Chapter 1.2
Introduction to Basic Concepts and Considerations of Wireless Networking Security

Carlos F. Lerma
Universidad Autónoma de Tamaulipas, Mexico

Armando Vega
Universidad Autónoma de Tamaulipas, Mexico

INTRODUCTION

Local networks have been, from the beginning, a controversial topic. The organizations that have implemented these types of networks have shown their concern about their levels of security. Ever since the discovery of vulnerabilities among first-generation wireless networks (Borisov, Goldberg, & Wagner, 2001), analysts and security companies have tried to understand and mitigate those risks. Some of those efforts have contributed towards the study of wireless security. Other efforts have failed, presented a different group of vulnerabilities, or require expensive proprietary software and hardware. Finally, other efforts try to mitigate the problem piling up a complex group of security technologies, like virtual private networks.

Despite the benefits they bring, a great number of concerns related to security have limited the massive adoption of wireless networks, particularly in sectors that are highly aware of the existing security risks such as the financial and government sectors. Even though there are a significant number of risks inherent to the mass transmission of data to any individual within the boundaries of a wireless network, a good amount

DOI: 10.4018/978-1-61350-323-2.ch1.2

of these are installed without any security measure at all. However, the majority of businesses that have implemented some sort of wireless security measures have done so in the most rudimentary way, bringing a false sense of security to users.

When the first IEEE 802.11 wireless standards were in the phase of development, security was not as important as it is today. The level of complexity of network threats was much lower and the adoption of wireless technologies was still in an introductory phase. It was under these circumstances that the first standard for wireless network security, known as wired equivalent privacy (WEP), was originated. WEP underestimated the necessary means to turn air security into an element equivalent to the security provided by a cable. In contrast, the security methods of modern wireless networks are designed to work in hostile environments where there is a lack of well-defined physical network perimeters.

BACKGROUND

Every network environment is susceptible to risks, and wireless networks are not the exception. According to a survey by the Federal Bureau of Investigation of the United States, the only category of threats that shows a significant increase in number of attacks and/or possibility of misuse in the last few years is "wireless network abuse." The broadcasting nature of these networks has turned them into perfect targets for nonauthorized users.

According to Arbaugh (2001), these problems are exacerbated by the myriad of free security-threatening tools widely available for download on the Internet and because of the inherent vulnerabilities of wireless networks themselves. One of the most exploited vulnerabilities is the WEP protocol (Fluhrer, Mantin, & Shamir, 2002; Peikari & Forgie, 2002), which is such a severe problem that many companies have decided to abandon the wireless business.

On the other hand, a good amount of the deployment strategies of wireless networks lack a cohesive and effective integration with the authentication services infrastructure of the organization in which they are implemented (Arbaugh & Shankar, 2002). This common mistake is easy to mitigate, and its correction is evident almost immediately by closing the gap between the number of authorized and unauthorized users. This is evident because authorized users are checked against a database with secure access methods inside the wired network.

In other cases, security problems go beyond the merely technological element (National Institute of Standards and Technology, 2007). Commonly, the lack of planning of the wireless network is a decisive coverage and placement factor. Other elements, such as security policies, access procedures, internal policies governing the use of and access to resources and guidelines governing confidentiality and protection of information serve as a complementary regulatory framework that provides support to the technological infrastructure, establishing limitations related to the way in which information is and/or should be used.

TECHNOLOGICAL ANALYSIS

Wireless networks have experienced a rising trajectory in the last 8 years. Basically, access to wireless technology (access points, wireless network cards) has become easier due to relatively low equipment prices and easiness to set up equipment. Many pieces of network equipment are advertised under the commercial designation SOHO (small office home office), whose installation in inherently simple to carry out due to the fact that the people who purchase those pieces of equipment are relatively new to network equipment installations or users with basic computer skills.

Current advantages of implementing a wireless network include (Planet3 Wireless, 2005):