Security analysis in mobile WiFi environment

Péter Orosz, oroszp@delfin.unideb.hu
Zoltán Gál, zgal@cis.unideb.hu
Andrea Karsai, kandrea@fox.unideb.hu

University of Derbrecen, Service Center of Informatics

Abstract

In the world of data communication technologies of local area networks wireless mechanisms are dynamically spreading due to the large scale mobility. Whereas radio transmission reveals complex security issues for the professionals. A high priority issue is that how the currently available (EAP based) authentication mechanisms, encryption (WEP, WPA, WPA2, VPNs) protocols and technologies impact on the transmission parameters of the WiFi system, specially on the duration of roaming that occurs when mobile station passes across radio cells.

We already know from previous analysises that cell change of the mobile station during its physical movement significantly impacts on TCP and UDP traffics as well. Then roaming process occurs at the data-link layer, therefore the mobile station deassociates from the previous AP and reassociates with a new one that has the appropriate signal and transmission parameters in the new cell. At this point the reauthentication plays a key role. Reauthentication feature is included in the advanced EAP mechanisms. We may ask the following questions with reason: How much does the reauthentication increases the period of traffic-loss during roaming, and how does the data loss in the radio physical layer take effect on the behaviour of the upper layers' protocols?

Data encryption protocols (WPA, WPA2) that comply with today's network security requirements dynamically changes user keys. In this paper we analyse the behaviour of the mentioned protocols during roaming events. Analysises performed in the mobile WiFi test environment may give the answer to these questions.