Security analysis of PEAP protocol using NuSMV tool

Martin Očenáš

iocenas@fit.vutbr.cz

Faculty of information technology
University of technology
Brno, Czech republic

Abstract

PEAP (Protected EAP) is extension of EAP (Extensible Authentication Protocol), which is used for authentication on computer network. It is used for one way authentication against authentication server. For instance 802.1X authentication usually uses some form of EAP. PEAP introduces a TLS into EAP, which creates secure tunnel between authenticating device and authentication server, and also allows using a server certificate. So using PEAP should provide authentication of server and confidentiality and integrity of transferred secret.

PEAP is widespread solution for network authentication os it is important that it has no security issues in it's design. In this article we will present formal analysis of PEAP using NuSMV tool. NuSMV is a symbolic model checker, used for verification of models based on finite state machines. Goal of this verification is to prove that PEAP design holds confidentiality, integrity and authentication with no security issue or find a counterexample that breaks at least one of these security goals.