WUIL: Una base de datos para probar mecanismos de detección de intrusos

J. Benito Camiña y Raúl Monroy

Departamento de Ciencias Computacionales,
Campus Estado de México del Tecnológico de Monterrey,
Atizapán, Estado de México, México
{a00965049,raulm}@itesm.mx

Resumen En el mundo actual, donde la información tiene un valor enorme, se ha vuelto una parte vital la detección de intrusos durante una sesión en la computadora. El estudio de la detección de intrusos tomó fuerza a partir del trabajo de Schonlau *et al.* [1]. en el cual presentan una base de datos para comparar diversos métodos de detección de intrusos con base en comandos en UNIX. Sin embargo, la base de datos y el método en sí de detectar intrusos con base en comandos no fue lo suficientemente útil. Por tal motivo se empezaron a realizar nuevas bases de datos basándose en otras fuentes de comportamiento del usuario, pero aún no se han encontrado los resultados esperados. En este artículo se presenta una base de datos que pretende cubrir algunas de las deficiencias de bases de datos pasadas y que se base en el comportamiento del usuario en su interacción con el sistema de archivos de su computadora. Además se presentan métodos de cómo utilizaremos la base de datos para detectar intrusos.

Palabras clave: base de datos, detección de intrusos, seguridad computacional.

1. Introducción

Debido a la cantidad de información sensible que se guarda en las computadoras, el problema de detectar intrusos de forma rápida se ha vuelto algo primordial en los últimos años. Esto con el fin de evitar que las personas tengan pérdidas incalculables.

La detección de intrusos es regularmente abordada como una tarea de detección de anomalías, donde se crea el perfil del usuario con base en su comportamiento y si el nuevo comportamiento se desvía del comportamiento normal, se detecta como un intruso. Esto se comenzó a estudiar principalmente a partir del trabajo de Schonlau *et al.* [1] donde perfila a los usuarios con base en los comandos que utiliza durante una sesión en UNIX. Shonlau *et al.*s' crearon una base de datos, llamada SEA, la cual se utilizó durante mucho tiempo como el estándar para desarrollar y comparar mecanismos de detección de intrusiones.

Lamentablemente SEA presenta limitaciones. La más importante es que no cuenta con ataques reales, en lugar de eso utiliza el método de Uno-Contra-Los-Otros (OVTO, por sus siglas en inglés). Utilizando este método, una sesión de un usuario se compara contra alguna de otro usuario y se busca detectar diferencias en su comportamiento, sin que en realidad haya un ataque. Además, se ha probado que el uso de comandos para distinguir a un usuario de un atacante no es lo suficientemente poderoso [2].

Como resultado las investigaciones se han centrado a otros tipos de fuente de actividades del usuario, como el uso de dispositivos, principalmente el teclado [3,4]. Con esto se han creado nuevas bases de datos, sin embargo, siguen con el problema de utilizar el método OVTO.

Por lo tanto se decidió crear la base de datos: Bitácoras de Usuarios e Intrusos simulados para Windows (WUIL, por sus siglas en inglés). Los registros de WUIL contienen información del qué y el cómo accede los archivos un usuario. Con esto es posible crear un perfil del usuario y determinar si un comportamiento nuevo pertenece o no al usuario.

En este trabajo se maneja la hipótesis de que hay ciertos rasgos en la forma en que un usuario interactúa con el sistema de archivos, con los cuales se puede diferenciar de un intruso. Además, se muestran varias formas de validar esta hipótesis utilizando los siguientes conceptos: localidad, tareas, número de accesos y de accesos nuevos.

La base de datos WUIL está disponible en:

`http://homepage.cem.itesm.mx/raulm/wuil-ds/`

La organización del documento es la siguiente, primero en la sección 2 se muestra el trabajo relacionado, donde se habla de SEA y otras bases de datos que se han realizado. En la sección 3 se presenta la base de datos WUIL y se explica cómo se realizó esta base de datos. Luego en la sección 4, se muestra el trabajo en proceso que tenemos y cómo vamos a detectar intrusos utilizando la base de datos. Finalmente, en la sección 5 se presentan las conclusiones y el trabajo futuro.

2. Trabajo relacionado

En los últimos años las investigaciones en el área de detección de intrusiones ha sido abundante. Los trabajos realizados se han basado en el análisis de diferentes fuentes de actividad del usuario. Sin embargo, los trabajos realizados no han brindado resultados concluyentes y se continúan realizando investigaciones en el área.

2.1. La Base de datos SEA

A partir del trabajo realizado por Schonlau *et al.* [1] en el cual presentan a SEA [5] el interés en el área de detección de intrusiones ha ido en aumento. SEA es una base de datos que permite probar distintos mecanismos de detección de

intrusiones. La base de datos contiene bitácoras de la actividad de 70 usuarios en el sistema operativo UNIX, cada una de las bitácoras de los usuarios consiste de 15,000 comandos sin argumentos.

El mayor problema que tiene SEA es que utilizan el concepto de OVTO en el cual no se tienen ataques realizados en las máquinas de los usuarios, si no que utiliza bitácoras de ciertos usuarios como usuarios legítimos y bitácoras de otros usuarios como bitácoras contaminadas. Para lograr esto primero seleccionaron 50 usuarios como usuarios legítimos y los otros 20 los consideran, de forma artificial, como intrusos. Después, dividen las bitácoras de los usuarios en bloques de 100 comandos, cada bloque recibe el nombre de sesión, con lo cual quedan 150 sesiones por usuario. Las primeras 50 sesiones no se modifican y se utilizan para construir el perfil del usuario, las otras 100 sesiones se utilizan para la validación de la base de datos y pueden o no estar contaminadas.

Cada sesión de validación puede estar o no totalmente contaminada, si está contaminada se dice que hay un intento de intrusión. Para crear una sesión contaminada lo que realizan es el reemplazo de una sesión de validación por una de un usuario seleccionado como intruso de manera arbitraria. Ellos brindan una matriz donde indican por cada usuario cuáles son las sesiones que están contaminadas.

Como se puede ver SEA brinda la posibilidad de comparar distintos métodos de detección de intrusos, sin embargo la información que brindan es artificial al no haber ataques reales. Además, de que el únicamente considerar los comandos para detectar intrusos, es insuficiente [2]. Por tal motivo los trabajos en el área de detección de intrusiones han buscado nuevas fuentes de actividad para detectar intrusos como son el uso del algún dispositivo, como el teclado [3,4] o el comportamiento abstracto del usuario [6].

2.2. Otras bases de datos

Una de las fuentes de actividad alternativa que más se ha estudiado es el análisis de los patrones de tecleo [7,8,9,10,11,12,13]. En la mayoría de estos trabajos se utiliza el tecleo de una contraseña, la cual es repetida cierto número de veces. Es muy difícil comparar estos trabajos, ya que cada uno utiliza su propia base de datos y varían aspectos entre ellas como son la información que guarda cada uno o el número de veces que repiten la contraseña.

Uno de los trabajos más relevantes en cuanto al análisis de los patrones de tecleo es el de Maxion y Killourhy [4]. En este trabajo utilizan 51 usuarios para recolectar 400 registros por cada uno de ellos, en varias sesiones de 50 registros en diferentes días. Ellos recolectan información que va desde el tiempo en el que presionan las teclas, hasta el género o si el usuario es zurdo o diestro para tener una base de datos completa.

Aunque guardan información muy completa de los usuarios, su propuesta presenta dos problemas principales. Primero, porque utilizan de nuevo el enfoque OVTO, ya que todos los usuarios escriben la misma contraseña y lo que buscan es diferenciar como escribe un usuario la contraseña contra los demás, aunque es razonable porque el trabajo es sobre el conocimiento y forma de capturar

una contraseña y si fueran diferentes sería complejo poder realizar el estudio. Segundo el tener que escribir 50 veces seguidas por sesión la misma contraseña, es poco realista.

Por otro lado, hay trabajos que consideran combinaciones de distintas fuentes de actividad como es el caso de [6] en el cual utilizan 22 tipos de actividades del usuario, incluyendo qué archivos del sistema se utilizan, comunicaciones, búsquedas, etc. La base de datos se utiliza para modelar el comportamiento a la hora de realizar búsquedas principalmente. Cuentan con 18 usuarios y con intrusiones simuladas de 40 diferentes individuos, durante un período de cuatro días y tienen más de 500,000 registros por usuario en promedio. El problema es que son muy pocos días de recolección de información y aun así el tamaño del conjunto de datos es de diez Gbytes.

En ese trabajo se les ordenó a los intrusos actuar siguiendo uno de tres distintos escenarios: *malicioso*: el objetivo era encontrar información financiera de un compañero de trabajo en un período de 15 minutos; *benigno*: similar al primero pero el intruso utiliza la computadora del compañero para propósitos buenos, asumiendo que no tiene acceso a su computadora por alguna razón; *neutral*: los intrusos tenían la libertad de ver lo que quisieran en la computadora del compañero de trabajo. Un problema es que todo lo que manejan depende del Sistema Operativo utilizado.

Un trabajo muy similar al que se presenta en este documento fue realizado con anterioridad [14] y los resultados fueron alentadores. En ese trabajo también se analizaba la interacción del usuario con el sistema de archivos. Sin embargo, sólo se utilizaban tres usuarios y son muy pocos para dar resultados concluyentes.

2.3. Desventajas de las bases de datos actuales

En este punto pretendemos mostrar a manera de resumen los tres problemas primordiales que creemos que existen en las bases de datos actuales:

1. Varían en cuanto el número de usuarios, tiempo de captura y plataforma utilizada.
2. Varía el tipo de información que se recolecta de un trabajo a otro aunque utilicen la misma fuente de actividad del usuario.
3. No cuentan con verdaderos ataques realizados en las computadoras de los usuarios.
4. Algunas bases de datos no son públicas y no las pueden utilizar otros investigadores para experimentar con ellas.

Como se puede ver las bases de datos existentes tienen muchas deficiencias, principalmente en el hecho de que los ataques que tienen no son fieles a la realidad. Por ese motivo se buscó la creación de una base de datos que contenga ataques simulados pero que se acerquen mucho a ser reales, así como brindamos la posibilidad de compartir la base de datos para que otros investigadores puedan utilizarla y con ello poder comparar resultados entre clasificadores.

Tabla 1. Información básica de los usuarios de WUIL: Su labor, la versión de MS Windows que utiliza y el número de días durante los cuales se recolectó información.

Usuario	Labor	Versión de MS Windows	# de días de la bitácora
1	Administrador	Windows XP	49
2	Administrador	Windows XP	48
3	Área de Sistemas	Windows XP	35
4	Contador	Windows XP	29
5	Secretaria	Windows XP	54
6	Secretaria	Windows XP	55
7	Secretaria	Windows XP	56
8	Secretaria	Windows XP	31
9	Secretaria	Windows XP	34
10	Envíos	Windows Vista	33
11	Secretaria	Windows XP	13
12	Programador	Windows 7	44
13	Estudiante	Windows Vista	40
14	Ventas	Windows 7	34
15	Estudiante de Doctorado	Windows Vista	54
16	Estudiante de Doctorado	Windows 7	37
17	Estudiante	Windows 7	35
18	Estudiante	Windows 7	30
19	Secretaria	Windows Vista	36
20	Estudiante de Doctorado	Windows XP	23

3. La base de datos WUIL

Debido a las deficiencias que hay en las bases de datos actuales así como a que los resultados obtenidos con las fuentes de actividades que manejan no han sido concluyentes, se creó una base de datos nueva para este trabajo. La hipótesis manejada es que el análisis de la interacción del usuario con su sistema de archivos nos brinda la posibilidad de detectar intrusos. La base de datos contiene información tanto de usuarios legítimos como de tres ataques realizados en cada una de las computadoras de los usuarios legítimos.

Para validar la hipótesis se crearon bitácoras, en las cuales se guarda información de los archivos que se están accediendo. Después de procesar las bitácoras, se puede obtener información que indique qué objetos del sistema operativo está accediendo el usuario, así como la forma en que lo hace (por ejemplo, dependencias entre objetos, frecuencia de uso, etc).

3.1. Bitácoras de usuarios

Al momento de la escritura de este documento WUIL cuenta con 20 usuarios con períodos de recolección que van desde cinco hasta diez semanas, la información general de los usuarios se puede ver en la tabla 1. Este número de usuarios se espera que vaya incrementando de forma continua para enriquecer la base de datos.

Para la recolección de los datos se utilizó la herramienta Audit de Windows, la cual registra los objetos utilizados por el usuario durante su sesión. Aunque se realizó en Windows la idea general se puede realizar en cualquier Sistema Operativo. Al ser demasiadas carpetas las que hay en el Sistema Operativo completo, nos enfocamos en un par de carpetas: `Escritorio` y `Mis Documentos`.

Tabla 2. Número de accesos por cada usuario antes y después de filtrar.

Usuario	Número de accesos original	Número de accesos después de filtrar
1	293,894	272,642
2	77,608	63,536
3	40,708	15,159
4	147,418	129,847
5	350,800	338,788
6	369,440	356,194
7	352,910	335,081
8	91,852	85,482
9	178,602	178,460
10	127,532	108,643
11	547,545	545,715
12	2,692,858	197,639
13	2,307,804	2,307,253
14	1,752,639	19,812
15	454,280	453,204
16	1,444,914	1,290,295
17	245,862	213,147
18	10,409	10,315
19	90,357	54,302
20	76,943	57,608

Estas carpetas fueron seleccionadas a través de encuestas realizadas a estudiantes universitarios preguntándoles dónde buscarían información relevante de una persona si tuvieran acceso a su computadora durante 5 minutos.

Una ventaja de WUIL es que los datos fueron registrados durante el uso normal del Sistema Operativo por el usuario, y no de forma artificial como en otras bases de datos. Sin embargo, uno de los problemas al momento de guardar los registros es que guarda información que no es necesaria, como registros que no estaban contenidos en `Escritorio` o en `Mis Documentos`, por lo cual se tuvo que hacer un pre-procesamiento y se tuvo que filtrar esta información, en la tabla 2 se pueden ver los números de acceso por usuario antes y después del filtrado. Probablemente el usuario número 13 haya que dividirlo en varios usuarios debido a la cantidad de accesos que tiene aún después del filtrado, ya que en análisis previos encontramos que puede ser complicado procesar bitácoras de esas dimensiones.

3.2. Ataques y su simulación

Se simularon tres diferentes tipos de ataques que buscan abarcar ataques desde ataques que fueron hechos sin premeditación hasta ataques que fueron planeados con anticipación. Los ataques fueron simulados lo más fieles a la realidad posible, para esto se hicieron encuestas a estudiantes dónde debían indicar que pasos seguirían para realizar un ataque en una computadora la cual esta desatendida durante cinco minutos y desean obtener información sensible del usuario al que pertenece. A partir de los resultados de la encuesta se pudieron determinar los tres tipos de ataque: básico, intermedio y avanzado.

Ataque básico El ataque básico es un ataque que modela el caso de un intruso ocasional, lo que significa que trata de aprovechar una oportunidad que se le

presenta en lugar de crear él la oportunidad. En este caso se asume que el intruso no tiene consigo una memoria USB ni la posibilidad de copiar la información en ningún medio electrónico. Por lo tanto, el intruso únicamente puede abrir y cerrar archivos y si quiere extraer información únicamente puede ser utilizando su propia memoria o copiandola en papel.

Ataque intermedio En el ataque intermedio, el intruso trae una memoria USB consigo. Por lo tanto, el intruso buscará archivos que le parezcan interesantes (por ejemplo, cuenta, contraseña, o extensiones como *.doc) utilizando la herramienta de búsqueda de Windows y los copiará en su memoria USB para posteriormente revisarla y ver si hay información que le sirva.

Ataque avanzado En este caso, el intruso no sólo trae la USB si no que trae un archivo .bat que con solo ejecutarlo se encargará de realizar la búsqueda de archivos interesantes y copiarlos en la USB sin la necesidad de que el busque manualmente. Con esto el atacante se ahorra tiempo y puede robar más información.

Todos los ataques se realizaron directamente en la computadora de cada uno de los usuarios y los tres ataques dentro de una computadora fueron realizados por la misma persona. Los archivos extraídos nunca fueron revisados y se borraron después de acabar el ataque. En la tabla 3 se puede ver el número de registros por cada uno de los ataques realizados.

Finalmente, podemos decir que WUIL es una base de datos que supera algunas de las deficiencias de otras bases de datos: WUIL contiene ataques simulados muy parecidos a ataques reales y al ser una base de datos pública muchos investigadores podrán utilizarla y los resultados entre experimentos pueden ser comparables. Sin embargo, no supera algunas deficiencias, por ejemplo, la de tener tiempos de captura distintos.

4. Trabajo en proceso

Actualmente se está en el proceso de experimentar utilizando la base de datos. Para esto se considera que hay ciertos rasgos en la forma en la que interactúa el usuario con su computadora que pueden ayudar a diferenciar su comportamiento del de un atacante. A continuación explicaremos los rasgos que se busca probar que sirven para detectar intrusos.

4.1. Localidad

Hay un par de términos sobre localidad a la hora de hablar de Sistemas Operativos, en especial al hablar de las lecturas en memoria. El primer concepto es la localidad temporal, la cual argumenta que si una localidad de memoria es referenciada probablemente sea referenciada nuevamente en un período de tiempo corto. El segundo concepto es la localidad espacial y argumenta que si

Tabla 3. Bitácoras de los atacantes: número de accesos de los antacantes antes del filtrado y después del iltrado.

Usuario	Ataque 1		Ataque 2		Ataque 3	
	Accesos Totales	Accesos Filtrados	Accesos Totales	Accesos Filtrados	Accesos Totales	Accesos Filtrados
1	2,476	2,353	4,851	4,352	14,825	14,825
2	2,049	2,032	4,203	3,968	1,423	1,273
3	2,240	2,155	1,112	1,069	1,904	1,836
4	3,702	3,646	7,603	7,422	1,1369	1,1235
5	3,085	3,001	15,507	14,925	10,378	10,378
6	3,594	3,499	8,902	8,530	7,466	7,466
7	3,184	3,090	18,916	18,625	11,464	11,464
8	5,331	5,267	8,265	7,898	10,404	10,404
9	3,546	3,546	10,761	10,711	9,519	9,519
10	1,038	730	973	499	148	13
11	6033	6033	25162	25162	842	842
12	1,966	1,953	3,411	3,411	16,269	16,265
13	259	254	16098	16096	1004	1004
14	13,404	1,084	4,403	1,315	4,537	1,726
15	1,284	1,284	6,100	6,100	4,171	4,171
16	2,893	2,893	919	919	2,075	2,075
17	1,585	1,585	2,289	2,289	3,342	3,342
18	1,770	1,770	498	498	1,495	1,495
19	1,003	588	1,215	392	225	139
20	3,455	3,443	52,819	52,804	10,361	10,361

una localidad de memoria es referenciada es muy probable que otras localidades de memoria cercanas a ésta sean referenciadas en un período de tiempo corto.

Se cree que al utilizar estos conceptos, pero llevándolo a archivos y no a localidades de memoria nos puede ayudar a detectar intrusos. Se considera que en general los usuarios si se encuentran realizando un trabajo en especial, accederán archivos que se encuentran en una misma carpeta y probablemente lo hagan de forma repetida. Por otro lado se piensa que un intruso saltará entre carpetas y archivos para buscar información interesante y sin repetir archivos.

Para lograr esto es importante encontrar un valor que diga que tan cercano es un archivo de otro. Además, se debe decidir sobre una unidad de tiempo que permita ver si un archivo se está accediendo de nueva cuenta en un período de tiempo corto o no.

4.2. Tareas

Normalmente cada archivo en una computadora pertenece a una tarea de un usuario (por ejemplo, un estudiante tendrá tareas como trabajo, escuela, videojuegos, películas, pasatiempo, etc.). Se piensa que si se etiqueta cada uno de los archivos con la tarea a la que pertenecen y se analizan los cambios entre estas tareas se podran identificar patrones que ayuden a crear un perfil del usuario y con ello detectar intrusos.

El reto que es que no es posible pedirle a cada uno de los usuarios que digan cada uno de sus archivos a que tarea pertenece, por lo tanto se debe buscar algún método para etiquetar las tareas de forma automatizada. En un principio se cree que archivos contenidos dentro de una carpeta pertenecen a la misma tarea.

Después se debe crear un perfil donde se guarde la información relacionada con los cambios entre cada una de las tareas. Con esto se puede revisar nuevas transiciones entre tareas e identificar si se trata de un intruso o del usuario legítimo.

4.3. Número de accesos y número de accesos nuevos

Observando el comportamiento de los usuarios mientras interactúan con su sistema de archivos se ha notado que suelen trabajar con calma y realizando un número reducido de accesos cada cierto tiempo. Los atacantes en cambio, realizan muchos accesos en períodos de tiempo corto, revisando muchos archivos, algunos de los cuales el usuario utiliza muy poco o que en realidad nunca ha utilizado. Un acceso nuevo puede ser realizado tanto porque el archivo se acaba de crear, como porque desde que se tiene el sistema de detección activado nunca se había utilizado.

Por tal motivo, se piensa que si se revisa el número de accesos y de accesos nuevos realizados durante cierto período de tiempo, nos ayudará a detectar intrusos. Para eso hay que utilizar las bitácoras de la base de datos e ir revisando que archivos son los que utiliza el usuario y con qué frecuencia lo hace. Además hay que buscar una forma de marcar como nuevos archivos que no se han utilizado dentro de un período de tiempo largo.

5. Conclusiones y trabajo futuro

Utilizando la base de datos empleando los conceptos antes mostrados se espera obtener resultados satisfactorios en la detección de intrusiones. Además se espera que la base de datos sea utilizada por otros investigadores para poder comparar nuestros resultados con los suyos e identificar así el mejor mecanismo para detectar intrusos.

La base de datos presentada y que se está compartiendo se considera que puede ser de mucha utilidad en el área principalmente por dos motivos: primero, porque pocas veces las bases de datos son compartidas y por ende los resultados entre trabajos no son comparables; segundo, porque la base de datos contiene ataques simulados fieles a la realidad, que es algo que no se ha hecho en otros trabajos del área.

El trabajo futuro se divide en dos partes primordiales. La primera, es que además del trabajo en proceso mostrado en la sección 4 se deben buscar nuevas formas de aprovechar la base de datos. Y la segunda, se debe mantener WUIL actualizada agregando nuevos usuarios tanto de Windows como de otros sistemas operativos.

Agradecimientos Este proyecto fue apoyado parcialmente por CONACyT mediante una beca de doctorado con número de becario 241856, una beca de estancia postdoctoral a nombre de Carlos Herández Gracidas y un proyecto de investigación básica con número 105698.

Referencias

1. Schonlau, M., DuMouchel, W., Ju, W., Karr, A., Theus, M., Vardi, Y.: Computer intrusion: Detecting masquerades. Statistical Science **16**(1) (2001) 58–74
2. Razo-Zapata, I., Mex-Perera, C., Monroy, R.: Masquerade attacks based on user's profile. Journal of Systems and Software **85**(11) (2012) 2640–2651
3. Garg, A., Rahalkar, R., Upadhyaya, S., Kwiat, K.: Profiling users in GUI based systems masquerade detection. In: Proceedings of the 7th IEEE Information Assurance Workshop, IEEE Computer Society Press (2006) 48–54
4. Killourhy, K.S., Maxion, R.A.: Why did my detector do *that*?! - predicting keystroke-dynamics error rates. In Jha, S., Sommer, R., Kreibich, C., eds.: Recent Advances in Intrusion Detection, 13th International Symposium, RAID 2010. Volume 6307 of Lecture Notes in Computer Science., Springer (2010) 256–276
5. Schonlau, M.: Masquerading user data. http://www.schonlau.net (2008)
6. Ben-Salem, M., S., S.: Modeling user search behavior for masquerade detection. Computer Science Technical Reports 033, Columbia University (2010)
7. Joyce, R., Gupta, G.: Identity authentication based on keystroke latencies. Commun. ACM **33**(2) (February 1990) 168–176
8. Bleha, S., Slivinsky, C., Hussien, B.: Computer-access security systems using keystroke dynamics. Pattern Analysis and Machine Intelligence, IEEE Transactions on **12**(12) (dec 1990) 1217 –1222
9. Cho, S., Han, C., Han, D.H., il Kim, H.: Web based keystroke dynamics identity verification using neural network. Journal of Organizational Computing and Electronic Commerce **10** (2000) 295–307
10. Haider, S., Abbas, A., Zaidi, A.: A multi-technique approach for user identification through keystroke dynamics. In: Systems, Man, and Cybernetics, 2000 IEEE International Conference on. Volume 2. (2000) 1336 –1341 vol.2
11. Yu, E., Cho, S.: Ga-svm wrapper approach for feature subset selection in keystroke dynamics identity verification. In: Neural Networks, 2003. Proceedings of the International Joint Conference on. Volume 3. (july 2003) 2253 – 2257 vol.3
12. Araujo, L., Sucupira, L.H.R., J., Lizarraga, M., Ling, L., Yabu-Uti, J.: User authentication through typing biometrics features. Signal Processing, IEEE Transactions on **53**(2) (feb. 2005) 851 – 855
13. Kang, P., Hwang, S.s., Cho, S.: Continual retraining of keystroke dynamics based authenticator. In: Proceedings of the 2007 international conference on Advances in Biometrics. ICB'07, Berlin, Heidelberg, Springer-Verlag (2007) 1203–1211
14. Camiña, B., Monroy, R., Trejo, L., Sánchez, E.: Towards building a masquerade detection method based on user file system navigation. In Batyrshin, I., Sidorov, G., eds.: Proceedings of the Mexican International Conference on Artificial Intelligence, MICAI'11. (2011) 174–186