Secure Firmware Updates for Point of Sale Terminals

Hippolyte Djonon Tsague Johannes Van Der Merwe Terrence Moabalobelo
Council for Scientific and Industrial Research (CSIR)
Modeling and Digital Science (MDS)
Johannesburg, South Africa
hdjonontsague@csir.co.za

Abstract

A large number of electronic transactions are performed with credit or debit cards at point of sale terminals located at merchant stores. The success of this form of payment however, has an associated cost due to the management and maintenance of the equipment. In particular, there is an important cost related to the deployment of new software upgrades for the point of sale terminals, since in most cases human intervention is required. In this paper, we present a lightweight protocol for secure firmware updates for smart card based point of sale terminals. The protocol has especially been designed with respect to the limited hardware resources in such devices. Also, the low bandwidth and the risk of packet loss in the wireless link have been taken into consideration. The protocol provides data integrity and authenticity protection, and thus prevents an attacker from modifying a firmware in transit and installing malicious firmware in the terminals. In addition, terminals can verify that, the received firmware originated from a trusted source. The protocol includes confidentiality protection, and thus the proprietary firmware is kept secret from attackers.