A Summary of 'An Empirical Study of Cryptographic Misuse in Android Applications'

Ally Smith

due April 28, 2022

The Android mobile operating system provides common functionality to cryptographic APIs, so that developers may more easily secure things like passwords and personal information. However, this study finds that a substantial number of developers still make mistakes that minimize the security overall. The authors of the paper also identified factors that contribute to this level of misuse, including missing lightweight security checks like in their program CryptoLint, and the default behavior of the library not being recommended practices. They believe that by including a set of tools to evaluate the security of a developer's program, they are more likely to adhere to cryptographic best practices. Additionally, by changing the default behavior of the API to be more secure practices, it is more likely for a more layman developer to follow good cryptographic security guidelines, as the program does this by default now. They also highlight how much of the API is missing documentation on how it is intended to be used, and they believe that adding a 'security discussion' would help address this. I believe that the recommendations in this paper are all logical and would provide much-needed security improvements to cryptographic APIs. Even during the short amount of programming with cryptography in this class that we have done, I have seen first hand how poorly documented some of these functionalities can be, and it would be very beneficial to many developers if it was made easier to comply with these standards.