Chapter 3.21
Exposing the Wired Equivalent Privacy Protocol Weaknesses in Wireless Networks

Kevin Curran
University of Ulster at Magee, UK

Elaine Smyth
University of Ulster at Magee, UK

ABSTRACT

This article highlights a number of security issues within wireless networks. Signal leakage for instance, means that network communications can be picked up outside the physical boundaries of the building in which they are being operated, meaning that a hacker can operate from the street outside or discretely from blocks away. In addition to signal leakage, the Wired Equivalent Privacy (WEP) protocol is inherently weak. There are also various other attacks that can be initiated against WLANs, all with detrimental effects. During our investigation, a war-driving expedition was conducted to ascertain the number of unprotected WLAN devices in use locally. We concluded that there was an apparent and serious lack of security on WLAN devices. Even those users that have implemented WEP do not seem to realize just how weak this protocol is or how their networks could be affected.

INTRODUCTION

On the surface, WLANs act the same as their wired counterparts, transporting data between network devices. However, there is one fundamental and quite significant difference: WLANs are based upon radio communications technology as an alternative to structured wiring and cables. Data are transmitted between devices through the air by utilizing the radio waves. Devices that participate

in a WLAN must have a Network Interface Card (NIC) with wireless capabilities. This essentially means that the card contains a small radio device that allows it to communicate with other wireless devices within the defined range for that card (e.g., the 2.4-2.4853 GHz range). In order for a device to participate in a wireless network, first it must be permitted to communicate with the devices in that network, and second, it must be within the transmission range of the devices in that network.

To communicate, radio-based devices take advantage of electromagnetic waves and their ability to be altered in such a manner that they can carry information (called modulation. Information is transferred by mixing the electromagnetic wave with the information to be transmitted. At the receiving end, the signal is compared to an unmodulated signal to reverse the process (called demodulation). There are three main types of modulation techniques: Amplitude Modulation (AM), Frequency Modulation (FM), and Phase Modulation (PM). Because FM is more robust against interference, it was chosen as the modulation standard for high frequency radio transmissions (Harte, 2000).

Radio devices utilized within WLANs operate in the 2.4-2.4845GHz range of the unlicensed Industrial Scientific and Medical (ISM) frequency band, using either Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS), which are special modulation techniques used for spreading data over a wide band of frequencies, sacrificing bandwidth to gain signal-to-noise (S/N) performance (Harte, 2000).

WLAN Network Modes

Wireless devices have the option of participating in two types of networks: ad hoc and infrastructure. An ad hoc (also known as peer-to-peer) network is the simplest form of WLAN. It is composed of two or more nodes communicating without any bridging or forwarding capability; all nodes are of equal importance, and may join and leave the network at any time, each device also has equal right to the medium. Access Points (APs) are not necessary. For this to work, the devices wishing to participate in an ad hoc network must be within transmission range of each other; when a nodes goes out of range, it will lose connection with the rest of the devices. The range of this type of network is referred to as a *single cell* and is called an Independent Basic Service Set (IBSS) (Tourrilhes, 2000).

In an infrastructure network, communications take place through an AP in a many-to-one configuration with the AP at the single end. In its simplest form, it consists of one AP and a group of wireless clients/devices, which must be within transmission range of the AP and be properly configured to communicate with the AP. This type of network is called a Basic Service Set (BSS) (Sikora, 2003). If two or more BSSs are operated in the same network by linking the APs via a background network, it is called an Extended Service Set (ESS). Such a configuration can cover larger, multi-floor, buildings. However, support is required for roaming between different APs on the network, which is the hand-off between a device leaving one AP's range and going into the range of another AP (Geier, 1999).

APs can overlap if they are each given a different channel within the 2.4-2.4835GHz range on which to communicate. There are 11 overlapping frequencies specified in IEEE 802.11, which means that, with careful planning, multiple networks can co-exist in the same physical space without interfering with each other (Tourrilhes, 2000). APs also must be configured with a Service Set Identifier (SSID), also known as the network name. It is a simple 1-32 byte alphanumeric string given to each ESS that identifies the wireless network and allows stations to connect to one desired network, when multiple independent networks operate in the same physical area. It also provides a very basic