**Research vulnerabilities in android's audio infrastructure focusing on unauthorized eavesdropping**

SE-B-13

Mor Bar; morba1@ac.sce.ac.il

Advisors: Dr. Marina Litvak1, Mr. Mordi Hagis2

1SCE - Shamoon College of Engineering, Be'er-Sheva

2HIT - Holon Institute of Technology, Holon

This research investigates vulnerabilities in Android’s audio infrastructure, focusing on unauthorized eavesdropping as a critical threat. The study examines Android’s complex audio architecture comprising eight layers from application to kernel level, identifying potential weaknesses that could allow malicious actors to bypass Google’s security enhancements introduced in Android 9 (Pie). Through systematic analysis and empirical testing, the research demonstrates how zero-day vulnerabilities can facilitate covert eavesdropping through unauthorized applications. The methodology encompasses architectural mapping, vulnerability assessment, exploitation research, and validation across multiple Android versions. The project identifies specific security gaps in audio permission models and background processing restrictions, contributing to the understanding of mobile eavesdropping vulnerabilities and providing a foundation for developing more robust safeguards against emerging threats.

Keywords: android security, audio infrastructure, background recording, eavesdropping, mobile privacy, surveillance, zero-day vulnerabilities.