Chapter 14
Network Security through Wireless Location Systems

André Peres
Federal Institute of Science and Technology – Rio Grande do Sul, IFRS, Brazil

Raul Fernando Weber
Instituto de Informática, UFRGS, Brazil

EXECUTIVE SUMMARY

The advantage of wireless local area networks, giving the mobile stations the possibility of moving freely inside the network access range comes with a security drawback. The fact that microwave signals can transpose walls and suffers with attenuation, reflections, refraction, diffraction and dispersion, depending of the obstacles, makes very difficult to define the network access range. Without the knowledge of the network boundaries, the network administrator cannot define a physical delimiter to network access. Without the user-location, it is impossible to restrict the network access based on the physical access boundaries defined by the administrator. When the wireless network operates indoor, the many obstacles and the dynamic behavior of these obstacles (some people moving around, for instance) make the microwave signal behavior change the range and aspect of the network. This work proposes a new approach to indoor user-location mechanism, based on the dynamic behavior of the obstacles and consequent changes on network range in IEEE 802.11 networks. Finally a new authentication system WlanAuth, based on the user location is proposed.

INTRODUCTION

When we use wireless networks, our goal is to grant network access with stations mobility and flexibility. The stations must be capable of access the network while moving freely around the access area, without losing connection, and the network physical infrastructure must support the addition of new wireless devices and the disconnection of them without any physical impact.

Because of the behavior of the signal propagation, however, when we compare wireless networks with wired ones, we identify that there are some differences in the management and security aspects that must be considered.

DOI: 10.4018/978-1-60960-015-0.ch014

In wired networks we can easily confine the physical network inside a room or building, according to the network connection points (switch ports and cables). Also, it is easy to segregate different subnets in the same building, in separate rooms or areas using routers and/or firewalls.

When we have a minimal IP address organization (subnet oriented), it is easy to determine the physical location of a station, only analyzing the IP address information.

In wireless networks, the physical coverage area is difficult to define due to the microwave signals behavior. The reflection, refraction, diffraction, scattering, attenuation and multi-path, distribute the coverage area with non-uniform patterns. The network access area is defined by the obstacles that the microwave signal encounters in the environment.

This means that the network physical access area definition is not possible in a easy way, and a wireless station can capture the network signals even outside the building.

Related to segregation, besides the fact that the WLAN (Wireless Local Area Networks) IEEE802.11 uses multiplexed channels to deliver different networks in the same environment, the responsibility of channel selection relies on the wireless station. This means that the network manager can not control the subnet in which a client tries to connect.

Because of the mobility, the wireless stations can be in any place inside the coverage area. This means that only by analyzing network data, it is not possible to locate the device. A malicious stations can be anywhere inside (or outside) the building.

In order to conceive a wireless network with the minimum of security, the IEEE presents some mechanisms to achieve device authentication and data privacy in IEEE802.11 networks. The data privacy is achieved by one of the mechanisms IEEE (1999), IEEE (2003), IEEE (2004):

- *WEP*: Wired Equivalent Privacy. It is a symmetric cryptography protocol (same key to cypher and decipher the data) base in the RC4 algorithm;
- *WPA*: Wireless Protected Access. Based in the WEP algorithm, but with temporal keys - TKIP (Temporal Key Integrity Protocol). Can be used with an initial pre-shared-key (PSK) or with 802.1x protocol;
- *WPA2*: or IEEE802.11i. It uses the AES cryptography algorithm, which is much more robust than WEP and WPA. It also can be used with a PSK or 802.1x.

WEP was proven by Fluhrer (2001) to have security vulnerabilities based on weak keys generated by the cryptography algorithm. The WPA tries to overcome this vulnerabilities through TKIP, changing the shared secret from time to time. It is possible to break WPA by capturing the authentication packets and discovering the first key (pre-shared key) through brute force Moskowitz (2003).

Because WPA2 uses AES, it is considered the more robust cryptography protocol for IEEE802.11 networks.

The authentication can be made trough the protocols Gast (2002):

- *open system*: the station submits an authentication request, and the access point always returns a success response. This means that open system is a null authentication protocol as all stations are always accepted;
- *shared key*: the station submits an authentication request. The AP (Access Point) generates a challenge (random text) e sends it to the station. The station must then cipher the challenge with the WEP algorithm, and returns the result to the AP. The AP then verifies that the station knows the shared key.
- *802.1x*: uses a RADIUS server in order to identify the user with user/password challenge. The AP manages a communication