Análisis y control de riesgos de seguridad informática: control adaptativo

Un cambio de paradigma hacia la gestión de riesgos orientada al control adaptativo.

Juan Manuel García G.
Carol A. Martínez R.

La seguridad informática puede ser definida, básicamente, como la preservación de la confidencialidad, la integridad y la disponibilidad de los sistemas de información [Tipton, 2006]. Dependiendo del entorno de la organización, se pueden tener diferentes amenazas que comprometan a los objetivos previamente mencionados. Ante un riesgo concreto, la organización tiene tres alternativas: aceptar el riesgo, hacer algo para disminuir la posibilidad de ocurrencia del riesgo o transferir el riesgo, por ejemplo, mediante un contrato de seguro. A las medidas o salvaguardas que se toman para disminuir un riesgo se les denomina *controles de seguridad* [Tipton, 2006; Witman, 2007]. Los controles de seguridad informática usualmente se clasifican en tres categorías: controles físicos, controles lógicos o técnicos y controles administrativos [Tipton, 2006].

Para que los controles sean efectivos, éstos deben estar integrados en lo que se denomina una *arquitectura de seguridad informática* [Tudor, 2006], la cual debe ser congruente con los objetivos de la organización y las prioridades de las posibles amenazas de acuerdo al impacto que éstas tengan en la organización. Por lo tanto, una fase fundamental en el diseño de la arquitectura de seguridad informática es la etapa de análisis de riesgos [Peltier, 2005; Landoll, 2005].

Sin importar cual sea el proceso que se siga, el análisis de riesgos comprende los siguientes pasos [Peltier, 2005]:

1. Definir los activos informáticos a analizar.
2. Identificar las amenazas que pueden comprometer la seguridad de los activos.
3. Determinar la probabilidad de ocurrencia de las amenazas.
4. Determinar el impacto de las amenaza, con el objeto de establecer una priorización de las mismas.
5. Recomendar controles que disminuyan la probabilidad de los riesgos.
6. Documentar el proceso.

Las metodologías de análisis de riesgo difieren esencialmente en la manera de estimar la probabilidad de ocurrencia de una amenaza y en la forma de determinar el impacto en la organización. Las metodologías más utilizadas son *cualitativas*, en el sentido de que dan una caracterización de “alta/media/baja” a la posibilidad de contingencia más que una probabilidad específica. El estándar ISO/IEC 27001 adopta una metodología de análisis de riesgos cualitativa [Calder, 2007]. El ISO/IEC 27001 es un estándar internacional para los sistemas de gestión de la seguridad informática, que está estrechamente relacionado al estándar de controles recomendados de seguridad informática

ISO/IEC 17799 [Calder, 2003]. El estándar NIST 800-39 del gobierno americano también adopta una metodología cualitativa [NIST, 2002].

La dificultad de adoptar una metodología de análisis de riesgo cuantitativa es la complejidad de determinar el impacto de un evento no deseado [Anderson, 2001] y, principalmente, la falta de datos suficiente para poder determinar de manera exacta las funciones de distribución de probabilidad para las amenazas más comunes [Kotulic, 2003; Ciechanowicz, 1997]. Por otro lado, en las metodologías cualitativas, la estimación de probabilidades dependerá de la experiencia de quienes realizan el análisis.

Además de estas limitaciones en el enfoque actual de análisis de riesgos, existen otras de mayor alcance que exploraremos en la siguiente sección.

Limitantes del análisis de riesgo

En general, a pesar de que se han desarrollado muchas soluciones a los problemas de la seguridad en los sistemas de información, la apreciación general es que la inseguridad es un problema que no ha sido resuelto [Viega, 2005]. La perspectiva parece poco optimista, principalmente debido a que los atacantes han pasado de ser aficionados en busca de notoriedad a criminales en busca de lucro [Schneier, 2005].

Posiblemente una de las principales razones por las cuales los problemas de seguridad informática no han sido resueltos es la aparición frecuente de nuevas amenazas. Como un ejemplo de esto es la evolución del malware: los virus altamente nocivos y de amplia difusión han dado lugar a *botnets* furtivos, de difícil detección y dirigidos a objetivos específicos [Schultz, 2006].

Precisamente una de las debilidades de las metodologías de análisis de riesgo es que parten de una visión estática de las amenazas así como de los controles requeridos para disminuir los riesgos. El ciclo de vida establecido para las arquitecturas de seguridad informático suele ser demasiado extenso ante un entorno en cambio constante.

Los cambios en los riesgos que debe considerar una organización tienen dos orígenes:

a) El surgimiento de nuevas amenazas.
b) La adopción de nuevas tecnologías que da origen a riesgos no previstos.

Todo sistema de información evoluciona, debido a la integración de hardware y software con características nuevas y más atractivas para los usuarios, así como al desarrollo de nuevas funcionalidades. Estos cambios abren la posibilidad de riesgos imprevistos y también pueden crear vulnerabilidades donde antes no existían.

Algunos estudios han demostrado que existe una brecha entre el uso de tecnología moderna y el entendimiento de las implicaciones para la seguridad inherentes a su utilización [Loch, 1992]. En su momento, los administradores de sistemas de información que migraron sus organizaciones a entornos

altamente interconectados seguían visualizando las amenazas desde un punto de vista pre-conectividad. Como consecuencia, expusieron a sus organizaciones a riesgos de los cuales no eran concientes, se negaban a aceptar o frecuentemente estaban poco preparados para manejar [Loch, 1992]. Un escenario similar se ha presentado en la migración a las redes de área local inalámbricas. El uso de redes inalámbricas requiere de razonamientos distintos a los de la seguridad alambrada [Arbaugh, 2003].

Es entonces evidente que se requiere de arquitecturas de seguridad dinámicas, que sean altamente adaptables a los cambios en el entorno y en el sistema de información mismo, así como capaces de resistir a ataques no previstos. Se ha buscado alcanzar esas características imitando los mecanismos adaptativos de los seres vivos [Geer, 2007], tomando como modelo, por ejemplo, el sistema inmune [Ulieru, 2005].

En el presente trabajo proponemos una metodología de análisis y diseño de arquitecturas de seguridad informática basada en las técnicas de control adaptativo [Astrom, 1994].

Controles de seguridad adaptativos

En la mayoría de los casos, los controles de seguridad son de lazo abierto, esto es, el resultado de su funcionamiento no es retroalimentado para mejorar el desempeño del control. Por ejemplo, el cortafuego es uno de los controles más comúnmente utilizados en las redes informáticas. Las reglas de un cortafuego generalmente son fijas, y ante un cambio en los requerimientos de tráfico en la red, se deben cambiar manualmente las reglas de filtraje. Una manera de convertir al cortafuego en un mecanismo de lazo cerrado sería acoplarlo a un detector de intrusiones de modo tal que ante la detección de un posible ataque las reglas del cortafuego se modifiquen automáticamente para bloquear el tráfico sospechoso.

En general, la clave para lograr controles de seguridad adaptativos es convertirlos en controles de lazo cerrado. Para que el control pueda adaptarse a los cambios debe contar con un mecanismo de ajuste de sus parámetros de acuerdo al comportamiento actual del sistema y a un modelo de referencia que indique cuál debería ser el comportamiento deseado.

El primer punto es entonces establecer objetivos de control que se desean alcanzar mediante el mecanismo de control. Estos deben estar relacionados a la confidencialidad, integridad y/o disponibilidad de los datos, la información, los sistemas, etc. En segundo lugar, y como aspecto esencial, debe establecerse una medida del grado en que se están cumpliendo los objetivos de seguridad para determinar cuando es necesario un ajuste en los parámetros del controlador. Este punto supone que existe un modelo del comportamiento normal del sistema así como de las acciones requeridas para restablecerlo a la normalidad cuando se presente una anomalía.

La construcción de modelos para la detección de anomalías está siendo investigada como una técnica para la detección de intrusiones [Patcha, 2007].

Metodología propuesta

La metodología propuesta de análisis y diseño de una arquitectura de seguridad informática está centrada en el concepto de control adaptativo, si bien reconociendo que por la complejidad inherente a los sistemas de información, este concepto se aplicará como una referencia más que como una aplicación estricta de la teoría del control.

Esbozaremos solamente las etapas de la metodología propuesta:

1. Establecer los objetivos de control a alcanzar y/o mantener, en términos de confidencialidad, integridad y/o disponibilidad de los subsistemas del sistema a analizar.
2. Definir una medida que permita cuantificar el grado de logro de los objetivos de control o la desviación del mismo. Denominaremos a dicha medida, la *función de control,* la cual medirá el grado de confidencialidad, integridad y/o disponibilidad del subsistema.
3. El control de seguridad deberá diseñarse en términos de tres componentes: el *detector*, que medirá en tiempo real a la función objetivo, alimentándola al *ajustador* que en base a un modelo de referencia deberá establecer un ajuste de parámetros en el *controlador*.

El esquema anterior se utiliza frecuentemente cuando en el perímetro de una red se coloca a un detector de intrusiones, cuya función es analizar el tráfico de red y determinar si existe evidencia de un posible ataque, y de ser así, establecer reglas de filtraje adecuadas en un cortafuego. En este ejemplo, el IDS realiza las funciones del detector, el cortafuego las del controlador y el modelo de referencia estaría implícito en la programación de acoplamiento del IDS y del cortafuegos.

Un ejemplo: integridad de servidores

Para ilustrar como debería desplegarse la metodología previamente esbozada, discutiremos a continuación un ejemplo relacionado a la integridad de un servidor de red.

La integridad del sistema operativo de un servidor de red es una de las propiedades más relevantes a preservar. Existen diferentes herramientas para verificar la integridad de los archivos de un sistema operativo, que se basan en el uso de funciones de hash o MAC (*message authentication codes*) para detectar cuando un archivo ha sido alterado. Por sí mismas, dichas estas herramientas no previenen la alteración o pérdida de archivos de sistema, sin embargo, pueden ser de mayor utilidad cuando se integran a un mecanismo de control de acceso del sistema operativo.

Recientemente se han desarrollado implementaciones de modelos de control de acceso tales como el control de acceso obligatorio, seguridad multinivel o control de acceso basado en reglas [Jaruwek, 2006] que pueden ser utilizados como mecanismos de control de la integridad del sistema [Jaeger, 2003].

Una arquitectura colaborativa que detecta modificaciones no autorizadas a sus componentes para realizar en tiempo real modificaciones a la política de control

de acceso, lo que proporciona a dicha arquitectura cierta tolerancia a ataques, es revisada en [Blanc, 2006].

En [Lang, 2005] se muestra como, mediante la detección de violaciones a la integridad de la memoria de un sistema y su correlación a las entradas recibidas sobre la red, se pueden generar *automáticamente* firmas de ataques previamente desconocidos. De acuerdo a los autores, esta técnica conduciría a servidores que se auto-protegen.

Conclusiones

Hemos argumentado como el enfoque actual de análisis y gestión de riesgos de seguridad informática es inadecuado dado el constante avance tecnológico que lleva al surgimiento de amenazas emergentes. Se ha propuesto entonces una metodología que considere el diseño de controles adaptativos. Consideramos que este enfoque lleva a todo un cambio de paradigma en la gestión de la seguridad informática.

Referencias

[Tipton, 2006] Harold F. Tipton, Micki Krause (eds.), *Information Security Management Handbook, 5th Ed.*, CRC Press, 2006.

[Whitman, 2007] Michael E. Whitman, Herbert J. Mattord, *Management of Information Security*, Course Technology, 2007.

[Tudor, 2006] Jean Killmeyer Tudor (ed.), *Information Security Architecture: An Integrated Approach to Security in the Organization*, CRC Press, 2006.

[Peltier, 2005] Thomas R. Peltier, *Information Security Risk Analysis*, CRC Press, 2005.

[Landoll, 2005] Douglas J. Landoll, *The Security Risk Assesment Handbook: A Complete Guide for Performing Security Risk Assesments*, CRC Press 2005.

[Calder, 2003] Alan Calder, Steve Watkins, *IT Governance: A Manager's Guide to Data Security & BS 7799/ISO 17799, 2nd Ed.*, Kogan Page Ltd., London, 2003.

[Calder, 2007] Alan Calder, Steve Watkins, *Information Security Risk Management for ISO 27001/ISO 17799*, IT Governance Publishing, 2007.

[Loch, 1992] Karen D. Loch, Houston H. Carr, Merrill E. Warkentin, "Threats to Information Systems: Today's Reality, Yesterday's Understanding", *MIS Quarterly*, vol. 16, no. 2, 1992, pp. 173-186.

[NIST 2002] NIST, Risk Management Guide for Information Technology Systems, NIST Special Publication 800-30, 2002. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[Anderson, 2001] R. Anderson, "Why information security is hard – An economic perspective", *Proceedings of the 17th Annual Computer Security Applications Conference ACSAC'01*, IEEE Computer Society, 2001.

[Kotulic, 2003] Andrew G. Kotulic, Jan Guynes Clark, "Why there aren't more information security research studies", *Information & Management*, vol. 41, no. 5, pp. 597-607, 2003.

[Ciechanowicz, 1997] Zbigniew Ciechanowicz, "Risk analysis: requirements, conflicts and problems", *Computers & Security*, vol. 16, no. 3, pp. 223-232, 1997.

[Viega, 2005] John Viega, "Security – Problem solved?", *Queue*, vol. 3, no. 5, pp. 40-50, 2005.

[Schneier, 2005] Bruce Schneier, “Attack Trends: 2004 and 2005”, *Queue*, vol. 3, no. 5, pp. 52-53, 2005.

[Schultz, 2006] Eugene Schultz, “Where have the worms and viruses gone? – New trends and malware”, *Computer Fraud & Security*, vol. 2006, no. 7, pp. 4-8, 2006.

[Arbaugh, 2003] William A. Arbaugh, “Wireless Security is Different”, *Computer*, vol. 36, no. 8, pp. 99-101, 2003.

[Geer, 2007] Daniel E. Geer, “The evolution of security”, *Queue*, vol. 5, no. 3, pp. 30-35, 2007.

[Ulieru, 2005] M. Ulieru, P. Wortingthon, “Holonic risk management framework”, *IEEE International Conference on Systems, Man and Cybernetics*, vol. 1, pp. 209-214, 2005.

[Astrom, 1994] K. J. Astrom, B. Wittenmark, *Adaptive Control*, Addison Wesley, 1994.

[Patcha. 2007] Animesh Patcha, Jung-Min Park, “An overview of anomaly detection techniques: Existing solutions and latest technological trends”, *Computer Networks: The International Journal of Computer and Telecommunications Networking*, vol. 51, no. 12, 2007.

[Jaruwek, 2006] Marek Jaruwek, “RSBAC: A framework for enhanced Linux system security”, disponible en http://www.rsbac.org/doc/media/rsbac-marek2006.pdf

[Jaeger, 2003] Trent Jaeger, Reiner Sailer, Xiaolan Zhang, “Analyzing integrity protection in the SELinux example policy”, *SSYM’03: Proceedings of the 12th conference on USENIX Security Symposium*, pp. 5, 2003.

[Blanc, 2006] M. Blanc, J. Briffaut, P. Clemente, M. Gad El Rab, C. Toinard, “A Collaborative Approach for Access Control, Intrusion Detection and Security Testing”, *Proceedings of the International Symposium on Collaborative Technologies and Systems (CTS 2006)*, pp. 270-277, 2006.

[Lang, 2005] Zhenkai Lang, R. Sekar, “Fast and automated generation of attack signatures: a basis for building self-protecting servers”, *CCS’05: Proceedings of the 12th ACM Conference on Computer and Communications Security*, pp. 213-222, 2005.

Juan Manuel García G., Carol A. Martínez R. *Departamento de Sistemas y Computación Instituto Tecnológico de Morelia, Morelia, México.*