LIBRARY DETEKSI *ROOT* DAN *FLAG SECURE* PADA PERANGKAT *ANDROID*

Oleh

MOHAMMAD ARBI YOGANATA

E-mail: mohammadarbiyoganata@gmail.com

ABSTRAK

Keamanan aplikasi *android* menghadapi ancaman canggih seperti *root hiding* dan *runtime tampering* sehingga perlu adanya sebuah *library* keamanan komprehensif untuk mendeteksi berbagai ancaman tersebut. Dengan pendekatan deteksi berlapis yang menggabungkan analisis statis, heuristik, dan pemanfaatan kode *native C++*, *library* ini dikembangkan untuk mengidentifikasi status *root*, emulator, aplikasi berbahaya, dan *bypass flag secure*. Validasi dilakukan melalui pengujian *white-box*, *black-box*, dan pengujian ahli dengan metode *Aiken's V*. Hasil menunjukkan *library* ini berhasil menembus teknik *root hiding* modern seperti *Magisk Hide, Zygisk*, dan *Shamiko*, serta mencapai tingkat keberhasilan 100% pada skenario fungsional. Penilaian ahli menghasilkan koefisien validitas isi sebesar 0.75, yang tergolong tinggi. Penelitian ini menghasilkan sebuah *library* keamanan yang efektif dan selaras dengan standar OWASP MASVS, dengan batasan teridentifikasi pada *framework hooking Lsposed* yang menjadi arah pengembangan selanjutnya.

Kata kunci: Deteksi *Root*, *Flag Secure*, Keamanan *Android*, Pustaka *Android*, Keamanan *Mobile*.

ROOT DETECTION *LIBRARY* AND SECURE FLAG ON *ANDROID* DEVICES

By

MOHAMMAD ARBI YOGANATA

E-mail: mohammadarbiyoganata@gmail.com

ABSTRACT

Android application security faces advanced threats such as root hiding and runtime tampering, so a comprehensive security library is needed to detect these various threats. With a layered detection approach that combines static analysis, heuristics, and the use of native C++ code, this library was developed to identify root status, emulators, malicious applications, and bypass security flags. Validation was performed through white-box, black-box, secure flag bypasses. Validation was conducted through white-box, black-box, and expert testing using Aiken's V method. The results show that the library successfully penetrates modern root hiding techniques such as Magisk Hide, Zygisk, and Shamiko, achieving a 100% success rate in functional scenarios. Expert assessment yielded a content validity coefficient of 0.75, which is considered high. This research produced an effective security library that aligns with OWASP MASVS standards, with identified limitations in the Lsposed hooking framework, which will be the focus of future development.

Keywords: Root Detection, Flag Secure, Android Security, Android Library, Mobile Security.