Understanding the security of mobile apps in Africa

January 2 2024, by Hannah Diorio-Toth

Report cover. Credit: Approov

Researchers from CyLab-Africa and the Upanzi Network recently partnered with the mobile security provider Approov to explore the security of common financial services apps used across Africa. After surveying 224 popular financial applications, the researchers found that 95% of these Android apps exposed secrets that can be used to reveal personal and financial data. Across these applications, approximately

272 million users have the potential to be victims of security flaws.

The Carnegie Mellon University Africa team included alumni and a current student who are all working as researchers with CyLab-Africa in Rwanda: Theoneste Byagutangaza (MSIT '23), Trevor Henry Chiboora (MSIT '23), Joel Jefferson Musiime (MSIT '24), and Lenah Chacha (MSIT '17).

The project was part of a summer collaboration experience where the CyLab-Africa researchers received guidance and mentorship from Approov. CyLab-Africa co-directors Assane Gueye and Giulia Fanti served as advisors for this project

"Participating in this project was a rewarding yet challenging experience. It involved in-depth research into the consequences of secret key leaks, which initially proved to be a formidable task. However, collaborating with a diverse team enriched my problem-solving skills, honed during my time as a student at CMU, and made the project a valuable learning opportunity," says Byagutangaza.

The team selected and investigated Android applications from countries in North, Central, Eastern, Western, and Southern Africa and categorized the security threats into "high," "medium," and "low" severity. Most of the threats fell into the high (18%) and medium (72%) categories.

A high-severity classification was used for vulnerabilities that could potentially lead to unauthorized access, data breaches, and compromised user privacy. Medium severity was used for secrets that, if exposed, could potentially compromise the confidentiality of user data and application functionality.

"Being new in the field of mobile security, this project was a good

learning experience as it gave me an understanding of the design and deployment of mobile apps from a security perspective," says Musiime. "Collaborating with the experienced team at Approov in the field of mobile security greatly aided my learning process, as they were always ready and willing to offer guidance and support throughout the research."

The work culminated in a report which draws comparisons between other regions and Africa, pinpointing trends, commonalities, and disparities pertaining to the exposure of secret keys in a mobile application's binary package. For example, they found that apps deployed in West Africa were the most exposed in terms of high severity secret exposure (20%) and Southern Africa the least (only 6%).

"The project report holds significant value for a wide audience, including product owners, developers, and everyday users. It not only sheds light on security concerns related to secrets and API keys in Android packages but also provides valuable recommendations for mitigating these issues," says Chiboora.

More information: Report: approov.io/info/security-chall … obile-apps-in-africa

Provided by Carnegie Mellon University Africa

Citation: Understanding the security of mobile apps in Africa (2024, January 2) retrieved 13 May 2024 from https://techxplore.com/news/2024-01-mobile-apps-africa.html