Resumen

El Shoulder Surfing es un ataque de ingeniería social cuyo modus operandi se centra en sustraer información de la víctima mediante la “observación sobre su hombro”. Esto repercute en la seguridad de la información de la víctima, como de la organización a la que pertenece, de tal forma que puede causar daños financieros, reputacionales e incluso morales. El presente estudio busca detectar y mitigar esta problemática a través del desarrollo de un artefacto de software por medio de la implementación de tecnologías modernas como el Deep Learning a través del “Reconocimiento Facial” y las Redes Neuronales Convolucionales en conjunto con el Procesamiento de Imágenes y la Visión por Computador. Para lograrlo, se aplicó SCRUM por su peculiaridad para agilizar procesos, entrega de resultados y calidad en sus productos. La metodología para el módulo de reconocimiento facial se basó en un procedimiento de 9 pasos que van desde la carga y extracción de datos de las imágenes hasta la detección e identificación de personas, sin contar los pasos restantes de mitigación, registro y notificación adicionales implementados. Se realizaron pruebas de experiencia de usuario, rendimiento de la mitigación y rendimiento del reconocimiento facial. Los resultados muestran que el factor principal que determina las características de potencia para los dispositivos, es determinado por la resolución de video que es suministrado en tiempo real al sistema. Para el reconocimiento facial se desarrolló una ecuación para determinar el tiempo de procesamiento, que determinó que, por cada 5 imágenes, el tiempo incrementa 3.06 segundos aproximadamente de procesamiento. Estos resultados podrían incrementar el nivel de ciberseguridad en las personas más vulnerables de la familia, la academia, la empresa y la industria.

Palabras clave: Shoulder Surfing, Deep Learning, Face Recognition, Social Engineering, Mitigation.

Abstract

Shoulder Surfing is a social engineering attack whose modus operandi focuses on stealing information from the victim through "over-the-shoulder observation." This affects the security of the victim's information and the organization to which it belongs in such a way that it can cause financial, reputational, and even moral damage. The present study seeks to detect and mitigate this problem by developing a software artifact by implementing modern technologies such as Deep Learning through "Facial Recognition" and Convolutional Neural Networks in conjunction with Image Processing and Computer Vision. To achieve this, SCRUM was applied due to its peculiarity to streamline processes and deliver results and quality in its products. The methodology for the facial recognition module was based on a 9-step procedure that goes from loading and extracting data from images to detecting and identifying people, not counting the remaining steps of additional mitigation, registration, and notification implemented. Tests were performed on user experience, mitigation performance, and facial recognition performance. The results show that the main factor determining the devices' power characteristics is the video resolution supplied in real-time to the system. For facial recognition, an equation was developed to determine the processing time, which picked that for every five images, processing time increases by approximately 3.06 seconds. These results could improve cybersecurity in the most vulnerable people in the family, academia, business, and industry.

Keywords: Shoulder Surfing, Deep Learning, Face Recognition, Social Engineering, Mitigation.