Evaluating the privacy of Android mobile applications under forensic analysis

Christoforos Ntantogian, Dimitris Apostolopoulos, Giannis Marinakis, Christos Xenakis

May 7, 2018

1 Summary

The security of mobile device and user account credentials is a burning issue nowadays. In this paper, the possibility of recovering authentication credentials of mobile applications from the volatile memory of Android mobile devices are analyzed. They also explored the patterns and expressions that indicate the exact position of authentication credentials in a memory dump.Here some special scenarios are considered and almost eighty percent cases the authentication info can be recovered. Although some applications implemented encryption features that are not sufficient. Almost all password format contains string password or pass. With the help some open source forensic tools those can be easily recovered. The analysis of the results revealed that the majority of the considered Android applications are vulnerable to the recovery of authentication credentials from the volatile memory.The mobile-banking applications, have been proved to be vulnerable. We observed that the volatile memory did not contain proper authentication.Taking into account that users tend to reuse password across various websites and applications developers should use correct and secure programming techniques and guidelines.