TDP028 Project
Technical Memorandum

1 Introduction

Security and integration are one of the very critical issues on the internet nowadays. When it comes to the applications, it is the *permissions,* which is basically asking the user for access to the potential sensitive sources and information in the operative system. In my case, it is relevant e.g. asking for current location.

2 Before installation

As of Android 6 (Marshmallow), Google decided to change the whole procedure of *permission,* which was going from asking the user for *permissions* at the time of installation to asking the user only in case the application is using anything sensitive[1].

It has been demonstrated that if the applications ask for the *permissions* at the time of installation, there will be a very few number of people reading it or understand it whatsoever [1][2]. Therefore it will be utterly important for me to think more and apply accordingly when it comes to *permissions.*

3 In the application

It has proved itself that user is more likely to know what happens in the background, and in most cases the user is willing to block the toggle the *permission*-based activities happening in the background [1].
I will need to take even more things in consideration when it comes to *permissions* when the user is using the application e.g. sending pop-up windows asking for a specific permission which can lead to potential bugs and vulnerabilities in the application [3].

4 Tactics for the application

In order to not cause vulnerabilities in the app and provide a clear understanding to the user regarding what the application actually is doing, I should come up with a decision on which *permissions* I need in order to have a functioning application.

As Google audits the *permissions* constantly, which makes an older version of Android being asked for *permissions* which are unnecessary [3]. This affects in my decision-making as I will need to know which API level I should keep myself. In some cases, unnecessary *permissions* may cause the user to uninstall the application if they consider it outside their “comfort zone” [2].

References

[1] A. B. A. H. S. E. D. W. K. B. Primal Wijesekera, ”Android Permissions Remystified: A Field Study on Contextual Integrity,” i 24th USENIX Security Symposium (USENIX Security 15), Washington, D.C., USINEX Association, 2015, pp. 499-514.

[2] E. H. S. E. A. H. E. C. D. W. Adrienne Porter Felt, ”Android Permissions: User Attention, Comprehension, and Behavior,” Proceedings of the Eighth Symposium on Usable Privacy and Security, vol. III, nr 1, pp. 1-14, 2012.

[3] E. C. S. H. D. S. D. W. Adrienne Porter Felt, ”Android permissions demystified,” Proceedings of the 18th ACM conference on Computer and communication security, vol. 1, nr 18, pp. 627-638, 2011.