Maestría en

CIBERSEGURIDAD

Trabajo previo a la obtención del título de

Magíster en Ciberseguridad

AUTORES:

Cajamarca Peñafiel Jorge Andrés

Ortiz Guerra Karolain Mishell

Rosero Romero Cyntia Ibeth

Zurita Gaón Aquiles Aldemar

TUTOR/ES:

Alejandro Cortés López

Iván Reyes Chacón

TEMA:

Análisis Comparativo de la Seguridad en dos Versiones de una Aplicación Móvil y su Interacción con una Interfaz de Programación de Aplicaciones (API).

Quito - Ecuador

REINVENTEMOS EL FUTURO

Resumen

La presente investigación analiza la seguridad en aplicaciones móviles Android mediante un análisis comparativo de dos variantes de la aplicación d2®Movil, desarrollada por BIOMETRIKA SA. La versión básica incorpora mecanismos de seguridad fundamentales, mientras que la versión plus integra técnicas avanzadas de protección. Este estudio evalúa sistemáticamente el impacto de estas diferencias arquitectónicas en la confidencialidad, integridad y privacidad de la información durante las comunicaciones con la Interfaz de Programación de Aplicaciones (API) del sistema d2Web.

El abordaje metodológico combina técnicas de análisis estático y dinámico mediante herramientas especializadas como Burp Suite, Frida y JADX. Se aplicaron procedimientos de interceptación de tráfico de red, ingeniería inversa de código y evaluación de certificados digitales, manteniendo un enfoque ético que excluye pruebas de penetración en sistemas productivos. La investigación identifica vulnerabilidades significativas en la versión estándar, destacando la transmisión de credenciales sin cifrar, la ausencia de encriptación para información sensible y la atención de mecanismos de autenticación del dispositivo.

Los hallazgos muestran que la versión plus mejora significativamente la protección de datos, sin embargo, ambas versiones deben mejorarse para cumplir la normativa legal ecuatoriana. Además, ofrece un marco metodológico reproducible para evaluar la seguridad en aplicaciones móviles con directrices prácticas para fortalecer su arquitectura.

Palabras Claves: aplicaciones móviles, ingeniería inversa, API, análisis dinámico, análisis estático.

Abstract

This research analyzes the security of Android mobile applications through a comparative analysis of two variants of the d2®Movil application, developed by BIOMETRIKA SA. The basic version incorporates fundamental security mechanisms, while the plus version integrates advanced protection techniques. This study systematically evaluates the impact of these architectural differences on the confidentiality, integrity, and privacy of information during communications with the d2Web system's Application Programming Interface (API).

The methodological approach combines static and dynamic analysis techniques using specialized tools such as Burp Suite, Frida and JADX. Network traffic interception, code reverse engineering, and digital certificate evaluation procedures will be applied, maintaining an ethical approach that excludes penetration testing on production systems. The research identifies significant vulnerabilities in the standard version, highlighting the transmission of unencrypted credentials, the lack of encryption for sensitive information, and the lack of device authentication mechanisms. The findings show that the Plus version significantly improves data protection; however, both versions must be optimized to comply with Ecuadorian regulations. It also offers a reproducible methodological framework for evaluating mobile app security, along with practical guidelines for strengthening their architecture.

Keywords: mobile applications, reverse engineering, API, dynamic analysis, static analysis.