Vashek Matyáš
Fakulta informatiky
Masarykova univerzita
Botanická 68a, 602 00 Brno

MASTER THESIS REVIEW

Date: 13 / 6 / 2014

Student: Ondřej Güttner

Title: Group key agreement in Android-based mobile devices

Report: The submitted work focuses on the area of random sequence generation and group key agreement protocols for Android-based mobile devices. A brief overview of randomness extraction concepts and issues is provided in the first chapter, the second chapter discusses selected protocols for group key agreement. The third chapter presents the Android environment and the following chapter then discusses implementation issues. The fifth chapter concludes this thesis. The analyses and discussions of both randomness extractions issues as well as group key agreement are insightful, and the thesis as such provides some very interesting views and results of the author that are to be appreciated.

The language of the submitted work is acceptable; I only found some cases of wrong ordering of words in sentences, also missing articles and other minor issues. Overall, this submission was comprehensible, despite being written in English – that is not a native language of the author, as far as I know.

I have to commend that the author proposed and undertook both theoretical as well as implementation work during his engagement with this project, and delivered work exceeding my original expectations. The thesis submitted shows a thorough and diligent approach of the author.

I would definitely rank this thesis within the top 5% of the Master theses of the Faculty of Informatics.

Final recommendation:

Considering the above mentioned, I recommend that the submitted work is **approved** as the Master thesis of the candidate and that it is marked **A**, yet I would find mark B also acceptable in case of an unconvincing presentation.

I also suggest this thesis for the Dean's Award nomination.

Vashek Matyáš
(supervisor)