A Review of Android operating system security issues

By Mohamed Razeed Mohamed Nowfeek

The decided on research paper(Razeed and Nowfeek, 2022) delves into the world of operating system (OS) security, mainly focusing at the Android operating device. Android OS, being one of the maximum typical cellular working systems globally, affords a essential vicinity for investigation due to its sizeable utilization throughout smartphones and different devices. In the chosen research paper, the writer conducts a complete evaluation of the triumphing protection challenges in the Android OS ecosystem.(Kapoor and Agarwal, 2017). These challenges embody a spectrum of risks, starting from spyware and permission escalation attacks to information leakage and denial of service threats. By synthesizing present literature, the paper lays a strong foundation for expertise the multifaceted safety landscape within the Android OS. The research paper significantly evaluates the identified protection vulnerabilities in the Android OS environment. It scrutinizes the efficacy of proposed solutions and elucidates regions in which further refinement is essential. Through this critical analysis, the paper goals to pinpoint gaps and opportunities for enhancing the overall security posture of the Android OS.

Within the paper, numerous ability research goals are outlined. These goals embody a huge spectrum of security upgrades, together with the improvement of superior mechanisms to combat spyware, the implementation of robust permission control systems to mitigate escalation attacks, and the fortification of statistics safety measures to lower data leakage incidents. These targets feature guiding standards for future research endeavors geared towards bolstering report protection in the Android OS. The studies paper proposes numerous methods and solutions to cope with the identified protection challenges inside the Android OS. These answers encompass a various array of procedures, including RiskMon, Kirin, Crowdro, Paranoid Android(Mateus-Coelho, 2021), and DroidScope. Each method offers unique skills, which encompass runtime behavior assessment, permission verification, and malware detection, aimed in the direction of augmenting protection features in the Android OS surroundings.Each proposed solution inside the studies paper is observed thru a reason for its choice. For example, RiskMon leverages machine learning to know strategies to assess software program behaviors and become aware of capability risks, at the same time as Kirin specializes in certification mechanisms to save you the installation of risky apps. These justifications underscore the efficacy of the chosen strategies in enhancing document protection inside the Android OS.

**Reference list**

Kapoor, R. and Agarwal, S. (2017). Sustaining Superior Performance in Business Ecosystems: Evidence from Application Software Developers in the iOS and Android Smartphone Ecosystems. *Organization Science*, 28(3), pp.531–551. doi:https://doi.org/10.1287/orsc.2017.1122.

Mateus-Coelho, N. (2021). A New Methodology for the Development of Secure and Paranoid Operating Systems. *Procedia Computer Science*, 181, pp.1207–1215. doi:https://doi.org/10.1016/j.procs.2021.01.318.

Razeed, M. and Nowfeek, M. (2022). *IJRSI) |Volume IX, Issue I*. *International Journal of Research and Scientific Innovation*.