Universidad de Lima

Facultad de Ingeniería

Carrera de Ingeniería de Sistemas

PRUEBA DE CONCEPTO DE INTERFAZ TOUCHLESS EN TECLADO NUMÉRICO ALEATORIO PARA MITIGACIÓN DE SHOULDER SURFING EN CAJEROS AUTOMÁTICOS

Tesis para optar el Título Profesional de Ingeniero de Sistemas

Bruno Fabrizio Rios Villegas

Código 20163498

Asesor

Carlos Martin Torres Paredes

Lima – Perú

Julio de 2024

Prueba de concepto de interfaz touchless en teclado numérico aleatorio para mitigación de shoulder surfing en cajeros automáticos

Bruno Fabrizio Rios Villegas
20163498@aloe.ulima.edu.pe
Universidad de Lima

Resumen: La inclusión financiera en el Perú está en aumento, pues ya el 56 % de los adultos tiene productos financieros. Esto ha incrementado el uso de cajeros automáticos y los riesgos asociados a ellos, como el *shoulder surfing*. Buscando mitigar el riesgo de este ataque, se hizo una prueba de concepto de interfaz *touchless* que permite a los usuarios ingresar su PIN de manera segura, proponiendo un ejemplo para que sea usado por entidades bancarias o fabricantes de cajeros automáticos. Para esto, se generaron secuencias desordenadas aleatoriamente con los números del 0 al 9 sin que estos se repitan. Luego, se implementa sensores infrarrojos para ingresar los números del PIN. Se realizaron pruebas de mitigación y usabilidad con un grupo de 16 personas. La primera prueba mostró resultados alentadores, pues los a los atacantes se les dificulta identificar los dígitos ingresados por los usuarios y solo logaron registrar el 25 % correctamente. Asimismo, en las pruebas de usabilidad se obtuvo un promedio general de usabilidad de 78.4375, situando a la interfaz en un rango B+, por encima del umbral de 68 puntos. Considerando esto, se concluye que la propuesta cumple con el objetivo de permitir al usuario ingresar su PIN de manera segura ante ataques de *shoulder surfing*.

Palabras Clave: interfaces *touchless* / cajeros automáticos / *shoulder surfing* / teclado numérico aleatorio

Abstract: Financial inclusion in Peru is on the rise, with 56% of adults already having financial products. This has increased the use of ATMs and the risks associated with them, such as shoulder surfing. To mitigate the risk of this attack, a proof of concept of a touchless interface that allows users to enter their PIN securely was developed, seeking to inspire banking institutions or ATM manufacturers. For this purpose, randomly disordered sequences of numbers from 0 to 9 were generated without repeating them. Then, infrared sensors were implemented to enter the PIN numbers. Mitigation and usability tests were performed with a group of 16 people. The first test showed encouraging results, as the attackers found it difficult to identify the digits entered by the users and only managed to register 25% correctly. Likewise, in the usability tests, an usability average of 78.4375 was obtained, placing the interface in a B+ range, above the threshold of 68 points. Considering this, it is concluded that the proposal meets the objective of allowing the user to enter his PIN securely against shoulder surfing attacks.

Keywords: *touchless interfaces / automatic teller machines / shoulder surfing / random keypad*

Línea de investigación IDIC – ULIMA

Innovación: tecnologías y productos

Área y Sub-áreas de Investigación:

Área: Human-Centered Computing
Sub-área: Human-Computer Interaction

Objetivo (s) de Desarrollo Sostenible (ODS)
Industria, Innovación e Infraestructura

1. PLANTEAMIENTO DEL PROBLEMA

Los cajeros automáticos son una infraestructura de tecnología computarizada que provee a clientes de instituciones financieras el acceso a transacciones en un espacio público sin la necesidad de personal humano (Edem Udo Udo et al., 2017). Según la Superintendencia de Banca y Seguros y AFP (2020), se estimó que la cantidad de cajeros automáticos en el Perú en el año 2019 era de 28 407. Además, según datos de Statista (2023), en el año 2021 había 117.24 cajeros automáticos por cada 100 000 adultos peruanos. Esto es relevante puesto que, según Toledo y León (2023), la inclusión financiera en el país alcanzó el 56 %, lo cual significa que ese mismo porcentaje de personas adultas tienen, al menos, un producto financiero.

Lamentablemente, el uso de estos dispositivos también conlleva riesgos. En el ámbito de la seguridad uno de estos riesgos está asociado al PIN. Un inconveniente es que las personas tienen por costumbre utilizar el mismo código para autenticar diversos dispositivos o cuentas (celular, laptop, tarjeta, etc.) (Rajarajan et al., 2014). Asimismo, se suele elegir secuencias fácilmente recordables como fechas de nacimiento o números de casa. Paralelamente, los delincuentes han ideado diversos métodos para obtener el PIN de las personas como el *shoulder surfing*, el *key logging* y el *phishing* (Rajarajan et al., 2014). Según Abhishek et al. (2019), el número de robos y fraudes relacionados con cajeros automáticos crece cada día porque más del 90 % son vulnerables a ataques como el *shoulder surfing*. De hecho, una encuesta realizada por Ipsos (2019) revela que ya son 400 000 los peruanos que han sido víctimas de algún tipo de robo o fraude financiero.

2. OBJETIVO

El presente trabajo tuvo como objetivo la creación de una prueba de concepto de interfaz *touchless* en teclado numérico aleatorio para la mitigación del riesgo de *shoulder surfing* en cajeros automáticos.

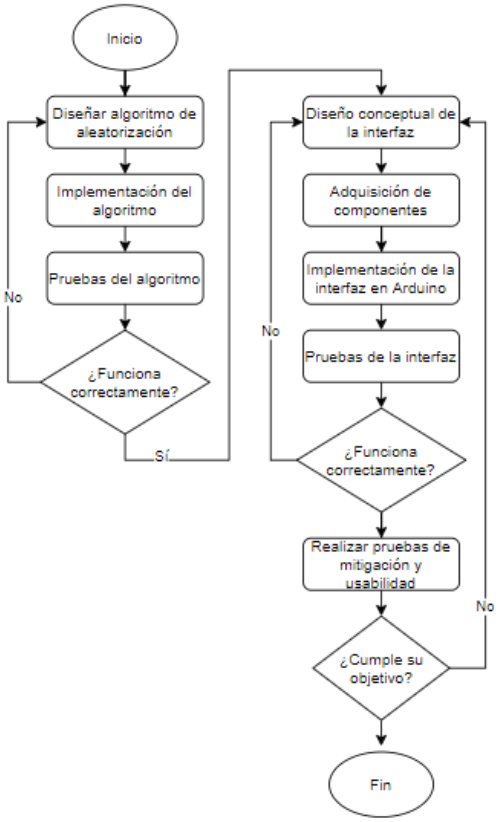
3. JUSTIFICACIÓN

A pesar de que en años previos se han explorado propuestas para mitigar el riesgo de un ataque de *shoulder surfing* haciendo uso de teclados aleatorios, se encuentra un vacío en la adición de nuevas tecnologías en las propuestas presentadas, especialmente soluciones *touchless*.

4. DISEÑO METODOLÓGICO

Figura 1

Diagrama de la metodología



Tal como se observa en la Figura 1, la metodología inicia con el diseño e implementación de un algoritmo para la generación de números aleatorios. Estos son usados para producir la secuencia que se le presenta en pantalla a cada usuario. Una vez que el algoritmo fue implementado se realizaron pruebas para medir su efectividad. Estas pruebas consistieron en comparar las secuencias aleatorias que el algoritmo va generando, de forma que se obtuvo el número de secuencias iguales en un determinado número de ejecuciones. Se estableció como límite que el promedio de secuencias repetidas en 1500 usos (ejecuciones) de la interfaz sea menor a uno; al cumplirse esta condición, se pasó a la siguiente etapa.

Luego, se procedió a adquirir los componentes necesarios para construir la interfaz de manera física. Finalizado este proceso se validó que los datos puedan ser ingresados correctamente. Para realizar esta validación se generaron secuencias aleatorias y se colocaron diferentes códigos PIN, revisando que cada valor ingresado corresponda con el dígito del PIN que se deseaba colocar. Al corresponder los valores en su totalidad, entonces se está logrando la funcionalidad deseada y se pasó a la siguiente fase.

En la etapa final se aplicaron dos tipos de pruebas: de mitigación y de usabilidad. La primera tuvo como objetivo comprobar que la interfaz cumple su misión de mitigar el riesgo de ataque de *shoulder surfing*. En esta prueba se reunió a un grupo de personas, el cual se subdividió en dos grupos de igual tamaño: usuarios y atacantes. La prueba consistió en que los atacantes intenten descubrir los dígitos del PIN de los usuarios mientras estos los ingresan en la interfaz; el grupo de usuarios no supo que estaba siendo observado. Para medir la efectividad de esta prueba se recogieron y analizaron los resultados para posteriormente compararlos con los de la literatura

actual, de forma que se conozca si la implementación obtuvo resultados similares a otras implementaciones. La segunda prueba buscó conocer la experiencia de los usuarios hacia el uso de la interfaz implementada. Para esto se le solicitará al grupo previamente reunido que haga uso de la interfaz y se les pidió que completen el cuestionario SUS al terminar. Para medir la efectividad de esta prueba se recogieron y analizaron los datos y se compararon con la puntuación media general de usabilidad SUS, la cual es de 68 puntos.

AGRADECIMIENTOS

Agradezco principalmente a mis padres por hacer posible estudiar en una universidad de tan alta calidad como la Universidad de Lima y siempre estar para mí y apoyarme día y noche a lo largo de toda mi carrera universitaria y mi vida. De igual manera me gustaría agradecer a mis amigos pertenecientes a la Carrera de Ingeniería de Sistemas por hacer estos años inolvidables y siempre apoyarnos los unos a los otros en todos los cursos. Finalmente, me gustaría agradecer a todos mis amigos fuera de la carrera y de la universidad por haber sido un gran soporte emocional a lo largo de estos años.

REFERENCIAS

Abhishek, K., Verma Kumar, M., & Prasad Singh, M. (2019). Automated random colour keypad. *Int. J. Information and Communication Technology*, *15*(2), 162–175. https://doi.org/10.1504/IJICT.2019.10018383

Adithya, P., Aishwarya, S., Megalai, S., Priyadharshini, S., & Kurinjimalar, R. (2018). Security enhancement in automated teller machine. *Proceedings of 2017 International Conference on Intelligent Computing and Control, I2C2 2017*, *2018-Janua*, 1–5. https://doi.org/10.1109/I2C2.2017.8321773

Agarwal, M., Mehra, M., Pawar, R., & Shah, D. (2011). Secure authentication using dynamic virtual keyboard layout. *International Conference and Workshop on Emerging Trends in Technology 2011, ICWET 2011 - Conference Proceedings*, *Icwet*, 288–291. https://doi.org/10.1145/1980022.1980087

Ahmad, A. G. (2013). Arduino as a learning tool. *Sensing Technologies for Global Health, Military Medicine, and Environmental Monitoring III*, *8723*, 872313.

Alsuhibany, S. A. (2021). A Camouflage Text-Based Password Approach for Mobile Devices against Shoulder-Surfing Attack. *Security and Communication Networks*, *2021*. https://doi.org/10.1155/2021/6653076

Borsci, S., Federici, S., Bacci, S., Gnaldi, M., & Bartolucci, F. (2015). Assessing User Satisfaction in the Era of User Experience: Comparison of the SUS, UMUX, and UMUX-LITE as a Function of Product Experience. *International Journal of Human-Computer Interaction*, *31*(8), 484–495. https://doi.org/10.1080/10447318.2015.1064648

Bultel, X., Dreier, J., Giraud, M., Izaute, M., Kheyrkhah, T., Lafourcade, P., Lakhzoum, D., Marlin, V., & Motá, L. (2018). Security analysis and psychological study of authentication methods with PIN codes. *Proceedings - International Conference on Research Challenges in Information Science*, *2018-May*, 1–11. https://doi.org/10.1109/RCIS.2018.8406648

Chakraborty, T., Nasim, M., Bin Malek, S. M., Sami, M. T. H. M., Saeef, M. S., & Al Islam, A. B. M. A. (2016). Sporshohin: A tale of devising visible light based low-cost robust touchless input device. *Proceedings of the 7th Annual Symposium on Computing for Development, ACM DEV-7 2016*. https://doi.org/10.1145/3001913.3001914

Edem Udo Udo, E., Abiso Kabir, A., Yusuff, A. M., & Bukola Simeon, A. (2017). Impact of Automated Teller Machine on Customer Satisfaction and Profitability of Commercial Banks. *IIARD International Journal of Banking and Finance Research*, *3*(2). www.iiardpub.org

Ipsos. (2019, October 14). *Hay 400,000 que sufrieron algún tipo de robo o fraude financiero*. 1. https://www.ipsos.com/sites/default/files/ct/publication/documents/2019-10/hay_400000_que_sufrieron_algun_tipo_de_robo_o_fraude_financiero.pdf

Lewis, J. R. (2018). Measuring Perceived Usability: The CSUQ, SUS, and UMUX. *International Journal of Human-Computer Interaction*, *34*(12), 1148–1156. https://doi.org/10.1080/10447318.2017.1418805

Lewis, J. R., Utesch, B. S., & Maher, D. E. (2013). UMUX-LITE - When there's no time for the SUS. *Conference on Human Factors in Computing Systems - Proceedings*, *October*, 2099–2102. https://doi.org/10.1145/2470654.2481287

Maiti, A., Jadliwala, M., & Weber, C. (2017). Preventing shoulder surfing using randomized augmented reality keyboards. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017*, 630–635. https://doi.org/10.1109/PERCOMW.2017.7917636

Montanaro, L., Sernani, P., Dragoni, A. F., & Calvaresi, D. (2016). A touchless human-machine interface for the control of an elevator. *CEUR Workshop Proceedings*, *1746*, 58–65.

Rajarajan, S., Maheswari, K., Hemapriya, R., & Sriharilakshmi, S. (2014). *Shoulder Surfing Resistant Virtual Keyboard for Internet Banking*. *31*(7), 1297–1304. https://doi.org/10.5829/idosi.wasj.2014.31.07.378

Roth, V., Richter, K., & Freidinger, R. (2004). A PIN-entry method resilient against shoulder surfing. *Proceedings of the ACM Conference on Computer and Communications Security*, 236–245. https://doi.org/10.1145/1030083.1030116

Sevilla-Gonzalez, M. D. R., Moreno Loaeza, L., Lazaro-Carrera, L. S., Bourguet Ramirez, B., Vázquez Rodríguez, A., Peralta-Pedrero, M. L., & Almeda-Valdes, P. (2020). Spanish Version of the System Usability Scale for the Assessment of Electronic Tools: Development and Validation. *JMIR Human Factors*, *7*(4), e21161. https://doi.org/10.2196/21161

Shukla, S., Helonde, A., Raut, S., Salode, S., & Zade, J. (2018). *Random Keypad and Face Recognition Authentication Mechanism*. 3685–3688.

Statista Research Departmen. (10 de Agosto de 2023). Number of automated teller machines (ATMs) per 100,000 adults in Peru from 2005 to 2021. Obtenido de Statista: https://www.statista.com/statistics/1079224/peru-automated-teller-machines-atm-penetration/

Statista Research Department. (8 de Agosto de 2023). Number of ATM transactions in selected countries in Latin America in 2019. Obtenido de Statista: https://www.statista.com/statistics/823923/number-atm-transactions-latin-america-country/

Still, J. D., & Bell, J. (2018). Incognito: Shoulder-surfing resistant selection method. *Journal of Information Security and Applications*, *40*, 1–8. https://doi.org/10.1016/j.jisa.2018.02.006

Superintendencia de Banca y Seguros y AFP. (2020). *Perú: Indicadores de Inclusión Financiera de los sistemas financieros, de seguros y de pensiones - Junio 2020*. 1–40.

Toledo Concha, E., & León Reyes, V. (2023). FINANCIAL INCLUSION IN PERU: APPRAISAL AND PERSPECTIVES. *QUIPUKAMAYOC*, *31*(65), 73–84. https://doi.org/10.15381/quipu.v31i65.25882

Yu, M., Zhuge, J., Cao, M., Shi, Z., & Jiang, L. (2020). A survey of security vulnerability analysis, discovery, detection, and mitigation on IoT devices. *Future Internet*, *12*(2), 1–23. https://doi.org/10.3390/fi12020027

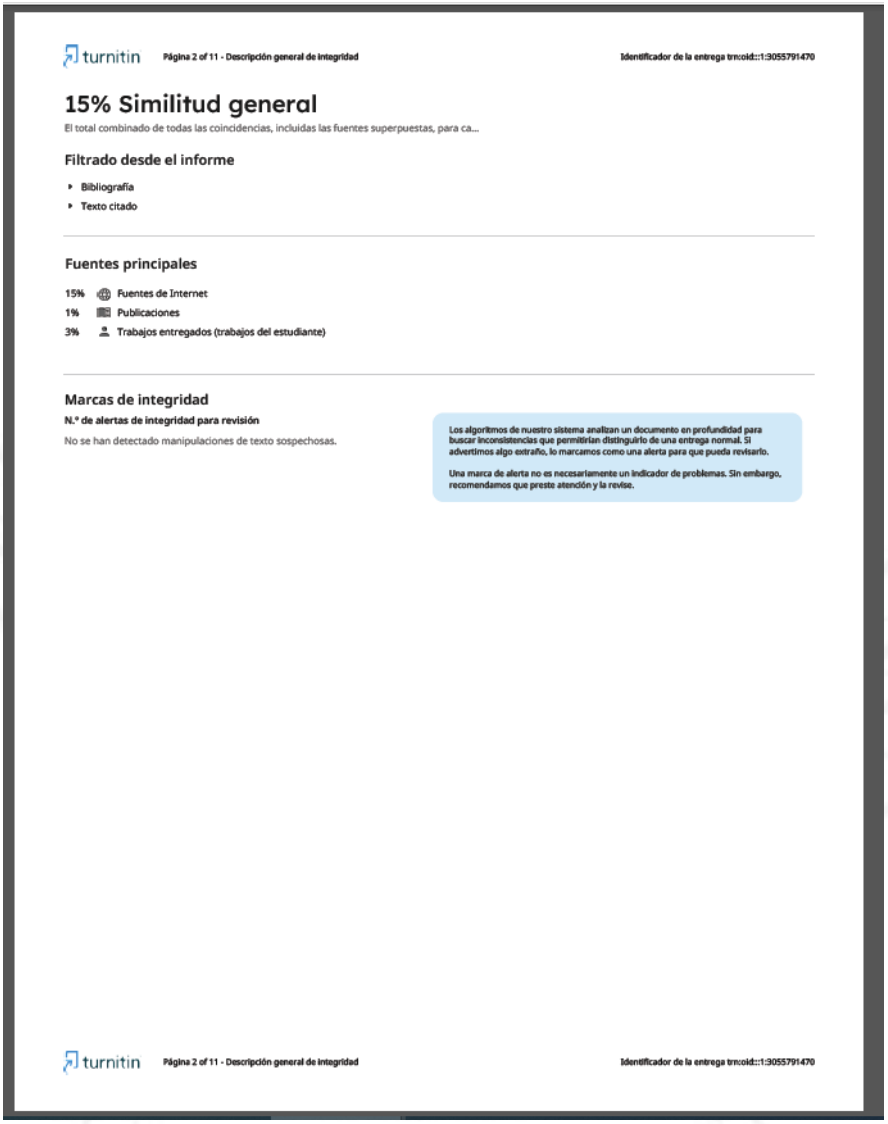
ANEXOS

Datos del artículo publicado

- Nombre del artículo: Prueba de concepto de interfaz *touchless* en teclado numérico aleatorio para la mitigación de *shoulder surfing* en cajeros automáticos
- Autores: Bruno Fabrizio Ríos Villegas
- Co autor(es): Carlos Martín Torres Paredes

Publicación en revista

- Nombre de la revista: Interfases
- Volumen:
- Número: 018
- Año: 2023
- Pp: 207-233
- Enlace web donde se encuentra publicado el artículo (identificador DOI, ISBN, ISSN o equivalentes): https://revistas.ulima.edu.pe/index.php/Interfases/article/view/6557



turnitin Página 2 of 11 - Descripción general de integridad Identificador de la entrega trn:oid:::1:3055791470

15% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado

Fuentes principales

15% Fuentes de Internet
1% Publicaciones
3% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

turnitin Página 2 of 11 - Descripción general de integridad Identificador de la entrega trn:oid:::1:3055791470