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 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):

- Availability: Members of an organization can have access to information resources anywhere without depending on a wired infrastructure.
- Mobility: A user can go from one place to another inside a building or between buildings without leaving the network's coverage area while still having access to network resources. This characteristic trait poses one of the main advantages and threats to wireless networks.
- Productivity: Due to the fact that wireless networks can provide a connection virtually anywhere, this feature enables users to keep working no matter where they are. This feature gains a significant value when wireless networks are implemented in the business sector, due to factors like access to business information and management information systems.
- Ease of installation: A wireless network can be deployed in a matter of minute,s and can be transferred from one place to another as fast as it was set up in the first place. Basically, this advantage tends to be more noticeable in networks with a steady level of permanence and low level of complexity. However, ease of installation does not mean that important security and planning aspects should be omitted, such as carrying out a site survey, and the configuration of security protocols and authentication methods.
- Scalability: Wireless networks can rapidly adapt to an increasing population of users. To achieve this, a network administrator needs less pieces of wireless equipment than wired equipment. Scalability should also be determined before installation of a network, due to the fact that an administrator needs to know an estimated number of the users that will be connecting to the network and the number of pieces of equipment that will support those users, as well as the applications that will be supported by the network.
- Cost: Even though wireless network equipment is more expensive than their wired counterparts, their prices are still reasonable for the home user. Enterprise-scale equipment tends to be extremely expensive, but it comes preloaded with advanced security and management features, is built to be used outdoors, and can support a bigger amount of users.

On the other hand, wireless networks have clear disadvantages that are a result of their own nature (LaRocca & LaRocca, 2002). Generally, they can be:

- Security: Aided with proper equipment and pertinent knowledge concerning the basic operation of a wireless network, any person can capture information that travels through the air, product of a wireless transmission. For an intruder, it is only needed to position oneself within a relative close distance to the network from which one can have an acceptable level of signal reception and possess the tools needed to perform the decryption of the information.
- Distance: The coverage area of wireless networks used today is considered in tens of meters (taking into account that most networks used in infrastructure mode are part of the 802.11 standard). It is necessary to acquire and install accessories and equipment, such as antennas and repeaters, in order to further enhance the coverage area of the network.
- Reliability: Wireless technology is subject to the effects of interference, the environment, and terrain features. Most of the times, an administrator can deal with these phenomena, but it is an undeniable fact that their effects are strongly felt, producing unpleasant results and undermining network performance (in different degrees).
- Speed: Wireless network speed is low by nature, and it is not comparable to those of wired networks, which offer speeds and transfer rates much more advanced than wireless networks. Even though special components can be used to increase the speed and performance of a wireless network, this cannot be translated to higher transfer rates and increased speed, which is still a major disadvantage.

By analyzing disadvantages, it can be concluded that security is, without a doubt, the most important of them all when it comes to wireless networks, and is the one factor that originates the higher amount of challenges. Even though reliability is an area where antenna design and other important areas are put to better use, and are of extreme importance to the development of new generations of networks, security takes a more dynamic posture. A solution has not fully matured when there is a new problem to solve and a new countermeasure to develop. Wireless security is seen as a modular problem, that is, or can be solved by integrating several technologies.