Sistema de Detección de Atacantes Emascarados Basado en Técnicas de Alineamiento de Secuencias

Jorge Maestre Vidal, Luis Javier García Villalba

Grupo de Análisis, Seguridad y Sistemas (GASS), Departamento de Ingeniería del Software e Inteligencia Artificial
Facultad de Informática, Despacho 431, Universidad Complutense de Madrid (UCM)
Calle Profesor José García Santesmases, 9, Ciudad Universitaria, 28040 Madrid
Email: jmaestre@ucm.es, javiergv@fdi.ucm.es

***Resumen*—Los ataques enmascarados constituyen la actividad malintencionada perpetrada a partir de robos de identidad, entre la que se incluye la escalada de privilegios o el acceso no autorizados a activos del sistema. Este trabajo propone un sistema de detección de atacantes enmascarados mediante la observación de las secuencias de acciones llevadas a cabo por los usuarios legítimos del sistema. La clasificación de la actividad monitorizada es modelada y clasificada en base a algoritmos de alineamiento de secuencias locales. Para la validación del etiquetado se incorpora la prueba estadística no paramétrica de Mann-Whitney. Esto permite el análisis de secuencias en tiempo real. La experimentación realizada considera los conjuntos de muestras de Schonlau. La tasa de acierto al detectar ataques enmascarados es 98,3 % y la tasa de falsos positivos es 0,77 %.**

Palabras clave*—Atacantes enmascarados, ataques internos, detección de intrusiones, seguridad de la información. *(Masquerader attacks, insider attacks, intrusion detection, information security)

I. Introducción

La mayor parte de los accesos no autorizados a un sistema de la información se producen desde el interior, lo que comúnmente se conoce como *ataques internos*. Este tipo de ataques no necesitan explotar vulnerabilidades para atravesar los diferentes controles de acceso ya que de alguna manera, los atacantes satisfacen los requisitos para acceder haciéndose pasar por usuarios legítimos. Los atacantes internos se clasifican en: *traidores* y *enmascarados* [1]. Los *traidores* son usuarios legítimos que ganan privilegios para acceder a información restringida. Los *enmascarados* son atacantes con acceso no autorizado al sistema que suplantan la identidad de usuarios autorizados. Las propuestas para la identificación de atacantes internos varían en función de su clasificación. Dado que los *traidores* son usuarios legítimos, habitualmente conocen las características y la organización del sistema protegido. En consecuencia su detección se centra en la elaboración de trampas y señuelos [2]. Sin embargo la detección de *enmascarados* se centra en la identificación de comportamientos anómalos respecto a los perfiles del uso habitual del sistema. Para ello se tienen en consideración eventos que se producen a nivel local, como los comandos ejecutados, llamadas al sistema, movimientos entre directorios o accesos a ficheros.

El sistema propuesto en este trabajo detecta atacantes enmascarados mediante el análisis de las acciones llevadas a cabo por los usuarios del sistema. Para ello se aplican algoritmos de alineamiento de secuencias, lo que permite modelar su comportamiento e identificar actividades asociadas a su modo de uso indebido. A diferencia de las propuestas anteriores, se introduce el uso de técnicas de alineamiento locales y la prueba de Mann-Whitney para la verificación de sus clasificaciones. Esto permite el análisis en tiempo real de la actividad del usuario sin disminuir la precisión de los procesos de detección. Además cada vez que el usuario ejecuta nuevas acciones su actividad vuelve a ser evaluada. El sistema permite gestionar la emisión de alertas en situaciones dudosas, produciendo una mejora adicional en la etapa de etiquetado.

Este trabajo está estructurado en 7 secciones, siendo la primera de ellas la presente introducción. En la sección II se describen los trabajos previos relacionados con la detección de atacantes enmascarados. En la sección III se explican las principales técnicas de alineamiento de secuencias y sus principales características. En la sección IV se detalla la arquitectura y las características del sistema propuesto. En la sección V se introduce la técnica de validación de etiquetado que complementa al sistema de detección. En la sección VI se describe la experimentación realizada y los resultados obtenidos. Por último, en la sección VII se presentan las conclusiones y las propuestas de trabajo futuro.

II. Trabajos Relacionados

La detección de atacantes enmascarados tiene sus orígenes en propuestas que tienen como objetivo la identificación de comandos poco utilizados por los usuarios legítimos. En [3] se introduce la separación de los comandos ejecutados en usuales e inusuales. La etapa de análisis es llevada a cabo mediante cadenas de Markov: a mayor concentración de comandos inusuales, mayor es la probabilidad de que se trate de un atacante enmascarado. En [4] se propone el estudio de cadenas de acciones mediante el uso de una ventana deslizante de tamaño fijo y la incorporación de un alfabeto de secuencias. Cuando el contenido de la ventana analizada no encaja con ninguna palabra del alfabeto, se gestiona como una cadena extraña, incrementando la posibilidad de que sea etiquetada como una intrusión.

Es importante destacar la aportación de Scholau et al. [5] [6]. [5] presenta la estrategia *Uniqueness*, basada en el análisis de la aparición de comandos que no figuran en los conjuntos de

ISBN: 978-84-9717-323-0

muestras de referencia. Asimismo, proponen la aplicación de métodos de compresión y la identificación de la naturaleza de las secuencias mediante el análisis de su comportamiento. [6] estudia la precisión de diferentes técnicas de detección, destacando entre ellas *Uniqueness*, factores bayesianos, Markov, compresión o encaje de secuencias. Para llevar a cabo su evaluación aplica por primera vez el *dataset* conocido como SEA. Este conjunto de muestras es aplicado posteriormente por otros autores en la evaluación de propuestas similares. No obstante, tal y como señalaron Maxiom y Townsend, su uso es controvertido [7]. Su crítica se centra en que las capturas de los distintos usuarios están mezcladas, se desconoce la información sobre sus fuentes, se desconocen los períodos de captura y no se da información específica acerca de las tareas que llevaron a cabo los usuarios legítimos durante el proceso de captura. A pesar de ello los conjuntos de muestras de Schonlau son considerados un estándar funcional para la validación de este tipo de sistemas.

Algunos trabajos han propuesto alternativas al estudio de las secuencias de comandos o llamadas al sistema. En [8] la elaboración de los perfiles de usuario considera la frecuencia entre *clics* y otras características de los movimientos del ratón. Asimismo algunas propuestas se centran en el estudio de la actividad de ususarios en redes. Este es el caso de [9], donde sus perfiles se elaboran en base a eventos como búsquedas, descargas, impresiones o movimientos en redes sociales.

[10] es uno de los trabajos de mayor impacto. Su objeto de análisis son los comandos introducidos por los usuarios. Sin embargo, en esta ocasión propone su tratamiento tras un agrupamiento y etiquetado en base a su funcionalidad, como la recopilación de recursos, búsquedas o procesos de comunicaciones. También propone técnicas para la generación de conjuntos de muestras con actividades anómalas. Las muestras de sus experimentos se basan en los resultados de un juego de *captura de bandera* en el que usuarios desconocedores del sistema tratan de localizar un archivo determinado mientras su actividad es monitorizada

En [11] se propone el modelado de eventos del sistema mediante los PHMMs (*Profile Hidden Markov Models*), previamente aplicados en el campo de la bioinformática. Los experimentos realizados arrojan una gran precisión cuando se consideran conjuntos pequeños de muestras para su entrenamiento. En [12] se introduce el concepto de ataque de mimetismo en el contexto de la detección de atacantes enmascarados. Asimismo se demuestra la vulnerabilidad de la mayor parte de las propuestas actuales frente a estrategia de evasión similares y se proponen algoritmos para su mitigación. En [13] se introducen las técnicas de alineamiento de secuencias para el análisis de las acciones llevadas a cabo por los usuarios del sistema. Entre su contenido destaca la discusión sobre la aplicación de las diferentes técnicas de alineamiento, el diseño de técnicas para la actualización en tiempo real de los diccionarios de referencia y la propuesta de diferentes sistemas de puntuación. Los algoritmos implementados implica un alto consumo de recursos computacionales. En consecuencia se proponen heurísticas para reducir su consumo a costa de penalizar la precisión de la etapa de análisis.

III. Alineamiento de Secuencias

El alineamiento de secuencias es una técnica procedente del campo de la bioinformática que tiene como finalidad establecer el grado de similitud entre cadenas de ADN, ARN o diferentes proteínas. Las secuencias alineadas generalmente corresponden a nucleótidos o aminoácidos, y se identifican mediante símbolos de un alfabeto. Cuando el ancestro de un linaje de individuos es común, las diferencias son consideradas mutaciones puntuales (sustituciones). A los huecos se los denomina *indels* (inserciones o eliminaciones). La similitud es estudiada como una medida de conservación entre linajes, que habitualmente conlleva una importancia funcional y estructural de las muestras.

Las diferentes técnicas de alineamiento de secuencias habitualmente son consideradas como una generalización del problema de la detección de la longitud de la sub-secuencia más larga común entre dos cadenas, conocida como LCS (*Longest Common Subsequence*). Para la obtención de la LCS el proceso de alineamiento consiste en la eliminación de símbolos y en añadir huecos (*gaps*) hasta que aparezcan sub-secuencias similares, determinándose las de mayor dimensión. Las estrategias de alineamiento de secuencias se clasifican en función de su objeto de análisis. Cuando las secuencias son alineadas considerando su extensión total reciben el nombre de alineamiento global. Si lo hace considerando sus diferentes sub-secuencias reciben el nombre de alineamiento local. Finalmente, cuando se combinan de tal manera que se considera la similitud de una secuencia completa respecto a sub-secuencias de otra secuencia diferente, reciben el nombre de alineamiento semi-global.

IV. Sistema de Detección de Atacantes Enmascarados

El sistema de detección propuesto construye secuencias de acciones llevadas a cabo por los usuarios del sistema a nivel de eventos, y aplica el algoritmo de Smith-Waterman [14] para su alineamiento local. El análisis de sub-secuencias permite la identificación de aquellas situaciones en las que las acciones efectuadas por el atacante se mezclan con las del usuario legítimo: por ejemplo, cuando el usuario con acceso autorizado abandona su puesto de trabajo sin cerrar sesión. En este caso el atacante puede aprovechar su ausencia para efectuar actividades maliciosas, retirándose antes de ser detectado.

En la Figura 1 se muestra su arquitectura. El proceso de detección se lleva a cabo de la siguiente manera: una vez comenzada la monitorización de las acciones realizadas por un usuario, cada vez que se ejecuta una nueva acción es incluida en la cadena *Test*. El proceso de análisis consiste en alinear *Test* con cada una de las secuencias de la colección $Legit = l_1, l_2, .., l_m$, las cuales contienen acciones realizadas habitualmente por usuarios legítimos del sistema. Para contrastar los resultados, *Test* también es alineada con las secuencias de la colección $Intrusions = I_1, I_2, .., I_p$, las cuales contienen actividades anómalas perpetradas por

usuarios no familiarizados con el sistema. Una vez establecidas las puntuaciones se aplica la prueba de validación. Cuando el nivel de parecido de *Test* con alguna de las colecciones es lo suficientemente representativo, es etiquetada acorde a las características de sus secuencias El sistema propuesto repite este proceso por cada nueva acción monitorizada, y solo se detiene si la prueba de validación es superada. De lo contrario, se sobrentiende que no se dispone de suficiente información para decidir la naturaleza del usuario, y se espera a que se ejecuten nuevas acciones.

El sistema de puntuaciones para el algoritmo de alineamiento de secuencias añade $+3$ a la puntuación final en los casos en que el valor de una posición de *Test* conincide con el de su posición análoga en alguna secuencia de las colecciones de referencia. Sin embargo, en caso de incoherencia no se producen modificaciones. La penalización por *gap* en las secuencias de las colecciones es de -2 mientras que en la cadena Test es de -3. A pesar de ello, la puntuación mínima emitible (menor nivel de similitud) es 0.

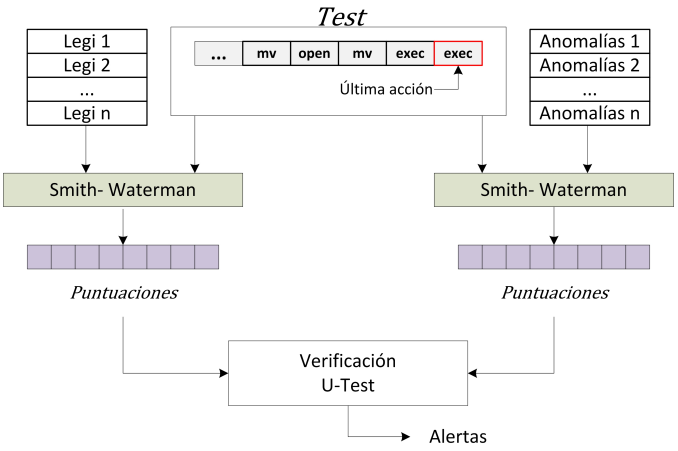

Figura 1. Arquitectura del sistema de detección

V. Validación del Etiquetado

La validación del etiquetado se realiza mediante la prueba de Mann-Whitney, conocida como U-test. Se trata de una extensión del T-test de Student no paramétrica adaptada al análisis de dos muestras independientes. Su objetivo es la comprobación de que dos muestras simétricas han sido extraídas a partir de la misma población. Para ello los datos deben de estar medidos en una escala ordinal, lo que implica la necesidad de ordenar las puntuaciones obtenidas. El cálculo del estadístico U, parte de los valores U_1 y U_2, y es definido como $U = min\{U_1, U_2\}$ donde

$$U_1 = n_1 n_2 \frac{n_1(n_1+1)}{2} - R_1 \quad (1)$$

$$U_2 = n_1 n_2 \frac{n_2(n_2+1)}{2} - R_2 \quad (2)$$

Siendo n_1 y n_2 las longitudes de los vectores de las puntuaciones ordenadas y R_1 y R_2 las sumas de los rangos de las observaciones de las muestras. Dado que el número de muestras es grande, U tiende a parecerse a la distribución normal, de manera que

$$z = \frac{U - M_u}{\sigma_u} \quad (3)$$

Donde m_u y σ_u son la media y la desviación estándar de U, formuladas de la siguiente manera

$$m_u = \frac{n_1 n_2}{2} \quad (4)$$

$$\sigma_u = \frac{n_1 n_2 (n_1 + n_2 + 1)}{12} \quad (5)$$

Una vez obtenida la probabilidad de pertenencia, se comprueba que la cota de porcentaje de error sea admisible. En ese caso puede confirmarse que la diferencia entre las puntuaciones de *Test* con las colecciones de secuencias es considerable. El siguiente paso es decidir con cuál de ellas presenta un mayor parecido. Para ello se considera la media de las puntuaciones obtenidas con cada grupo. La secuencia de puntuaciones cuyo promedio es más bajo corresponde con el conjunto de mayor similitud. Cuando *Test* presenta un mayor parecido con la colección de secuencias legítimas, el usuario se etiqueta como legítimo. Si lo hace con la colección de secuencias anómalas es etiquetado como atacante enmascarado. Si no hay una diferencia clara, la prueba concluye de manera indeterminada: no se tiene suficiente información para establecer un etiquetado preciso. En ese caso se añaden nuevas acciones a *Test* y se repite el proceso hasta que la prueba de validación es superada.

VI. Evaluación del Sistema

Para llevar a cabo los experimentos se ha empleado la colección de muestras de Schonlau [6]. Los datasets de Schonlau están compuestos por capturas de las actividades realizadas por 50 usuarios distintos operando sobre entorno Unix en el año 1998. A pesar de su antigüedad son consideradas un estándar funcional para la evaluación de sistemas de detección de ataques enmascarados. Están organizados de manera que a cada usuario le corresponde un fichero que contiene una serie de 15,000 acciones llevadas a cabo durante el periodo de captura. Los primeros 5,000 comandos corresponden a actividades legítimas, por lo que han sido utilizadas en la elaboración de la colección de secuencias de actividades legítimas. Los siguientes 10,000 comandos pueden tratarse tanto ataques de enmascaramiento, como de actividades legítimas. Se ha extraído parte de los ataques enmascarados para la elaboración de la colección de actividades anómalas.

La evaluación del sistema de detección consiste en un proceso de validación cruzada que involucra los distintos usuarios y los ataques enmascarados presentes en las colecciones de Schonlau. La Tabla I muestra la tasas de falsos positivos o TPR (*True Positive Ratio*) y la tasa de falsos positivos o FPR (*False Positive Ratio*) obtenidos al determinar diferentes longitudes en las secuencias que componen la colección de actividades legítimas de referencia.

Tabla I
TPR/FPR EN FUNCIÓN DE LA LONGITUD DE SECUENCIA

Prec.\Long.	10	20	30	40	100	200	400	600	800
TPR	0.96	0.97	0.96	0.960	0.97	0.983	0.974	0.9701	0.9712
FPR	0.02	0.02	0.02	0.01	0.01	0.0077	0.0172	0.0232	0.0276

El mejor resultado se obtiene con secuencias de longitud 200, siendo $TPR = 98{,}3\,\%$ y F$PR = 0{,}77\,\%$ Sin embargo el peor resultado se obtiene cuando la longitud es 10, con $TPR = 96{,}9\,\%$ y $FPR = 2{,}68\,\%$. Los cambios más representativos se encuentran en las variaciones de FPR. La curva que describe estos cambios muestra un punto de inflexión al considerarse longitud 200, siendo este su valor mínimo.
El análisis por separado del comportamiento de los usuarios del sistema con secuencias de longitud 200 indica que existen usuarios más propensos a ser suplantados con éxito que otros.

En la Figura 2 se muestra la representación en el espacio ROC (*Receiver Operating Characteristic*) de la precisión obtenida en cada uno de ellos. El eje Y del espacio ROC lo constituyen los valores FPR de los experimentos, mientras que el eje X contiene el valor de los FPR. Esto habitualmente es interpretado como el intercambio entre los beneficios obtenidos (TPR) por el sistema, y los costes que conlleva (FPR). La ubicación óptima en el espacio ROC es la esquina superior izquierda con $TPR = 1, FPR = 0$. A este punto se le llama *clasificación perfecta*, y su proximidad determina la calidad de la precisión del sistema.
El valor TPR ha oscilado en el intervalo aproximado del $98 \pm 2\,\%$. El FPR ha variado en el intervalo aproximado $5 \pm 5\,\%$, lo que indica una desviación algo más representativa. La clasificación perfecta ha sido alcanzada por 22 de los 50 usuarios que han participado en la prueba.
A la vista de los resultados arrojados en los experimentos queda demostrada la gran capacidad del sistema propuesto de identificar atacantes enmascarados.

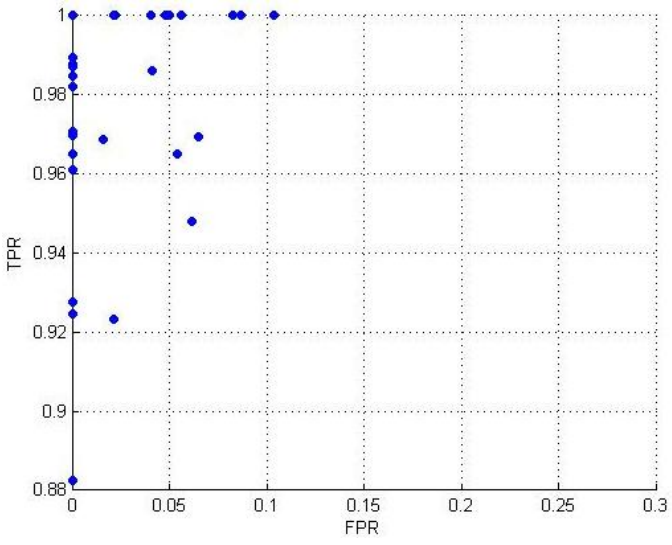

Figura 2. TPR/FPR de cada usuario en el espacio ROC

VII. CONCLUSIONES

Se ha propuesto un sistema para el análisis de la actividad realizada por los usuarios del sistema en tiempo real e identificar atacantes enmascarados. En su evaluación a partir de los conjuntos de muestras de Schonlau ha alcanzado valores promedios de $TPR = 98{,}3\,\%$ y $FPR = 0{,}77\,\%$, lo que demuestra un alto grado de precisión. Sin embargo los experimentos indican que el sistema es sensible a cambios en la longitud de las secuencias que componen las colecciones de actividades legítimas y anómalas. Asimismo se ha comprobado cómo la capacidad de acierto en el etiquetado es mejor en algunos usuarios que en otros. Como trabajo futuro se propone la aplicación de técnicas para homogeneizar la calidad de los conjuntos de entrenamiento y fortalecer el sistema frente a ataques de evasión.

REFERENCIAS

[1] M. B. Salem, S. Hershkop, S. J. Stolfo, "A Survey of Insider Attack Detection Research," *Insider Attack and Cyber Security. Advances in Information Security*, Vol. 39, pp. 69-90, 2008.
[2] M. B. Salem, S. J. Stolfo, "Decoy document deployment for effective masquerade attack detection," *Proceedings of the 8th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA)*, Amsterdam, The Netherlands. Lecture Notes in Computer Science, Vol. 6739 pp. 35-54, July 2011.
[3] H. W. Ju, Y. Vardi, "A hybrid high-order Markov chain model for computer intrusion detection," *Journal of Computational and Graphical Statistics*, Amsterdam, The Netherlands. Lecture Notes in Computer Science Vol. 10(2), pp. 277-295, 2001.
[4] K. Tan, A. Roy, "Why 6?: Defining the operational limits of stide, an anomaly-based intrusion detector," *Proceedings of the IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, pp. 188-201, May 2002.
[5] M. Schonlau, M. Theus, "Detecting masquerades in intrusion detection based on unpopular commands," *Information Processing Letters*, Vol. 76, pp. 33-38, November 2000.
[6] M. Schonlau, W. DuMouchel, W. H. Ju, A. F. Karr, M. Theus, Y. Vardi, "Computer intrusion: Detecting masquerades," *Statistical Science*, Vol. 16, No.1, pp. 58-74, February 2001.
[7] R. A. Maxion, T. N. Townsend, "Masquerade detection using truncated command lines," *Proceedings of the IEEE International Conference on Dependable Systems and Networks (DSN)*, Bethesda, MD, USA, pp. 219-228, June 2002.
[8] A. Garg, R. Rahalkar, S. Upadhyaya, K. Kwiat, "Profiling users in GUI based systems for masquerade detection," *Proceedings of the IEEE Information Assurance Workshop (IAW)*, West Point, NY, USA, pp. 48-54, June 2006.
[9] M. A. Maloof, G. D. Stephens, "Elicit: A system for detecting insiders who violate need-to-know," *Proceedings of the 10th International Symposium on Recent Advances in Intrusion Detection (RAID)*, Gold Goast, Australia. Lecture Notes in Computer Science, Vol. 4637, pp. 146-166, September 2007.
[10] M. B. Salem, S. J. Stolfo, "Modeling User Search Behavior for Masquerade Detection," *Proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection (RAID)*, Menlo Park, CA, USA. Lecture Notes in Computer Science, Vol. 6961, pp. 181-200, September 2011.
[11] L. Huang, M. Stamp, "Masquerade detection using profile hidden Markov models," *Computers & Security*, Vol. 30 (8), pp. 732-747, November 2011.
[12] J. E. Tapiador, J. A. Clark, "Masquerade mimicry attack detection: A randomised approach," *Computers & Security*, Vol. 30 (5), pp. 297-310, May 2011.
[13] S. Coull, B. Szymanski, "Sequence alignment for masquerade detection," *Computational Statistics & Data Analysis*, Vol. 52 (8), pp. 4116-4131, April 2008.
[14] T. F. Smith, M. S. Waterman, "Identification of common molecular subsequences," *Journal of Molecular Biology*, Vol. 147 (1), pp. 195-197, 1981.