AVANCES EN ROBUSTECIMIENTO ANTE ATAQUES DE PRESENTACIÓN Y FALSIFICACIÓN PARA SISTEMAS BASADOS EN EL ANÁLISIS DE PATRONES DE TECLEO

Nahuel González [1], Jorge Ierache[1], Waldo Hasperué [2,3], Enrique P. Calot[1], Hernán Merlino[1]

Laboratorio de Sistemas de Información Avanzados, Departamento Computación
Facultad de Ingeniería, Universidad de Buenos Aires[1]

Instituto de Investigación en Informática (III-LIDI),
Facultad de Informática, Universidad Nacional de La Plata[2]
Investigador Asociado - Comisión de Investigaciones Científicas (CIC) [2]

{ngonzalez,jierache,ecalot,hmerlino}@lsia.fi.uba.ar
whasperue@lidi.info.unlp.edu.ar

Resumen

El Laboratorio de Sistemas de Información Avanzados (LSIA) de la Facultad de Ingeniería de la Universidad de Buenos Aires (FIUBA) lleva adelante una línea de investigación sobre dinámica de tecleo, que se enmarca en un Proyecto de desarrollo Estratégico (PDE-44 UBA 2019-2020). Los aportes relevantes que se han publicado en la materia incluyen la formulación del método de modelado por contextos finitos, el análisis de la robustez de la técnica ante variaciones emocionales del usuario, la generación de conjuntos de datos para evaluación, y la transferencia de los resultados teóricos anteriores a la industria. El objeto de investigación actual se centra en los tipos de ataques a los que un usuario malintencionado puede someter a este tipo de sistemas, y la formulación de técnicas de defensa eficaces contra ellos. En particular, se ha demostrado que las implementaciones actuales son vulnerables a los ataques de repetición, de presentación, y a la inyección de falsificaciones sintéticas. Aquí introducimos tanto una nueva modalidad sofisticada de ataque utilizando falsificaciones sintéticas como una defensa eficaz contra el mismo.

Palabras clave: *Seguridad Informática, Ataques de Presentación, Falsificación, Dinámica de tecleo, Contextos finitos.*

Contexto

El Laboratorio de Sistemas de Información Avanzados (LSIA) de la Facultad de Ingeniería de la Universidad de Buenos Aires fue creado en el año 2011 [LSIA, 2020]. Dentro de sus líneas

de investigación se cuenta el estudio de la dinámica de tecleo. Entre sus resultados publicados se cuentan el método de modelado por contextos finitos [González et. al., 2015], la generación de un extenso dataset realista y la replicación con él de experimentos previos destacados [González et. al., 2016], el análisis de la robustez de la técnica ante variaciones emocionales del usuario [Calot et. al., 2019], y la transferencia de los resultados anteriores a la industria, en el marco del Proyecto de desarrollo Estratégico PDE-44-2019, iniciado en el año 2019 [Ierache et. al., 2020]. El antedicho proyecto se basa en los resultados del proyecto UBACYT 20020130200140BA, titulado "Métodos de educción de cadencias de tecleo centrado en el contexto emocional de un individuo aplicando Interfaces Cerebro-Máquina (BMI)".

Los avances aquí presentados tienen como objetivo fortalecer la robustez de los métodos antedichos frente al estado del arte en ataques contra sistemas de autenticación continua basados en cadencias de tecleo.

Introducción

La dinámica de tecleo (*keystroke dynamics*) es un subcampo de la biometría del comportamiento y la interacción hombre-máquina, que estudia cómo se pueden utilizar los ritmos de escritura para descubrir o verificar la identidad de los usuarios, tanto en el momento de iniciar sesión como de forma continua durante el trabajo diario [Joyce & Gupta, 1990]. Multitud de técnicas, desde las más sencillas basadas en distancias hasta los más sofisticados clasificadores, han sido ensayadas para la verificación de identidad con dinámica de tecleo. Una comparación exhaustiva puede encontrarse en [Killourhy & Maxion, 2009]. El análisis de la dinámica de tecleo puede ser utilizado tanto para claves como para textos libres [Gunetti et. al., 2005].

Además de ser utilizada para autenticación, el análisis de dinámica de tecleo ha permitido correlacionar el estado emocional detectado por un clasificador con el reporte subjetivo de los usuarios [Epp et al., 2011], aunque alcanzando menor precisión. Otro trabajo realizado en contextos multimodales aplicando EEGs obtenidos por interfase cerebro-maquina registra el patrón de tecleo, bajo un enfoque dimensional; este fue desarrollados en el LSIA FIUBA en colaboración con el ISIER-UM. [Calot et. al., 2019].

En la última década se ha enfatizado la debilidad de los sistemas de autenticación basados en cadencia de tecleo [Rahman et. al., 2011] incluso ante ataques de gran simplicidad [Stefan et al, 2012] como la repetición exacta de una cadencia observada. Sin embargo, estos ataques presuponen acceso físico o lógico con privilegios elevados (suficientes para inyectar eventos de teclado) en los sistemas objetivo y un conocimiento muy detallado del patrón de escritura del usuario a falsificar. Una forma más

sofisticada de este ataque, pero con menos eficacia general, utiliza estadísticas generales para una población a los fines de suplir la ausencia de información de un usuario específico [Stanciu et. al., 2016].

En este artículo se enuncian los avances en materia de robustecimiento ante ataques de presentación y falsificación para sistemas basados en el análisis de patrones de tecleo. Aquí introducimos una nueva modalidad sofisticada de ataque utilizando falsificaciones sintéticas y una defensa eficaz contra el mismo, que asimismo ofrece adecuada protección contra los ataques que se han reseñado en el párrafo anterior.

Resultados y Objetivos

Con el objetivo de perseguir la línea de investigación presentada, se llevó a cabo el diseño y la implementación práctica de un sistema de autenticación continua donde se utiliza la dinámica de teclo en texto libre. Se integró un modelo de contextos finitos con un detector de falsificaciones sintéticas para brindar protección contra ataques de presentación y repetición, y la implementación se evaluó con varios conjuntos de datos disponibles públicamente para evaluar la generalización de los resultados. Idénticamente, se evaluó en condiciones del mundo real fuera de un ambiente de laboratorio. De manera consistente para todos los conjuntos de datos y respaldando la generalización de estos resultados, el error de clasificación se estabilizó asintóticamente a un valor entre 1% y 3%, con tasas de falsos negativos muy cercanas al 2% y tasas de falsos positivos que mostraron fluctuaciones más fuertes. Las figuras 1 y 2 muestran el detalle de tasas de error para la cantidad de teclas de entrenamiento en los datasets LSIA y KM.

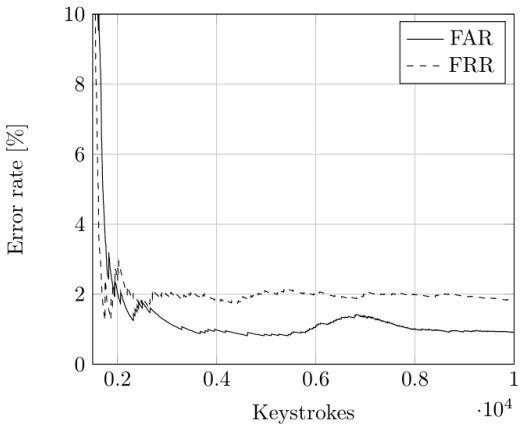

Figura 1. Tasas de error (FRR = falsos negativos, FAR = falsos positivos) de clasificación para el dataset LSIA.

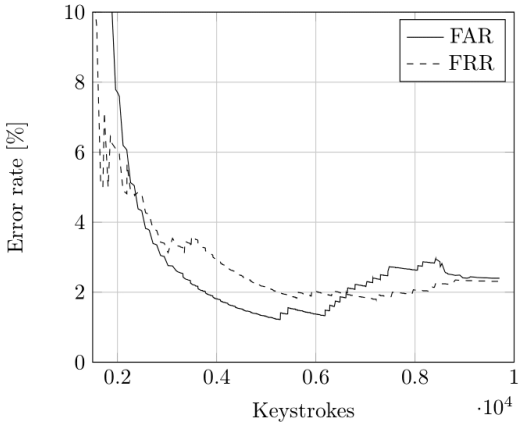

Figura 2. Tasas de error (FRR = falsos negativos, FAR = falsos positivos) de clasificación para el dataset KM.

El valor óptimo se alcanza con un entrenamiento de alrededor 4000

pulsaciones de teclas. Las tasas de error para el clasificador de falsificaciones sintéticas, que detecta ataques conocidos en sesiones individuales de aproximadamente 150 pulsaciones de teclas, se agruparon alrededor del 1% - 2%. Se observaron tasas de falsos negativos ligeramente más bajas que las tasas de falsos positivos, y se demostró que estas no se agregan a los errores del clasificador de usuarios legítimos debido a que ambos clasificadores actúan de manera complementaria.

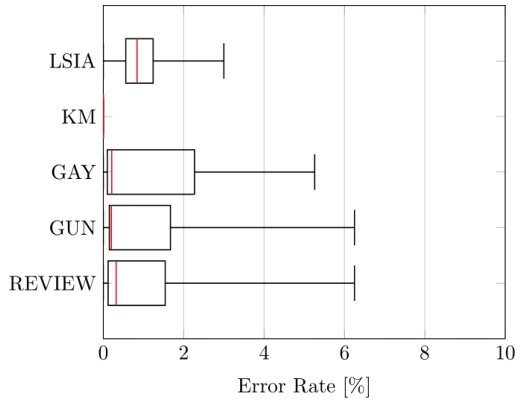

Figura 3. Distribución de falsos positivos utilizando falsificaciones sintéticas con un modelo de Markov de orden uno con desvío gausiano, para cinco conjuntos de datos.

Para evaluar el rendimiento de la etapa de prevención de ataques, se evaluaron falsificaciones sintéticas generadas con un modelo de Markov de orden uno, utilizando desvío gausiano, contra el clasificador de usuarios legítimos. Los resultados de rendimiento se muestran en la figura 3. Todos los conjuntos de datos muestran una tasa de error constantemente reducida, lo que demuestra la validez del supuesto. LSIA es el que tiene el efecto menos pronunciado, probablemente debido a la dificultad de este conjunto de datos. El modelado por contextos finitos puede ser utilizado también para la reconstrucción de un vector patrón que haga las veces de falsificación sintética, si esta puede ser inyectada en el sistema a ser atacado. Las mejoras respecto de un modelo de Markov involucran la variación en el tamaño óptimo del contexto, la selección y ponderación de modelos de distintos órdenes, y la posibilidad de utilizar distribuciones empíricas [González et. al., 2015].

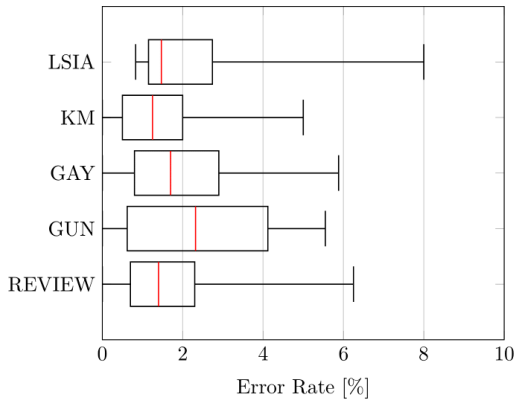

Figura 4. Distribución de falsos positivos utilizando falsificaciones sintéticas con un vector patrón generado con contextos finitos.

En la figura 4 se observa que, para todos los conjuntos de datos evaluados, la tasa de falsos positivos es mayor. La significación de este resultado es doble. En primer lugar, muestra que las falsificaciones sintéticas generadas con este método, más sofisticado, tienen una posibilidad más elevada de ser confundidas con el usuario legítimo. En segundo lugar, muestran que la etapa de

detección sigue siendo robusta aún frente a este tipo de ataques.

Formación de Recursos Humanos

En el marco de este proyecto se están desarrollando dos tesis doctorales. El equipo de investigación se conforma de tres investigadores formados y dos investigadores en formación.

Referencias

CALOT,E.,IERACHE,J.,HASPERUÉ,W. ROBUSTNESS OF KEYSTROKE DYNAMICS IDENTIFICATION ALGORITHMS AGAINST BRAIN-WAVE VARIATIONS ASSOCIATED WITH EMOTIONAL VARIATIONS. EN ADVANCES IN INTELLIGENT SYSTEMS AND COMPUTING, PÁGINAS 194-211, SPRINGER, CHAM, 2019 .

EPP, CLAYTON; LIPPOLD, MICHAEL; MANDRYK, REAGAN L. 2011. "IDENTIFYING EMOTIONAL STATES USING KEYSTROKE DYNAMICS", PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS, ACM, PP. 715-724.

GONZÁLEZ,N.; CALOT, E.; IERACHE, J.; FINITE CONTEXT MODELLING OF KEYSTROKE DYNAMICS IN FREE TEXT. EN 2015 INTERNATIONAL CONFERENCE OF THE BIOMETRICS SPECIAL INTEREST GROUP (BIOSIG), PÁGINAS 1–5, IEEE, 2015.

GONZÁLEZ,N.; CALOT, E.; IERACHE, J.; A REPLICATION OF TWO FREE TEXT KEYSTROKE DYNAMICS EXPERIMENTS UNDER HARSHER CONDITIONS. EN 2016 INTERNATIONAL CONFERENCE OF THE BIOMETRICS SPECIAL INTEREST GROUP (BIOSIG), PÁGINAS 1–6, SEP. 2016. DOII: 10.1109/BIOSIG.2016.7736905

GUNETTI, D.; PICARDI, C.; KEYSTROKE ANALYSIS OF FREE TEXT, EN ACM TRANSACTIONS ON INFORMATION AND SYSTEM SECURITY (TISSEC) 8.3, PÁGINAS. 312-347, 2005.

IERACHE, J; MERLINO, H.; CONCILIO, G.;CALOT E.; GONZÁLEZ, N. AVANCES EN RECONOCIMIENTO DE PATRONES DE TECLEO PARA LA IDENTIFICACIÓN DE PERSONAS EN AMBIENTES WEB, 2020. XXII WORKSHOP DE INVESTIGADORES EN CIENCIAS DE LA COMPUTACIÓN (WICC 2020), ISBN 978-987-3714-82-5, PP. 828–832.

KILLOURHY, K. S.; MAXION, R. A. 2009. COMPARING ANOMALY-DETECTION ALGORITHMS FOR KEYSTROKE DYNAMICS. IN INTERNATIONAL CONFERENCE ON DEPENDABLE SYSTEMS & NET- WORKS (DSN-09), PP. 125–134, ESTORIL, LISBON, PORTUGAL, 29 JUNE TO 02 JULY 2009. IEEE COMPUTER SOCIETY PRESS, LOS ALAMITOS, CALIFORNIA.

JOYCE, R.; GUPTA, G. 1990. IDENTITY AUTHENTICATION BASED ON KEYSTROKE LATENCIES. COMMUN. ACM 33, 2 (FEBRUARY 1990), PÁGINAS 168-176. HTTP://DOI.ACM.ORG/10.1145/75577.75582

LSIA: HTTP://LSIA.FI.UBA.AR, VIGENTE AL 22 DE FEBRERO DE 2021

RAHMAN, K.A., BALAGANI, K.S., PHOHA, V.V., 2011, June. Making impostor pass rates meaningless: A case of snoop-forge-replay attack on continuous cyber-behavioral verification with keystrokes. In *CVPR 2011 workshops* (pp. 31-38). IEEE.

STANCIU, V.D., SPOLAOR, R., CONTI, M. and Giuffrida, C., 2016, March. On the effectiveness of sensor-enhanced keystroke dynamics against statistical attacks. In *proceedings of the sixth ACM conference on data and application security and privacy* (pp. 105-112).

STEFAN, D., SHU, X., YAO, D.D., 2012. ROBUSTNESS OF KEYSTROKE-DYNAMICS BASED BIOMETRICS AGAINST SYNTHETIC FORGERIES. *COMPUTERS & SECURITY*, *31*(1), PP.109-121.