

# SECURING WIRELESS LOCAL AREA NETWORKS (WLAN)

by Reto Baumann

<http://security.rbaumann.net>

June 2002

## ABSTRACT

Wireless Local Area Networks (WLANs) are faster, more manageable and more interoperable than ever. Connecting to the network everywhere in a building can be a competitive gain and boost productivity. Unfortunately, most WLANs aren't adequately secured (or secured at all). This paper presents a kind of checklist to assure a certain level of security and get an optimum out of wireless networks. Even then, WLANs aren't completely secure. The implemented security standard Wired Equivalent Privacy (WEP) has some serious security flaws and can be successfully attacked in very little time. Several possibilities exist to circumvent these flaws and improve a WLANs security.

This paper will introduce a checklist for WLANs, to further secure them. Possibilities to secure WLANs to a level which is comparable to wired networks are presented.

## **OVERVIEW**

A WLAN has several new security problems compared to a wired network. The traditional parts of LAN security come into play as well as some new aspects. The biggest problem with every wireless technology is its range. Depending on weather conditions, buildings, antennas and strength of the signal, wireless technologies have different range of coverage. This invisible signal introduces some completely new opportunities to attack a network - no physical attachment is needed.

In the following chapters, different aspects of a WLAN security will be presented. These improvements are either based on settings or new services on the WLAN or network side (LAN). The third part will discuss alternatives to WEP to overcome its flaws.

## **SECURITY ON THE WLAN SIDE**

Securing a wireless network starts by configuring the WLAN to be as secure as possible. Multiple possibilities exist to improve the security and make it more difficult for an attacker.

### **Enable WEP**

It is well known, that WEP doesn't deliver real security. Several flaws in the design and implementation (see chapter WEP risks) introduces some serious attack possibilities. Never the less, it is important to make the best out of WEP. Not enabling WEP at all is certainly even worse than having a not so good encryption. Some statistics show that more than 50% of WLANs don't encrypt their traffic at all. Most vendors ship their access points with default settings set to use no encryption. The best practice is to enable 128bit WEP and change the keys frequently. Consider using 802.11b products with dynamic key generation. Enabling WEP encryption won't stop a determined hacker, but it will deter some untalented species.

Another important aspect of enabling WEP is more of a legal issue. It's very hard to sue somebody for accessing data, which wasn't secured at all. Having WEP shows the attackers attempt to access data which was encrypted and therefore wasn't meant for his eyes.

### **Change SSID**

The Service Set Identifier (SSID) is used to as a network ID which is attached to every packet. With this identifier, several independent networks can be configured. One common security mistake is not to change the default SSID. It is not a good idea to create the SSIDs with valuable information, as building number. An attacker can easily find out, which building houses sensitive data (like the financial department). Using some hard to guess and as long as possible SSIDs helps to improve a certain level of security. Changing the SSIDs from time to time can also help. Although security through obscurity is never a successful idea, it helps to slow down an attacker.

## **Broadcast**

Most access points broadcast their SSID with every second packet to make it easier and faster for new clients to associate to the network. Some vendor systems allow to disable SSID broadcast. New clients then have to probe if their SSID is available. The number of SSID broadcasts is minimized considerably - a broadcast only takes place, when a new clients tries to join the network. Obtaining the used SSID becomes harder as less broadcasts packets are on the network.

## **Access Point Location**

If possible, place access points in the center of the desired perimeter. Don't place them just behind windows as the active perimeter will be expanded outside your building and the signal is readable further away. By placing the access point in an optimal location, so that the signal only reaches intended places, the danger of eavesdropping can be reduced.

## **Lock Management Interfaces**

Check access points for management interfaces and lock their access. There is not much sense in having a hard guessable SSID and enabled WEP security when an attacker can gain entry to the access point and read or change these settings.

## **DHCP**

Most WLANs use DHCP. A new client can be configured easier and the environment can adapt automatically to disappeared and new clients. Keeping track of already used IPs as well as duplicate IP addresses on the network don't occur any more as the system takes care of distributing unique IP addresses. DHCP is handy, but makes it very easy for an attacker to gain full access as soon as he has the right SSID. It is advisable to use static IPs rather than DHCP.

## **MAC-based Access Restrictions**

Most access points have MAC-based access control lists. Once a MAC-address is listed in the accept group, all packets from this client are accepted by the access point and forwarded onto the network. Companies should track their equipment and enable access for their distributed wireless NICs. Should a NIC be stolen or lost, this MAC-address should be added to the deny list. The access point will then discard every packet from that MAC-address. These access restrictions only apply when active actions are performed, therefore sending packets onto the LAN. Receiving packets is always possible as this is a passive action which can't be controlled or detected by the access point.

As all these entries show, WLANs have several points where improvements are possible. Although, a WLAN can't still be considered to be as secure as a wire-based LAN. The shown steps help to improve the overall security, but all these precautions won't help to secure a WLAN to a sophisticated level of security.

## **SECURITY ON THE NETWORK SIDE**

As seen in the previous chapter, a WLAN can't be secured as good (or easily) as a wired network. By using some precautions on the network side, the danger for the whole net (not the transmitted data) can be minimized. The next chapters show some ideas and possibilities which help to secure a LAN against a WLAN segment. As a basic principle, a WLAN should be regarded like the Internet.

### **DMZ and Firewall**

A WLAN access point should be placed in a demilitarized zone (DMZ). This could be the already present DMZ from a network setup or even a specially created DMZ just for the WLAN. All packets from the WLAN should be considered to be hostile and the network is non trustable. Using a firewall between the company LAN and the WLAN enables the concept of a DMZ specially for the wireless network. Setting up rules that enable access only for known MAC and/ or IP addresses. This is no perfect solution, as these addresses can be spoofed or cloned, but an attacker has to be more sophisticated to exploit these vulnerabilities and it will deter or slow down his attempt.

### **Intrusion Detection System**

How does one know if an attacker already attack a system? Was his attack even successful or was the security tight enough to deny entry? The use of an intrusion detection system (IDS) can be a great tool to discover an intruder or an attempt to access a system. Monitoring the traffic from and to a wireless network can reveal some security or design flaws and help to improve the overall system security. An operational IDS is only as good as his operators who analyze the log files which in turn is a time costly task. Having an IDS only makes sense if the log files are evaluated on a regular basis.

### **Virtual Private Network**

To get a better encryption for the traffic which is sent to a wireless client, it is possible to use a virtual private network (VPN). As it is possible to use a VPN for the insecure Internet, it would be possible to use a VPN for the wireless network. All traffic is encrypted and all advantages of a VPN can be used. The cost for building up a working VPN solution can be high and time consuming. But once the VPN works is installed, the secured wireless network can be used without worrying about the security of the transmitted data.

## **PROBLEMS WITH WEP AND POSSIBLE ALTERNATIVES**

The implementation to provide security in WLANs in the 802.11b standard is called Wired Equivalent Privacy (WEP). The idea was to provide the same security as if wires were used. WEP relies on a secret key which is shared between the mobile client and access point. The secret key is used to encrypt packets before they are sent and an integrity check is used to prevent alteration of packets while in traffic. Most installations use single keys which have to

be distributed manually. More sophisticated mechanisms could be used to prevent some attacks.

## WEP Risks

Unfortunately, WEP wasn't implemented correctly which leads to some serious security flaws. These enable the following attacks

- ◆ Passive attacks to decrypt traffic
- ◆ Active attacks to insert new traffic from unauthorized sources
- ◆ Active attacks on the wireless access point to decrypt traffic
- ◆ Dictionary-building attack that, after analysis of about a day's worth of traffic, allows real-time automated decryption of all traffic.

These vulnerabilities clearly show that WEP can be considered to be secure. Tools for exploiting these flaws can be easily found on the Internet. No in-depth knowledge is necessary to successfully attack a wireless network.

## Short Problem Description

*“WEP uses the RC4 encryption algorithm, which is known as a stream cipher. A stream cipher operates by expanding a short key into an infinite pseudo-random key stream. The sender XORs the key stream with the plaintext to produce ciphertext. The receiver has a copy of the same key, and uses it to generate identical key stream. XORing the key stream with the ciphertext yields the original plaintext.*

*This mode of operation makes stream ciphers vulnerable to several attacks. If an attacker flips a bit in the ciphertext, then upon decryption, the corresponding bit in the plaintext will be flipped. Also, if an eavesdropper intercepts two ciphertexts encrypted with the same key stream, it is possible to obtain the XOR of the two plaintexts. Knowledge of this XOR can enable statistical attacks to recover the plaintexts. The statistical attacks become increasingly practical as more ciphertexts that use the same key stream are known. Once one of the plaintexts becomes known, it is trivial to recover all of the others.*

*WEP has defenses against both of these attacks. To ensure that a packet has not been modified in transit, it uses an Integrity Check (IC) field in the packet. To avoid encrypting two ciphertexts with the same key stream, an Initialization Vector (IV) is used to augment the shared secret key and produce a different RC4 key for each packet. The IV is also included in the packet. However, both of these measures are implemented incorrectly, resulting in poor security.*

*The integrity check field is implemented as a CRC-32 checksum, which is part of the encrypted payload of the packet. However, CRC-32 is linear, which means that it is possible to compute the bit difference of two CRCs based on the bit difference of the messages over which they are taken. In other words, flipping bit  $n$  in the message results in a deterministic set of bits in the CRC that must be flipped to produce a correct checksum on the modified message. Because flipping bits carries through after an RC4 decryption, this allows the attacker to flip arbitrary bits in an encrypted message and correctly adjust the checksum so that the resulting message appears valid.*

*The initialization vector in WEP is a 24-bit field, which is sent in the cleartext part of a message. Such a small space of initialization vectors guarantees the reuse of the same key stream. A busy access point, which constantly sends 1500 byte packets at 11Mbps, will exhaust the space of IVs after  $1500 \cdot 8 / (11 \cdot 10^6) \cdot 2^{24} = \sim 18000$  seconds, or 5 hours. (The amount of time may be even smaller, since many packets are smaller than 1500 bytes.) This allows an attacker to collect two ciphertexts that are encrypted with the same key stream and perform statistical attacks to recover the plaintext. Worse, when the same key is used by all mobile stations, there are even more chances of IV collision. For example, a common wireless card from Lucent resets the IV to 0 each time a card is initialized, and increments the IV by 1 with each packet. This means that two cards inserted at roughly the same time will provide an abundance of IV collisions for an attacker. (Worse still, the 802.11 standard specifies that changing the IV with each packet is optional!)” - Source is a study of the University of Berkeley about the security of WEP. For more details see <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>.*

### **Possible alternatives to WEP**

The security of WLANs is the biggest barrier to implement them in most business worlds. Over 80 percent of participants of a survey done by Network Computing answered, that the security flaws are the biggest obstacles for using wireless networks. The IEEE 802.11 task group recognized this problem and tried to bring up a new encryption schema. Unfortunately, this task group struggled to gain enough vendor consensus to release a new wireless security standard. Several companies recognized this opportunity and released their own WLAN security overlays.

These security overlays are independent, incompatible extensions from certain manufacturers (like Agere Systems, Cisco Systems, and others). Most of these overlays bring improved security as well as other features (like key management). The main drawback is the non existing standard - it's a proprietary development by every manufacturer individually and therefore lacks multivendor interoperability.

### **CONCLUSION**

Out of the box, WLANs aren't secure (most default values disable any security features). By enabling the built-in security features and tweaking the environment, the security of a WLAN can be improved a lot. Because of the faulty implementation of WEP, wireless LANs aren't secure enough to send vital information. By using VPN technology, WLANs can be further secured to provide a reliable, handy alternative to conventional networks.