resulta una problemática clave a tener en cuenta en cualquier solución propuesta, ya que el mismo puede comprometer seriamente la integridad de los sistemas.
- Seguridad lógica: Esta línea agrupa todas las medidas, procedimientos y decisiones destinados a proteger la información del sistema que impactan directamente sobre la implementación del mismo.

3. RESULTADOS OBTENIDOS/ESPERADOS

Las presentes líneas de investigación tienen por objetivo:

- Facilitar la comprensión de la temática, y el trabajo a realizar, capacitando a los técnicos y artesanos responsables de la implementación mediante tareas de investigación y actualización.

- Obtener una arquitectura de seguridad para el sistema, que sea independiente del medio, y cuya implementación no impacte fuertemente en la programación temporal del proyecto.
- Obtener una arquitectura de seguridad para el sistema, cuya implementación garantice los atributos de seguridad mínimos para un sistema de C2.

Los primeros resultados de la línea de investigación decantaron hacia un diseño de defensa por capas ("Layered Security Approach[b]") (3) (2) (4) (5) dadas las ventajas que ofrece:

- Independencia del medio.
- Independencia de la Tecnología.
- Muy Bajo índice de acoplamiento entre capas.
- Alto índice de transparencia al usuario.

Este diseño implica:

- Definición de Políticas.
- Definición de la Arquitectura.
- Definición de Mecanismos de seguridad.

Entre las políticas determinadas, podemos contar las siguientes:

- Autenticación Multifactor: Combinación del uso de dos o más credenciales distintas, de distinta naturaleza (distinto factor, por ejemplo, una clave alfanumérica y una clave biométrica como la huella digital) (6) (7).
- Encriptado de archivos, disco y dispositivos extraíbles: Encriptado de los medios que intervienen en el funcionamiento del sistema.
- Autenticación para las Comunicaciones: Definición de mecanismos de autenticación para el intercambio de información entre los diferentes usuarios del sistema.
- Cifrado de Comunicaciones: Cifrado de toda la información que se transmite en el sistema, entre las distintas terminales del mismo.
- Segmentación de los Datos: Segmentar una Base de Datos implica agrupar a los usuarios de la misma según determinados aspectos y características en común, con el fin de acotar el dominio de los datos a los que cada grupo o individuo tiene acceso.
- Seguridad por Control de Contenido: No todos los datos e información que circulan en un sistema tienen el mismo nivel de criticidad, ni requieren que se tomen las mismas medidas de seguridad.

Como objetivo final de la investigación se espera obtener una correcta definición de los mecanismos, así como una separación lógica de las distintas capas de la arquitectura, de modo tal que se pueda implementar cada una de forma independiente de la anterior, pero que a su vez sigan siendo complementarias entre sí (5) (8).

La investigación debería, en última instancia, dar como resultado un prototipo experimental-operacional que atienda a cada una de las políticas suscriptas por la arquitectura, de modo que permita ser evaluado por los organismos correspondientes.

4. FORMACIÓN DE RECURSOS HUMANOS

Una característica distintiva de los sistemas desarrollados por el CIDESO, es la estrecha colaboración con los laboratorios y departamentos de la EST. Esto pone al proyecto en un ámbito privilegiado para la formación de recursos humanos.

Por un lado, el CIDESO tiene amplia experiencia en la formación de recursos humanos en el terreno de la investigación aplicada en sistemas de información de diversa

[b] Consiste en la combinación de distintos controles y medidas de seguridad de efecto acumulativo, destinadas a resguardar recursos o información.

índole, incluyendo sistemas de simulación para el adiestramiento, sistemas de información geográfica, sistemas de visualización, sistemas inteligentes, sistemas móviles, sistemas de comunicación de alta complejidad y sistemas de cómputo de alto rendimiento. Por el otro, la EST tiene experiencia en investigación básica en el terreno de la ciencia de la informática, asociado estrechamente al hecho de poseer la carrera de Ingeniería Informática como parte de su oferta académica.

También cabe mencionar que cuenta con expertos informáticos, matemáticos y criptógrafos que dan cuerpo en numerosas ocasiones a las investigaciones de los trabajos finales de carrera que se realizan en los posgrados que brinda la universidad.

Tanto el CIDESO como los laboratorios de la EST, a través del dictado de materias de grado en Ingeniería Informática, aportan recursos humanos a la misma universidad. Es así que investigadores de los laboratorios dan cátedras en la EST y, de manera análoga, alumnos de la escuela aportan sus análisis a los laboratorios a través de trabajos prácticos de laboratorio, prácticas profesionales supervisadas o tesis y tesinas de grado y posgrado.

Para el próximo paso, se pretende continuar con esta interacción fluida entre los centros de investigación y el alumnado, formado profesionales con conocimientos de campo en el terreno de la computación de alto rendimiento y un conocimiento acabado sobre temas criptográficos.

Además, al expandirse el sistema para ser aplicado en cualquier problema que requiera altos niveles de cómputo, se pretende incorporar alumnos y docentes de otras cátedras, de cualquiera de las ingenierías que se dictan en la Facultad.

Así, pues, se formarán recursos humanos de todos los niveles, grado, posgrado o investigadores activos, incorporando más alumnos a los laboratorios y, potencialmente, becarios que se dediquen de modo formal (no sólo académico) a la profundización de los modelos propuestos.

5. BIBLIOFRAFÍA

1. **Blobel, Bernd and Roger-France, Francis.** *A systematic approach for analysis and design of secure health information systems.* s.l. : International Journal of Medical Informatics, 2001.

2. **Jim, Alves-Foss, Carol, Taylor and Paul, Oman.** *A Multi-layered Approach to Security in High Assurance Systems.* s.l. : University of Idaho .

3. **Baker, Bruce and Scheye, Eric.** *Multi-layered justice and security delivery in post-conflict and fragile states.* s.l. : Conflict, Security & Development, 2007.

4. **Mehmet, Yildiz, Jemal, Abawajy and Tuncay, Ercan.** *A Layered Security Approach for Cloud.* s.l. : 10th International Symposium on Pervasive Systems, Algorithms, and Networks, 2009.

5. **Shenk, Jerry.** *Layered Security: Why It Works.* s.l. : SANS Institute, 2013.

6. **Abhishek, Kumar, et al.** *A Comprehensive Study on Multifactor Authentication Schemes.* Berlin : Advances in Intelligent Systems and Computing, vol 177, 2013.

7. **on, Guidance.** *Guidance on Multi-factor Authentication.* s.l. : State Services Commission, 2016. 0-478-24466-5.

8. **Gupta, Kapil Kumar, Nath, Baikunth and Kotagiri, Ramamohanarao.** *Layered Approach Using Conditional Random Fields for Intrusion Detection.* Washington : IEEE Transactions on Dependable and Secure Computing, 2010.

9. **Zhiyuan, Shi and Lianfen, Huang.** *Layered security approach in LTE and simulation.* s.l. : 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication, 2009., 2009.

10. **Komninos, Nikos, Vergados, Dimitrios D. and Douligeris, Christos.**

Authentication in a layered security approach for mobile ad hoc networks. 2007.

11. **Behl, Akhil.** *Emerging security challenges in cloud computing.* s.l. : World Congress on Information and Communication Technologies, 2011.

12. **Payne, Bryan D., Sailer, Reiner and Cáceres, Ramón.** *A layered approach to simplified access control in virtualized systems.* New York : s.n., 2007.

13. **Banyal, Rohitash Kumar, Jain, Pragya and Jain, Vijendra Kumar.** *Multi-factor Authentication Framework for Cloud Computing.* 2013. 978-0-7695-5155-5.

14. *Multi-factor Authentication.* s.l. : SafeNet, 2013.