CONGRESO INTERNACIONAL DEL
XXVIII VERANO DE LA INVESTIGACIÓN CIENTÍFICA Y TECNOLÓGICA DEL PACÍFICO

# Análisis de seguridad de aplicaciones móviles wearables para sistema operativo Android

Dr. Alfonso Martinez Cruz – Instituto Nacional de Astrofísica, Óptica y Electrónica
Saul Isui Lugo Martinez – Instituto Tecnológico de Pachuca
ODS - Desarrollar infraestructuras resilientes, promover la industrialización inclusiva y sostenible, y fomentar la innovación.

## 1. Introducción

En un contexto donde las aplicaciones móviles wearables en Android son cada vez más populares, surge la necesidad de examinar su seguridad frente a los posibles ataques maliciosos. Por lo cual, en esta investigación se presenta la evaluación y búsqueda de código malicioso insertado en aplicaciones móviles wearables de manera intencional.

**1.1. Objetivo general:**

Realizar un análisis de seguridad a una aplicación móvil wearable para sistema operativo Android.

**1.2. Objetivos específicos:**

1) Realizar técnicas de inyección de código malicioso a una ampliación wearable
2) Realizar un análisis estático a una aplicación wearable
3) Realizar un análisis dinámico a una aplicación wearable

Figura 1. Figura ilustrativa de dispositivo wearable

## 2. Metodología

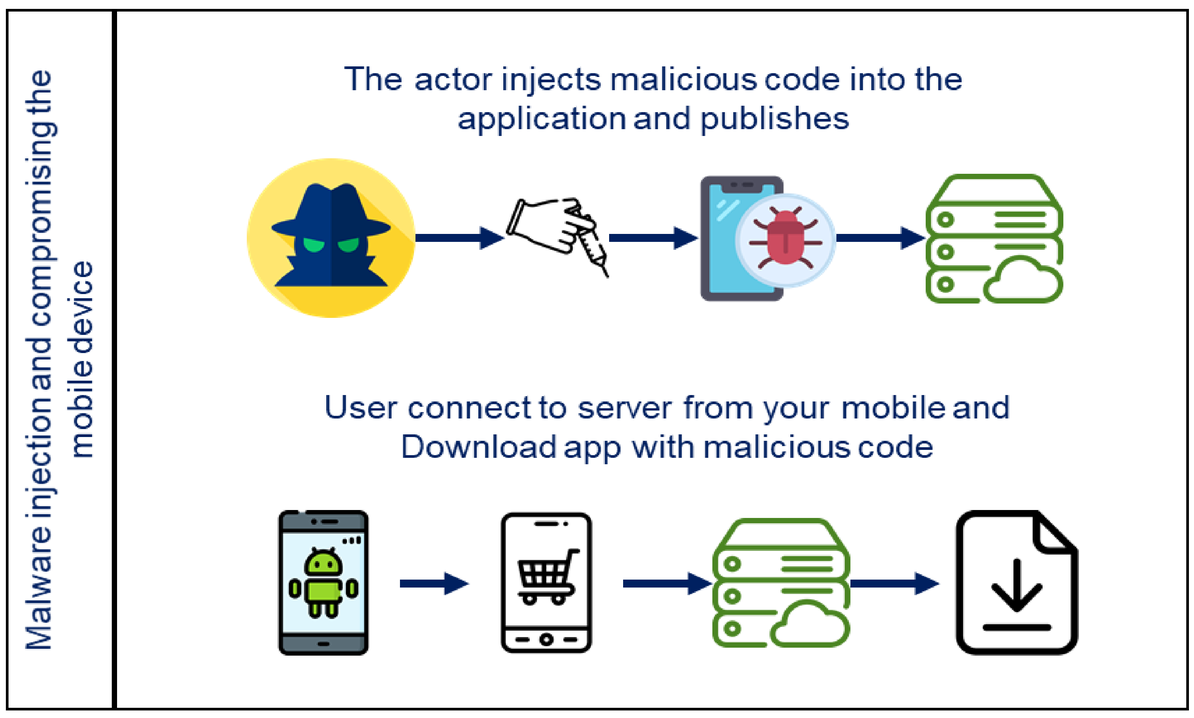


Figura 2. Inyección de código malicioso con Metasploit

## 3. Experimentación y resultados

Tabla 1. Experimentación y resultados

| Identificación de la vulnerabilidad o Payload | Resultado del análisis |
|---|---|
| **Elementos Sospechosos en la Aplicación** | Se identificaron cadenas de texto y patrones inusuales en la aplicación durante el análisis. |
| **Permisos Dudosos Identificados** | Se encontraron permisos sospechosos en la aplicación. Como grabación de sonido con el micrófono, permisos de videograbación con la cámara, lectura de SMS, etc. |
| **Clases y Métodos Relacionados con Payload de Metasploit** | En el manifiesto de Android, se detectaron clases y métodos relacionados con el payload de Metasploit. |
| **Referencias al Framework de Metasploit** | Se hallaron referencias al framework de Metasploit, utilizado para cargar el payload en la APK. |
| **Actividades Sospechosas Detectadas** | Durante el análisis, se identificaron actividades sospechosas, como la creación de procesos y cambios en la configuración de la aplicación. |
| **Inserción de Código malicioso en la APK** | Se evidenció la inserción de código malicioso en áreas específicas de la APK, indicando la integración del payload en el proceso de compilación. |

## 5. Referencias

[1] S. Hutchinson, Investigating Wearable Fitness Applications: Data Privacy and Digital Forensics Analysis on Android. 2022.
[2] K. W. Ching y M. M. Singh, “Wearable technology devices security and privacy vulnerability analysis”, Int. J. Netw. Secur. Appl., vol. 8, núm. 3, pp. 19–30, 2016.
[3] S. Mujahid, R. Abdalkareem, y E. Shihab, “Studying permission related issues in android wearable apps”, en 2018 IEEE International Conference on Software Maintenance and Evolution (ICSME), 2018.

Para enfrentar desafíos y asegurar la integridad de aplicación, es esencial contar con un entorno de pruebas controlado. Este estudio propone la creación de dicho entorno, que combina herramientas como Kali Linux, Ubuntu, Mobile Security Framework (MobSF) y Metasploit. Esto permitirá llevar a cabo un análisis de seguridad minucioso y eficaz en aplicaciones wearables para Android.

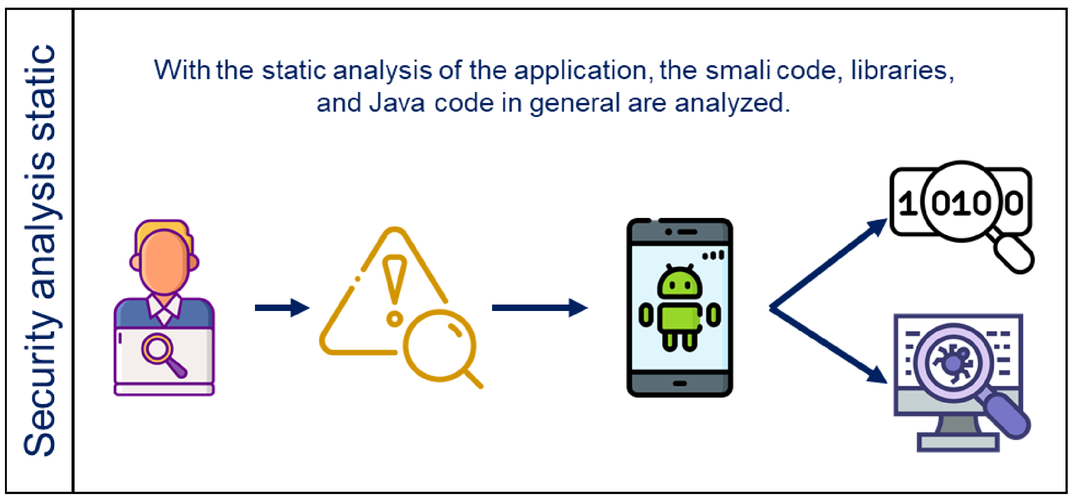


Figura 3. Análisis estático

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|---|---|---|
| android.permission.ACCESS_COARSE_LOCATION | dangerous | coarse (network-based) location | Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are. |
| android.permission.ACCESS_FINE_LOCATION | dangerous | fine (GPS) location | Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power. |

Figura 4. Resultados del análisis estático con el Mobile Security Framework en Kali Linux

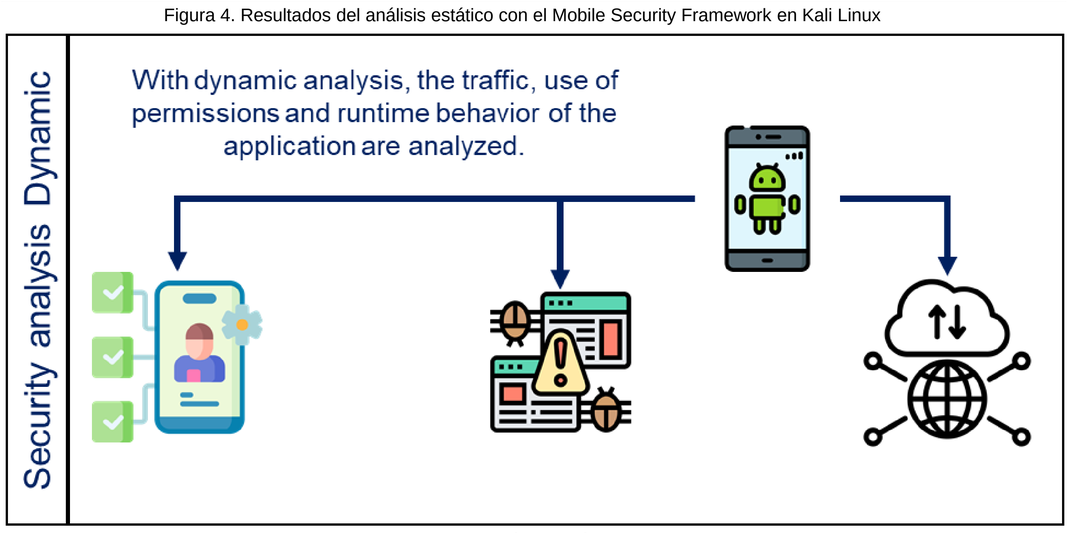


Figura 5. Análisis dinámico

## 4. Conclusiones

La preservación de la privacidad del usuario subraya la imperante necesidad de implementar medidas de seguridad para salvaguardar información. La identificación de riesgos como accesos no autorizados y vulneraciones de datos en la evaluación del código resalta la urgencia de adoptar medidas de seguridad durante el proceso de desarrollo y mantener una supervisión constante. Estos hallazgos están estrechamente vinculados al ODS de "Desarrollar infraestructuras resilientes, promover la industrialización inclusiva y sostenible, y fomentar la innovación", ya que subrayan la importancia de garantizar la seguridad en un entorno tecnológico en constante evolución para lograr un desarrollo inclusivo, sostenible y seguro. El verano de investigación científica ha sido una experiencia en donde desarrolle mis aptitudes y habilidades para la investigación, análisis y trabajo en equipo. El Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE) del CONAHCYT, me ha brindado una experiencia profesional y científica inolvidable, impulsándome a continuar con una carrera científica.

**PARA SABER MÁS DEL PROYECTO VISITA:**

México Colombia Costa Rica Perú Nicaragua E.U.A.