Evaluation of the security capabilities on NFC-powered devices

Antonio J. Jara, Alberto F. Alcolea, Miguel A. Zamora, Antonio F. G. Skarmeta
Department of Information and Communications Engineering Computer Science Faculty, University of Murcia, Murcia, Spain

Abstract

New generation of cellular devices and services are being defined with Near Field Communications (NFC) technology. Cellular phones are being considered to be used as credit card, ID card etc., where our private matters, information, identification and money are being managed. These new services must be reliable in order to protect our privacy. The problem is that NFC is based on RFID, where security was not considered. RFID was defined as a solution limited to identification. The problem arises because the applications of RFID are being extended with NFC to solutions where security needs to be considered, e.g. payment and identification. For this reason, this paper evaluates the security capa-bilities of NFC-powered devices: Smart phones (Google Nexus One), Personal Computer (PC) and Personal Digital As-sistant (Acer N30). Specifically, we are evaluating the capabilities of these devices to carry out asymmetric ciphered based on public key encryption algorithm (RSA). The data overload and latency have been evaluated for different plat-forms and for different key and information lengths. From that analysis was found some throughput problems to carry out asymmetric ciphered in constrained devices such as Pocket PC. For that reason, this paper concludes, proposing a hybrid security scheme to combine security based on asymmetric key encryption algorithm, such as RSA, to exchange a shared key and symmetric encryption algorithm, such as Advanced Encryption Standard (AES), to exchange the data.