Dissertação de Mestrado em Engenharia Informática (2017/2018)

Title: Android hard Disk Study.

Supervisor: Prof. Paul Crocker Email: crocker@di.ubi.pt

Description

The main aim of the thesis is to study whether encrypted android disks contain any useful retrievable information. Many studies have found that a considerable proportion of old disks, from the desktop and mobile universes contain private information, however an interesting case is that of encrypted android disks, see for instance details at [1]. In general for Android 5 and above the encryption key is bound to the hardware device, in order to prevent off line brute force attacks, however in the literature several methods for bypassing this process can be found, eg [2]. In this thesis a cloud based architecture for booting android disk images (copied from real phones)should be developed in order to asses the possibility of decrypting devices that use short passwords, dictionary based passwords or simple pins and patterns.

Work Plan

1 Literature and State of the Art Review
2 Study of the characteristics, algorithms and architectures to be used.
3 Implementation, Testing and Evaluation of the proposed solution
4 Publication of the results
5 Writing of the Dissertation.

References

[1] https://source.android.com/security/encryption/full-disk
[2] https://github.com/laginimaineb/ExtractKeyMaster
[3] https://santoku-linux.com/howto/mobile-forensics/how-to-brute-force-android-encryption/
[4] Frost, Forensic Recovery of Scrambled Telephones, Tilo M uller, Michael Spreitzenbarth, and Felix C. Freiling, The 11th International Conference on Applied Cryptography and Network Security (ACNS 2013)