Wireless Network Security

Kevin Curran
University of Ulster, Northern Ireland

Elaine Smyth
University of Ulster, Northern Ireland

INTRODUCTION

Wireless networks have a number of security issues. Signal leakage means that network communications can be picked up outside the physical boundaries of the building in which they are being operated, meaning a hacker can operate from the street outside or discretely from blocks away. In addition to signal leakage, the wired equivalent privacy protocol is inherently weak, and in addition to WEP's weaknesses, there are various other attacks that can be initiated against WLANs, all with detrimental effects. 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 on radio communications technology as an alternative to structured wiring and cables. Data is 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, for example, the 2.4-2.4853 GHz range. For a device to participate in a wireless network, it must firstly be permitted to communicate with the devices in that network, and secondly 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, known as modulation (Sundaralingham, 2004). Here we discuss wireless security mechanisms.

BACKGROUND

Wired networks have always presented their own security issues, but wireless networks introduce a whole new set of rules with their own unique security vulnerabilities. Most wired security measures are just not appropriate for application within a WLAN environment; this is mostly due to the complete change in transmission medium. However, some of the security implementations developed specifically for WLANs are also not terribly strong. Indeed, this aspect could be viewed as a *work-in-progress*; new vulnerabilities are being discovered just as quickly as security measures are being released. Perhaps the issue that has received the most publicity is the major weaknesses in WEP, and more particularly the use of the RC4 algorithm and relatively short initialization vectors (IVs). WLANs suffer from all the security risks associated with their wired counterparts; however, they also introduce some unique risks of their own. The main issue with radio-based wireless networks is signal leakage. Due to the properties of radio transmissions, it is impossible to contain signals within one clearly defined area. In addition, because data is not enclosed within cable, it makes it very easy to intercept without being physically connected to the network (Hardjono & Lakshminath, 2005). This puts it outside the limits of what a user can physically control; signals can be received outside the building and even from streets away. Signal leakage may not be a huge priority when organizations are implementing their WLAN, but it can present a significant security issue, as demonstrated below. The signals that are transmitting data around an organization's office are the same signals that can also be picked up from streets away by an unknown third party. This is what makes WLANs so vulnerable. Before WLANs became common, someone wishing to gain unauthorized access to a wired network had to physically attach themselves to a cable within the building. This is why wiring closets should be kept locked and secured. Any potential hacker had to take great risks to penetrate a wired network. Today potential hackers do not have to use extreme measures, there's no need to smuggle equipment on site when it can be done from two streets away. It is not difficult for someone to obtain the necessary equipment; access can be gained in a very discrete manner from a distance.

WIRELESS SECURITY MECHANISMS

To go some way towards providing the same level of security the cable provides in wired networks, the wired equivalent protocol (WEP) was developed. WEP was designed to provide the security of a wired LAN by encryption through use of the RC4 (Rivest Code 4) algorithm. Its primary function is to safeguard against eavesdropping (sniffing), by making the data that is transmitted unreadable by a third party who does

not have the correct WEP key to decrypt the data. RC4 is not specific to WEP, it is a random generator, also known as a key stream generator or a stream cipher, and was developed in RSA Laboratories by Ron Rivest in 1987 (hence the name Rivest Code). It takes a relatively short input and produces a somewhat longer output, called a pseudo-random key stream. This key stream is simply added modulo two that is exclusive ORed (XOR), with the data to be transmitted, to generate what is known as ciphertext (Briere, 2005).

WEP is applied to all data above the 802.11b WLAN layers (physical and data link layers, the first two layers of the OSI reference model) to protect traffic such as transmission control protocol/Internet protocol (TCP/IP), Internet packet exchange (IPX), and hyper text transfer protocol (HTTP). It should be noted that only the frame body of data frames are encrypted, and the entire frame of other frame types are transmitted in the clear, unencrypted (Karygiannis & Owens, 2003). To add an additional integrity check, an initialization vector (IV) is used in conjunction with the secret encryption key. The IV is used to avoid encrypting multiple consecutive ciphertexts with the same key, and is usually 24 bits long. The shared key and the IV are fed into the RC4 algorithm to produce the key stream. This is XORed with the data to produce the ciphertext; the IV is then appended to the message. The IV of the incoming message is used to generate the key sequence necessary to decrypt the incoming message. The ciphertext, combined with the proper key sequence, yields the original plaintext and integrity check value (ICV) (Hardjono & Lakshminath, 2005). The decryption is verified by performing the integrity check algorithm on the recovered plaintext and comparing the output ICV to the ICV transmitted with the message. If it is in error, an indication is sent back to the sending station. The IV increases the key size, for example, a 104-bit WEP key with a 24-bit IV becomes a 128-bit RC4 key. In general, increasing the key size increases the security of a cryptographic technique. Research has shown that key sizes of greater than 80 bits make brute force[1] code breaking extremely difficult. For an 80-bit key, the number of possible keys—10^24, which puts computing power to the test; but this type of computing power is not beyond the reach of most hackers. The standard key in use today is 64 bit. However, research has shown that the WEP approach to privacy is vulnerable to certain attacks regardless of key size (Karygiannes & Owens, 2003). Although the application of WEP may stop casual sniffers, determined hackers can crack WEP keys in a busy network within a relatively short period of time.

WEP's Weaknesses

When WEP is enabled in accordance with the 802.11b standard, the network administrator must personally visit each wireless device in use and manually enter the appropriate WEP key. This may be acceptable at the installation stage of a WLAN or when a new client joins the network, but if the key becomes compromised and there is a loss of security, the key must be changed. This may not be a huge issue in a small organization with only a few users, but it can be impractical in large corporations, which typically have hundreds of users (Gavrilenko, 2004). As a consequence, potentially hundreds of users and devices could be using the same, identical key for long periods of time. All wireless network traffic from all users will be encrypted using the same key; this makes it a lot easier for someone listening to traffic to crack the key, as there are so many packets being transmitted using the same key. Unfortunately, there were no key management provisions in the original WEP protocol.

A 24-bit initialization vector WEP is also appended to the shared key. WEP uses this combined key and IV to generate the RC4 key schedule; it selects a new IV for each packet, so each packet can have a different key (Walker, 2002). Mathematically there are only 16,777,216 possible values for the IV. This may seem like a huge number, but given that it takes so many packets to transmit useful data, 16 million packets can easily go by in hours on a heavily used network. Eventually the RC4 algorithm starts using the same IVs over and over. Thus, someone passively *listening* to encrypted traffic and picking out the repeating IVs can begin to deduce what the WEP key is. Made easier by the fact that there is a static variable (the shared key), an attacker can eventually crack the WEP key (Nakhjiri, 2005). For example, a busy AP, which constantly sends 1,500 byte packets at 11Mbps, will exhaust the space of IVs after 1,500 x 8/(11 x 10^6) x 2^24 = 18,000 seconds, or 5 hours. (The amount of time may actually be smaller since many packets are less than 1,500 bytes). This allows an attacker to collect two ciphertexts that are encrypted with the same key stream. This reveals information about both messages. By XORing, two ciphertexts that use the same key stream would cause the key stream to be cancelled out and the result would be the XOR of the two plaintexts (Vines, 2002).

War-Driving

So called *war-driving* is a term used to describe a hacker who—armed with a laptop, a wireless NIC, an antenna, and sometimes a GPS device—travels, usually by car, scanning or sniffing for WLAN devices, or more specifically unprotected or *open* and easily accessed networks. The name is thought to have come from another hacking technique called war-dialing, where a hacker programs a system to call hundreds of phone numbers in search of a poorly protected computer dial-up (Nakhjiri, 2005). Due to the increased use of WLANs in recent years, it is quite possible that the number of unsecured devices has also risen in tandem, thus providing potential hackers with more choice. After all that has been written about the insecurities of WLAN, some users/organizations still insist on implementing them with their