Wireless Security

Meletis Belsis
Telecron, Greece

Alkis Simitsis
National Technical University of Athens, Greece

Stefanos Gritzalis
University of the Aegean, Greece

INTRODUCTION

The fast growth of wireless technology has exponentially increased the abilities and possibilities of computing equipment. Corporate users can now move around enterprise buildings with their laptops, PDAs, and WiFi; enable VoIP handsets; and retain communications with their offices. Business users can work from almost anywhere by attaching their laptops to WiFi hotspots and connecting to their corporate network. However, not many enterprises know and understand the potential security vulnerabilities that are introduced by the use of WiFi technologies. Wireless technologies are insecure by their nature. Anyone with the appropriate hardware can steal information transmitted using the airwaves. This article discusses the security vulnerabilities that are inherited in wireless networks. Also, it provides a description of the current security trends and protocols used to secure such WiFi networks along with the problems from their application.

BACKGROUND

Currently, several enterprises consider information security as a monolithic architecture, in which simply they install a firewall or an intrusion detection system. Unfortunately security is not a single device or software:

> *In the real world, security involves processes. It involves preventive technologies, but also detection and reaction processes, and an entire forensics system to hunt down and prosecute the guilty. Security is not a product; it itself is a process.* (Schneier, 2000)

The above definition represents the fact that total protection of corporate networks goes beyond a firewall engine. Each appliance that is added and/or changed into a system should incorporate the re-designing of a system's overall security policy and infrastructure. The same principle exists when incorporating wireless devices to extend the overall enterprise architecture. Deploying a wireless network has as a consequence the change of the security risks and needs of the entire network infrastructure. Nowadays, the techniques that are used for the realization of attacks in wireless connected networks resemble those used to target common LANs. In the next paragraphs, we present the major categories of attacks, including techniques that have been successfully used for attacking corporate wireless networks.

Denial of Service. In their simplest form, an adversary can continuously transmit *association request* packets. Such action could render an access point unavailable to authorized users. Adversaries can use a powerful RF transceiver to transmit amplified signals in all frequency band frequencies (channels), creating an interjection that prevents the communication of terminals with the corporate access points (RF Jamming). Such an attack could be easily deployed from the outside premises of an enterprise (e.g., parking). An example appliance that can be used for the concretization of this attack is the Power Signal Generator (PSG -1) by the YDI.

Man-in-the-Middle Attacks. Combining an RF Jamming attack with the use of a portable computer and necessary software, an attacker can easily steal or alter corporate information (Akin, 2003). The adversary will use a denial-of-service attack to force authorized terminals connected to a corporate access point to identify and roam to an access point with better signal than the one already connected to. Using this predetermined behavior the attacker can masquerade his/her laptop as an access point and force all wireless clients to connect to it. By using this technique an adversary can intercept all wireless communications links and read or alter information on them.

Fresnel Zone Sniffing. Stealing information from point-to-point wireless links is difficult. The attacker needs to calculate the link path and identify ways to attach its laptop to the link's Fresnel Zone.

Rogue Wireless Gateways. A rogue wireless gateway is a security vulnerability that is detected in many of today's enterprise networks. A rogue wireless gateway is an unauthorized access point that is installed on an enterprise network. Such access points are usually installed by corporate users, to assist them in the everyday work (i.e., transfer files/e-mails from a desktop to a laptop computer). Unfortunately enterprise users do not know and understand the security implications of installing a wireless device on a system. Leaving such devices connected to the corporate network provides an opportunity to adversaries to connect and steal corporate information.

Ad Hoc Networks. The 802.11 protocol specification allows wireless terminals to interconnect without the use of an access point. This mode of operation is called ad hoc. Unfortunately many of today's corporate users enable the ad hoc facility on their laptops and PDAs either accidentally or deliberately in order to exchange files with other users. Enabling the ad hoc mode without deploying the necessary security procedures (i.e., encryption and authentication) could seriously damage corporate security. Adversaries can search for such unprotected ad hoc networks and connect to those. From there adversaries can either read the locally stored corporate information, or if the user's device is connected to the corporate networks (i.e., LAN, dialup, and VPN), access the corporate resources (Papadimitratos & Haas, 2002).

The previous example attacks emphasize the need for security that results from the use of wireless technology. The problem of security becomes more apparent when the technology of wireless networking is applied in government-owned systems. The need for security in those systems is extensive due to the legislation on personal data protection and the human lives factors involved.

MAIN THRUST OF THE ARTICLE

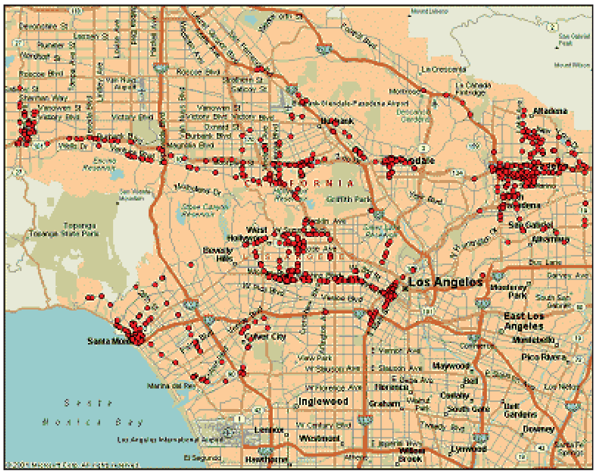
In the last few years, the computing and telecommunications community has realized the necessity of deploying security controls on wireless networks. Unfortunately most of today's wireless security controls have been proven unsafe or managerial infeasible to maintain. The next few paragraphs describe the most common security protocols and techniques, as well as their vulnerabilities.

Discovering Wireless Networks

Many enterprises support their notion of using insecure WiFi networks based on the idea that their *small wireless networks* are hidden from hackers and adversaries. This notion is called Security through Obscurity, and is something that the IT security community analyzed and abolished long before the appearance of wireless networks.

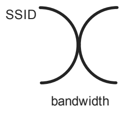
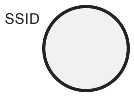
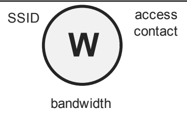
Modern hackers have invented a number of new techniques, collectively known as *War Driving* or *War Chalking,* which aim at discovering unprotected wireless networks. An adversary uses a laptop computer, along with appropriate discovery software (i.e., NetStumbler) and a GPS received, to pinpoint the exact location of access points on a map. Today such maps are distributed among the War Driving community. It is not unusual for enterprises to discover their company access points on maps found on War Driving Web sites (see Figure 1).

Figure 1. A War Driving result in Los Angeles



Many enterprise administrators try to hide their wireless networks by activating the *close system* option found on access point hardware equipment. This option prohibits the access point from transmitting the network's beacon information that incorporates the network's service set identifier (SSID). Unfortunately the SSID is incorporated into almost all network management frames. Software packages like

Table 1. War Chalking symbols

node	symbol
open node	
closed node	
WEP node	 SSID access contact W bandwidth