Towards a Secure and User Friendly Authentication Method for Public Wireless Networks

Carolin Latze

The goal of this thesis was to develop a secure and user friendly authentication scheme for public wireless networks (PWLANs). In contrast to private wireless networks, public wireless networks need a proper authentication scheme for several reasons. First of all, the network operator must be able to identify a user in case an incident happens. Furthermore, such networks are usually controlled by a commercial operator who will hardly allow access for free. This leads to the need for a secure and reliable authentication method. However, the authentication method must be user-friendly too in order to be acceptable. The only "wireless networks" users know so far are cellular networks, which are very easy to use. Users do therefore ask for a comparable experience in public wireless networks. This is obviously not given for the captive portals that are the most common authentication method today. Captive portals use the web browser as an authentication device by blocking all traffic until the first HTTP request is sent. That message redirects the user to the captive portal page where she is asked to give her user credentials. This is obviously rather complicated since the user has to open the browser in any case. Furthermore, captive portals usually carry a lot of advertisements which makes it impossible to automate the login process.

In order to overcome the security and usability problems of captive portals, operators provide EAP-SIM authentication. EAP-SIM uses the SIM credentials for PWLAN authentication. Since people are used to SIM cards due to the cellular networks, the acceptance for this authentication method is high. Furthermore, EAP-SIM provides a good level of security since the user credentials are held within trusted hardware. However, most of the devices used in public wireless networks do not have a SIM slot out of the box which renders EAP-SIM again uncomfortable.

Since the idea to store user credentials in trusted hardware is appealing, this thesis evaluates the Trusted Platform Module (TPM) as an authentication device. The TPM is a small cryptographic module built into almost every new computer. This thesis shows how to use the TPM as an authentication device in EAP-TLS. Furthermore, this thesis shows theoretical and real world evaluations of EAP-TLS with the TPM. It will be shown that this authentication method provides a good level of security as well as good usability.

Jury:
- Prof. Dr. Heinz Groeflin, University of Fribourg, Switzerland (jury president)
- Prof. Dr. Ulrich Ultes-Nitsche, University of Fribourg, Switzerland (PhD supervisor)
- Prof. Dr. Torsten Braun, University of Bern, Switzerland
- Prof. Dr. Rüdiger Grimm, University of Koblenz, Germany