Wi-Fi Security Dedicated Architectures

Eduard-Ionuț BOROȘEANU
EUROQUALROM, University POLITEHNICA of Bucharest, Romania
edi_eduard92@yahoo.com

Abstract

This article will emphasize architectures that were designed due to the new business generated by wireless infrastructures. First, authentication issues of wireless users in "hot spot" - also called "captive portal" - architectures will be discussed. Lastly, recent architectures such as WIDS/WIPS (Wireless Intrusion Detection Systems/Wireless Intrusion Prevention Systems) aiming at detecting any malicious wireless activity will be detailed.

Index terms: wireless, attacks, WIDS, hot-spot

References:

[1]. H. Chaouchi, M. Laurent-Maknavicius, Wireless and Mobile Network Security
[2]. K. Curran, Wi-Fi Security
[3]. H. Davis, R. Mansfield, The Wi-Fi Experience: Everyone's Guide to 802.11b Wireless Networking
[4]. J.R. Vacca, Guide to Wireless Network Security
[5]. K. Pahlavan, P. Krishnamurthy, Principles of Wireless Networks: A Unified Approach
[6]. R.K. Nichols, P.C. Lekkas, Wireless Security: Models, Threats and Solutions
[7]. R. Flickenger, Building Wireless Community Networks