CYSENI 2011, May 26-27, Kaunas, Lithuania
ISSN 1822-7554, www.cyseni.com

ANALYSIS OF THE IEEE 802.11 STANDARD WIRELESS SECURITY THREATS AND SECURITY MECHANISMS

E. Petersons, N. Bogdanovs
Riga Technical University
Lomonosova iela 1, LV-1019 Riga – Latvia

ABSTRACT

High bandwidth wireless local area networks are gaining popularity. Along with this popularity has come a well publicized series of vulnerabilities in the IEEE standard implementations. It is common knowledge, that Wireless LANs based on the 802.11 standard are the most likely candidate to become widely prevalent in corporate environments. With the increasing dependence on wireless LANs businesses and educational institutions are in need of a reliable security mechanism. The latest security protocol, the IEEE 802.11i assures rigid security for WLANs with the support of IEEE 802.1x protocol for authentication, authorization and key distribution.

This white paper describes the generic mechanisms available for authentication of users and the protection of the privacy and integrity of the data. We conduct a basic analysis of each security countermeasure by looking at the attack techniques addressed by the mechanism. Without these features, not only is a WLAN vulnerable, but the entire information infrastructure of which it is a part is at risk.

The security embedded in wireless LAN technologies falls short of providing adequate protection. Early-adopting organizations have found that evaluating, and where possible, mitigating these risks before deploying a wireless LAN is beneficial. Fortunately, this paper addresses the security concerns raised by both current and upcoming 802.11 network technologies.

Keywords: wireless, security, IEEE 802.11, LAN.