Advances in Intelligent Systems and Computing; Volume 760, 2019, Pages 421-437; 2nd International Conference on Computer, Communication and Computational Sciences, IC4S 2017; Kathu; Thailand; 11 October 2017 through 12 October 2017; Code 217109

Innovative security techniques to prevent attacks on wireless payment on mobile android OS

1. Cavallari, M.
2. Tornieri, F.
3. de Marco, M.

Università Internazionale Telematica UniNettuno, Rome, Italy

Abstract

Mobile technologies are increasingly pervading a substantial portion of everyday life. In particular, the economic sector of consumers and private sales has shown a very high rate of utilization of mobile applications. Mobile payments are no exception, and the economic development relies more and more on mobile technologies. Bank institutions and financial firms are privileged targets for cyber attacks and organized crime, exploiting vulnerabilities of smart mobile devices in particular for host card emulation wireless payments. The research analysis was based on mobile platform Android and identified ten original (novel) controls that can avoid possible attacks on payment transactions and/or privacy. The study has practical implications as practitioners and organizations, like banks, shall control the risks associated with the taxonomy of tamper IDs. Organizational implications can be regarded as the need for banks to look into software development for mobile applications.