World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:10, No:02, 2016

Security Analysis of SIMSec Protocol

Authors : Kerem Ok, Cem Cevikbas, Vedat Coskun, Mohammed Alsadi, Busra Ozdenizci

Abstract : Un-keyed SIM cards do not contain the required security infrastructure to provide end-to-end encryption with Service Providers. Hence, new, emerging, or smart services those require end-to-end encryption between SIM card and a Service Provider is impossible. SIMSec key exchange protocol creates symmetric keys between SIM card and Service Provider. After a successful protocol execution, SIM card and Service Provider creates the symmetric keys and can perform end-to-end data encryption when required. In this paper, our aim is to analyze the SIMSec protocol's security. According to the results, SIM card and Service Provider can generate keys securely using SIMSec protocol.

Keywords : End-to-end encryption, key exchange, SIM card, smart card
Conference Title : ICCCISE 2016 : International Conference on Computer, Communication and Information Sciences, and Engineering
Conference Location : London, United Kingdom
Conference Dates : February 25-26, 2016